Podręcznik Inspektora Ochrony Danych

Wytyczne dla inspektorów ochrony danych w sektorze publicznym i quasi-publicznym dotyczące sposobu zapewnienia zgodności z europejskim ogólnym rozporządzeniem o ochronie danych

(Rozporządzenie (UE) nr 2016/679)

Opracowano dla finansowanego ze środków UE programu „T4DATA”

(Numer umowy w sprawie przyznania dotacji: 769100 — T4DATA — REC-DATA-2016/REC-DATA-2016-01)

opracował

Douwe Korff

Emerytowany profesor prawa międzynarodowego, London Metropolitan University
Współpracownik Oxford Martin School, University of Oxford

oraz

Marie Georges

Niezależny specjalista ds. międzynarodowej ochrony danych
(Ex-CNIL, UE, Rada Europy, itd.)

Członkowie europejskiej grupy ekspertów ds. praw podstawowych
(Fundamental Rights Experts Europe (FREE) Group)

przy znaczącym wkładzie włoskiego urzędu ochrony danych

i partnerów projektu

(Zatwierdzone przez Komisję Europejską, lipiec 2019 r.)

O Podręczniku:

Niniejszy Podręcznik opracowano jako element materiałów szkoleniowych dla finansowanego ze środków UE programu szkolenia trenerów „T4DATA", którego celem jest szkolenie pracowników w ramach wielu organów ochrony danych w zakresie szkolenia inspektorów ochrony danych, w szczególności w sektorze publicznym, w związku z ich nowymi obowiązkami wynikającymi z unijnego ogólnego rozporządzenia o ochronie danych (Rozporządzenie 2016/679, RODO). Projekt realizowany jest pod auspicjami włoskiego organu ochrony danych, *Garante per la protezione dei dati personali* (dalej: *„Garante"* lub *„Garante della Privacy"),* zaś organem administrującym projekt jest *Fondazione Basso* wspierana przez dwóch ekspertów z europejskiej grupy ekspertów ds. praw podstawowych (*Fundamental Rights Experts Europe,* FREE), panią Marie Georges i prof. Douwe Korffa.

Podręcznik zawiera znaczny wkład przekazany od Garante, a także od innych partnerów-organów nadzorczych, którzy przesłali bardzo przydatne praktyczne przykłady i kopie własnych wytycznych dotyczących RODO.

Należy zauważyć, że jeżeli dana kwestia dotyczy jednej z wcześniejszych prac wyżej wspomnianych dwóch ekspertów, nazwisko eksperta jest podawane w odpowiednim przypisie wyłącznie wtedy, gdy mowa jest o ogólnodostępnych zasobach. W przypadku pani Marie Georges sytuacja taka rzadko ma miejsce, głównie z przyczyn instytucjonalnych lub poufnych dotyczących jej pracy nad ochroną danych na rzecz krajowych i międzynarodowych organów rządowych.

Więcej informacji na temat programu, partnerów i ekspertów dostępnych jest na stronie:

http://www.fondazionebasso.it/2015/wp-content/uploads/2018/04/T4Data_Brochure.pdf

Mimo że opracowano go dla programu T4DATA, autorzy mają nadzieję, że Podręcznik ten będzie także przydatny dla wszystkich osób zainteresowanych stosowaniem Rozporządzenia, w tym w szczególności dla innych inspektorów ochrony danych (w sektorze publicznym lub prywatnym). Podręcznik jest także udostępniany publicznie w ramach licencji „Creative Commons" (CC).

Uwaga: Ponieważ celem Podręcznika jest wspieranie szkolenia inspektorów ochrony danych w zakresie nowych obowiązków wynikających z RODO, koncentruje się on na unijnych przepisach o ochronie danych, a konkretnie na prawie ochrony danych w odniesieniu do spraw zwanych w przeszłości „filarem pierwszym" lub „rynkiem wewnętrznym". Niemniej jednak w sekcjach 1.3.4 - 1.3.6 oraz 1.4.3 - 1.4.5 znajduje się krótkie wprowadzenie do przepisów i instrumentów ochrony danych, które miały lub mają zastosowanie do innych kwestii objętych prawem UE, tj. kwestii wchodzących w zakres tego, co kiedyś nazywano „Wymiarem sprawiedliwości i sprawami wewnętrznymi" lub „trzecim filarem" - obecnie określanym jako przestrzeń „wolności, bezpieczeństwa i sprawiedliwości"; kwestii związanych z tzw. Wspólną Polityką Zagraniczną i Bezpieczeństwa (WPZiB) - poprzedni „drugi filar"; oraz działalności samych instytucji UE; natomiast sekcja 1.4.6 omawia przekazywanie danych między różnymi systemami UE. Podręcznik nie obejmuje ochrony danych poza UE/EOG, mimo że uważamy, iż inspektorzy ochrony danych powinni zdobyć co najmniej częściową wiedzę na temat znaczącego obecnego i przyszłego oddziaływania zasad UE na ochronę danych na świecie.

Mamy nadzieję, że będziemy w stanie dodać te kwestie do późniejszego, drugiego wydania Podręcznika, w którym powinniśmy także zaktualizować informacje na temat kwestii, które w trakcie pisania pierwszego wydania pozostawały jeszcze nierozstrzygnięte, w szczególności takie jak zmiany dotyczące rozporządzenia o e-prywatności, które w momencie pisania w dalszym ciągu są przedmiotem procesu legislacyjnego.

Podręcznik jest także dostępny w języku włoskim, chorwackim, bułgarskim, polskim, hiszpańskim (tj. w językach wszystkich partnerów). Rozważa się wydanie kolejnych wersji językowych (w szczególności wersji francuskiej) w zależności od zasobów finansowych.

<u>Informacja o zrzeczeniu się odpowiedzialności</u>:

Informacje i poglądy przedstawione w tym podręczniku pochodzą od autorów i niekoniecznie odzwierciedlają oficjalne stanowisko Unii Europejskiej. Zarówno instytucje i organy Unii Europejskiej, jak i żadna osoba działająca w ich imieniu nie mogą ponosić odpowiedzialności za sposób wykorzystania zawartych w podręczniku informacji.

Powielanie jest dozwolone pod warunkiem podania autorów i źródła.

Słowo wstępne

Wierzymy, że to pierwsze wydanie „Podręcznika", opracowanego w ramach finansowanego ze środków UE projektu „T4DATA - szkolenie organów ochrony danych i inspektorów ochrony danych", jest czymś więcej niż kolejnym podręcznikiem dotyczącym RODO. Jest to z pewnością praktyczny podręcznik, który powstał po pierwsze dzięki ciężkiej pracy i zaangażowaniu dwóch ekspertów wybranych do tego zadania: Pani Marie Georges i Profesora Douwe Korffa, którzy od wielu lat zajmują się prawami człowieka, technologiami informacyjno – komunikacyjnymi oraz kwestiami ochrony danych, zarówno w sferze koncepcyjnej, jak i praktycznej, a po drugie, dzięki kompetentnemu wkładowi urzędników i członków pięciu organów nadzorczych uczestniczących w projekcie, którzy dzięki swojej codziennej praktyce i doświadczeniu zapewnili znaczący wkład do Podręcznika.

Jest to przede wszystkim praca w toku, żywe prawo, a nie tylko martwa litera. Podręcznik ma przede wszystkim wyjaśnić nowe, niewątpliwie bardziej wymagające zadania związane z rozliczalnością, określone w nowych ramach prawnych UE – które mają na celu zapewnienie bardziej skutecznej ochrony danych na świecie, w którym przetwarzanie danych przejawia się we wszystkich wymiarach życia. Podręcznik przedstawia praktyczne, solidne, udokumentowane wskazówki i porady, które zostaną dostosowane i poszerzone dzięki krajowym działaniom upowszechniającym i szkoleniowym, kontynuowanym w 2019 roku na podstawach niniejszego podręcznika. Adresatami przedstawionych wskazówek są inspektorzy ochrony danych, a szczególnie inspektorzy ochrony danych pełniący tę funkcję w sektorze publicznym, którzy będą mogli wykorzystać Podręcznik jako swego rodzaju narzędzie do wzmocnienia i podniesienia swoich kompetencji odnośnie rozwiązywania problemów z zakresu ochrony danych z korzyścią dla wszystkich zainteresowanych stron - administratorów, osób których dane dotyczą oraz ogółu społeczeństwa.

W związku z powyższym, pięć organów nadzorczych zdecydowało się połączyć siły w celu wdrożenia Projektu T4DATA. Jesteśmy szczególnie usatysfakcjonowani wynikiem Projektu, jakim jest angielska wersja tego Podręcznika, który został przetłumaczony na nasze języki narodowe – mamy nadzieję, że w przyszłości również na język francuski - co również wzmocni łańcuch narzędzi naszej codziennej współpracy rozwijanej na poziomie europejskim.

dr Edyta Bielak – Jomaa, Prezes Urzędu Ochrony Danych Osobowych w Polsce

Mar España Martí, Dyrektor Hispańskiej Agencji Ochrony Danych

Ventsislav Karadjov, Przewodniczący Komisji Ochrony Danych Osobowych w Bułgarii

Anto Rajkovača, Dyrektor Chorwackiej Agencji Ochrony Danych Osobowych

Antonello Soro – Przewodniczący Włoskiego Organu Ochrony Danych Osobowych

SPIS TREŚCI

Zadania organizacyjne:

Funkcja monitorowania przestrzegania prawa:

Funkcje doradcze:

Współpraca i konsultacje z organem ochrony danych:

Obsługa wniosków osób, których dane dotyczą:

Informowanie i podnoszenie świadomości:

- o – O – o -

Wytyczne dla inspektorów ochrony danych w sektorze publicznym i quasi-publicznym dotyczące sposobu zapewnienia zgodności z unijnym ogólnym rozporządzeniem o ochronie danych

(Rozporządzenie (UE) nr 2016/679)

Wprowadzenie

Od 25 maja 2018 roku stosujemy nowe unijne Ogólne rozporządzenie o ochronie danych (**RODO** lub „**Rozporządzenie**")[1], które zastąpiło Dyrektywę o ochronie danych z 1995 roku („Dyrektywa z 1995 roku").[2] Przyjęte w odpowiedzi na masową ekspansję procesu przetwarzania danych osobowych, która miała miejsce od czasu wprowadzenia Dyrektywy z 1995 roku, a także na rozwój coraz bardziej inwazyjnych technologii, Rozporządzenie oparte jest na Dyrektywie oraz wydanym na jej podstawie orzecznictwie Trybunału Sprawiedliwości UE. Rozporządzenie znacząco poszerza postanowienia Dyrektywy i jednocześnie mocno wzmacnia główny system ochrony danych w UE. Wprowadza wiele zmian dotyczących znacznie większej harmonizacji, silniejszych praw osób, których dane dotyczą, bliższej transgranicznej współpracy egzekucyjnej pomiędzy organami ochrony danych itp.

Wśród najistotniejszych zmian jest wprowadzenie nowej zasady, tj. zasady „rozliczalności", oraz instytucji inspektorów ochrony danych. Obydwa te elementy są ze sobą powiązane - inspektorzy ochrony danych to osoby, które będą w praktyce zapewniać przestrzeganie zasady rozliczalności przez organizacje i w ramach organizacji, do których należą. Celem niniejszego Podręcznika jest wsparcie nowych inspektorów ochrony danych w sektorze publicznym w tego typu staraniach.

Niniejszy Podręcznik składa się z trzech części:

- **Część pierwsza** prezentuje koncepcje „poufności", „prywatności" i „ochrony danych" oraz pierwsze przepisy, zasady i instrumenty międzynarodowe w sprawie ochrony danych (w szczególności Konwencję Rady Europy o ochronie danych z 1981 roku), a następnie omawia stanowiące „pierwszy filar" unijne dyrektywy o ochronie danych z lat 90. XX wieku oraz początku XXI wieku i przedstawia ostatnio przyjęte i aktualnie oczekujące na przyjęcie instrumenty ochrony danych (RODO, proponowane rozporządzenie o e-prywatności i „zmodernizowaną" konwencję Rady Europy)[3]. Część pierwsza nie omawia jednak unijnych instrumentów „trzeciego filara" stosowanych w latach 90. XX wieku ani zasad ochrony danych dotyczących własnych instytucji UE i ich następców.*

  * Mamy nadzieję, że w przyszłości możliwe będzie opracowanie poszerzonego drugiego wydania niniejszego Podręcznika, w którym właściwie omówione zostaną także te instrumenty.

- **Część druga** prezentuje przegląd wszystkich kluczowych elementów ogólnego rozporządzenia o ochronie danych i następnie przechodzi do dodatkowej, nowej podstawowej zasady „rozliczalności" oraz zawartych w RODO koncepcji i zasad dotyczących inspektora ochrony danych;

- **Część trzecia** zawiera praktyczne wytyczne na temat tego, jak inspektorzy ochrony danych w sektorze publicznym mogą i powinni wypełniać swoje rozliczne zadania, z uwzględnieniem wziętych z życia przykładów, w szczególności w odniesieniu do trzech najważniejszych obszarów: edukacji, finansów i opieki zdrowotnej. W części tej zawarto także stosowne ćwiczenia.

---

[1] Pełny tytuł: Rozporządzenie (UE) 2016/679 Parlamentu Europejskiego i Rady z 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), O.J. L 119 z 4.5.2016, str. 1ff, dostępne na stronie http://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32016R0679&from=pl Należy zauważyć, że chociaż rozporządzenie zostało przyjęte w 2016 r. i zgodnie z prawem „weszło w życie" dwudziestego dnia po jego opublikowaniu w Dzienniku Urzędowym Unii Europejskiej, tj. 25 maja tego roku (art. 99 ust. 1), wszedł on w zakres „stosowania" - tj. został skutecznie zastosowany - od 25 maja 2018 r. (art. 99 ust. 2).

[2] Pełny tytuł: Dyrektywa Parlamentu Europejskiego i Rady 95/46/WE z dnia 24 października 1995 w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych, OJ L 281 z 23.11.1995 r. str. 31ff, dostępna na stronie: http://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:31995L0046&from=pl

[3] Kwestię ograniczeń dotyczących omawianych spraw przedstawiono w uwadze w polu „*O niniejszym Podręczniku*" na str. 1.

Poza wieloma odwołaniami i linkami do materiałów w stopce, w osobnym drugim tomie Podręcznika przedstawiono dalsze materiały, które zostaną udostępnione uczestnikom w trakcie szkoleń „T4DATA".

Strona internetowa:

Tak wiele, jak to możliwe, z powyższych materiałów i linków zostanie także opublikowanych na ogólnodostępnej stronie internetowej towarzyszącej niniejszemu Podręcznikowi (do której można uzyskać swobodny dostęp także ze strony w ramach licencji „Creative Commons"):

http://www.fondazionebasso.it/2015/t4data-training-data-protection-authorities-and-data-protection-officers/

CZĘŚĆ 1

Początki i znaczenie ochrony danych

W tej części staramy się wyjaśnić, czym jest ochrona danych i w jaki sposób rozwijała się ona w Europie oraz w jaki sposób nowe i „zmodernizowane" europejskie instrumenty ochrony danych mają sprostać najnowszym zmianom technologicznym.

- Punkt 1.1 prezentuje różne (lub nakładające się) opracowane w Europie koncepcje poufności, prywatności i życia prywatnego oraz ochrony danych i podejścia do ochrony danych, z uwzględnieniem wymogów dotyczących praw człowieka i praworządności, które stanowią podstawę ochrony danych w Europie.
- Punkt 1.2 obejmuje początki ochrony danych w Europie, pojawienie się podstawowych zasad i praw do ochrony danych oraz ich rozwój w europejskich i globalnych niewiążących instrumentach prawnych oraz w jednym wiążącym instrumencie, tj. Konwencji Rady Europy o ochronie danych z 1981 roku (z uwzględnieniem jej Protokołu dodatkowego z 2001 roku).
- Punkt 1.3 zajmuje się kierunkiem dalszych zmian odnośnie zasad ochrony danych z lat 90-tych i z początku 2000 roku (mających umożliwić rozwój unijnego „Wewnętrznego rynku", który wymagał zarówno swobodnego przepływu danych, jak i ochrony podstawowego prawa do ochrony danych) z naciskiem na Dyrektywę w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych z 1995 r. (a także na Protokół dodatkowy z 2001 roku do Konwencji z 1981 roku) (podsekcje 1.3.1 i 1.3.2); a także omawia specjalne zasady sektora telekomunikacyjnego (podsekcja 1.3.6).

  Ostatnie podsekcje tej części zwięźle zwracają uwagę na instrumenty ochrony danych w obszarze, który wcześniej nazywany był Wymiarem Sprawiedliwości i Spraw Wewnętrznych (WSiSW) (podsekcja 1.3.4); instrumenty związane ze Wspólną Polityką Zagraniczną i Bezpieczeństwa (WPZiB) (podsekcja 1.3.5); oraz instrumenty samych instytucji UE (podsekcja 1.3.6).
- Punkt 1.4 przedstawia najnowsze instrumenty prawne przyjęte, by spełnić przyszłe oczekiwania: unijne ogólne rozporządzenie o ochronie danych z 2016 roku (RODO, stosowane od 25 maja 2018 roku) (podsekcja 1.4.1) i proponowaną zamianę Dyrektywy WE o e-prywatności z 2002 roku wraz z Rozporządzeniem o e-prywatności (podsekcja 1.4.2).

  Kolejne podsekcje w tej sekcji zwięźle objaśniają nowy główny instrument ochrony danych w obszarze zwanym obecnie przestrzenią wolności, bezpieczeństwa i sprawiedliwości, Dyrektywę w sprawie ochrony danych w zakresie egzekwowania prawa z 2016 r. (podsekcja 1.4.3); sytuację w odniesieniu do WPZiB (podsekcja 1.4.4); oraz aktualizację instrumentu ochrony danych dla instytucji UE oraz rozporządzenie 2018/1725 (podsekcja 1.4.5). W podsekcji 1.4.6 omówiono przepływy danych między różnymi systemami ochrony danych w UE.

  „Zmodernizowana" Konwencja Rady Europy, otwarta do podpisu w październiku 2018 roku, została omówiona w końcowej podsekcji (podsekcja 1.4.7).

  Uwaga: Mamy nadzieję, że w drugim wydaniu Podręcznika uda nam się zaprezentować bardziej szczegółowo unijne instrumenty ochrony danych dla wyżej wymienionych obszarów (współpracy pomiędzy organami ścigania i sądami, WPZiB oraz instytucji UE) przyjętych w celu zastąpienia instrumentów z lat 90. XX wieku oraz początku XXI wieku, a także najnowsze zasady globalne.

RODO, stanowiące zasadniczy element Podręcznika, zostało bardziej szczegółowo przeanalizowane w części drugiej.

1.1 Poufność, prywatność/życie prywatne i ochrona danych: różne, ale uzupełniające się koncepcje w dobie cyfryzacji

1.1.1 Poufność i prywatność/życie prywatne

Zawsze istniały obszary, w których dane osobowe podlegały specjalnym zasadom **poufności**.

Klasycznymi przykładami są przysięga Hipokratesa składana przez **lekarzy**[4] oraz stosowana w kościele rzymskokatolickim „**tajemnica spowiedzi**"[5]. Ostatnio, w szczególności od XIX wieku, **bankierzy, prawnicy,** różni **duchowni, pracownicy pocztowi i telekomunikacyjni** oraz wiele innych osób zostało zobowiązanych do traktowania jako poufnych, uprzywilejowanych[6] lub nawet świętych, informacji otrzymanych od osób fizycznych w ramach pełnionych przez siebie funkcji urzędowych.

Takie zadania poufności ogólnie postrzegano jako służące zarówno jednostce, jak i społeczeństwu. Jednostka mogła wierzyć, że osoba, której ujawniała informacje, zachowa je w tajemnicy. Zaufanie takie z kolei służyło dobru publicznemu, gdyż jego brak może zniechęcić ludzi do poszukiwania pomocy lub ujawniania informacji organom, co osłabia zdrowie publiczne i inne świadczenia społeczne, np. w przypadku próby zapobiegania rozpowszechnianiu się chorób przenoszonych drogą płciową, czy ekstremizmu politycznego lub religijnego.

Jednak, jak wyjaśnia Frits Hondius, zastępca dyrektora ds. praw człowieka w Radzie Europy, który odpowiadał za sporządzenie projektu pierwszego międzynarodowego, wiążącego instrumentu o ochronie danych, tj. Konwencji Rady Europy o ochronie danych z 1981 roku, którą omówiono w pkt. 1.2.3 poniżej, pomimo obowiązku poufności:[7]

> nie przyznano odpowiedniego prawa pacjentom, klientom lub obywatelom, by mogli sprawdzić poprawność i stosowność dotyczących ich danych. I chociaż istniały sankcje umożliwiające karanie poważnych nadużyć w obsłudze danych, nie było przepisów określających pozytywne wskazania dotyczące sposobu właściwego tworzenia akt zawierających dane osobowe i zarządzania tego typu aktami.

Prawo do „**prywatności**" lub **„poszanowania życia prywatnego**" zostało zabezpieczone we wprowadzonych po II wojnie światowej międzynarodowych traktatach o prawach człowieka, Międzynarodowym Pakcie Praw Obywatelskich i Politycznych (ICCPR, art. 17) oraz Europejskiej Konwencji Praw Człowieka (ETPC, art. 8)[8]. Chroni ono przede wszystkim przed zbędną interwencją państwa w życie prywatne jednostki, taką jak przerywanie komunikacji przez agencje państwowe[9] lub uznanie prywatnych aktów seksualnych za przestępstwa[10]. Prawo to zostało także zinterpretowane przez Europejski Trybunał Praw Człowieka jako wymóg ochrony jednostek przez państwo przed publikacją ich zdjęć zrobionych przez podmioty prywatne bez ich zgody w prywatnych okolicznościach[11], oraz ochrona przed przerywaniem ich komunikacji przez pracodawców bez właściwej podstawy prawnej[12].

---

[4] Przysięgę Hipokratesa przypisywano Hipokratesowi (ok. 460-370 p.n.e.) w starożytności, chociaż nowe dane pokazują, że mogła ona zostać spisana już po jego śmierci. Najstarsza istniejąca wersja pochodzi z ok. 275 roku n.e. i brzmi następująco: ἃ δ᾽ ἂν ἐνθεραπείῃ ἴδω ἢ ἀκούσω, ἢ καὶ ἄνευ θεραπείης κατὰ βίον ἀνθρώπων, ἃ μὴ χρή ποτε ἐκλαλεῖσθαι ἔξω, σιγήσομαι, ἄρρητα ἡγεύμενος εἶναι τὰ τοιαῦτα. *„Cokolwiek bym podczas leczenia, czy poza nim, z życia ludzkiego ujrzał, czy usłyszał, czego nie należy na zewnątrz rozgłaszać, będę milczał, zachowując to w tajemnicy"* (tłumaczenie ze strony http://www.oil.org.pl/xml/oil/oil68/tematy/hipokr), zob.: https://pl.wikipedia.org/wiki/Przysiega_Hipokratesa

[5] W kościele rzymsko-katolickim „tajemnica spowiedzi" lub „pieczęć sakramentalna" jest nienaruszalna. Zob.: https://www.catholiceducation.org/en/religion-and-philosophy/catholic-faith/the-seal-of-the-confessional.html

[6] Według brytyjskiej Izby Adwokackiej (Solicitors Regulation Authority (SRA)), która nadzoruje adwokatów i kancelarie prawne w Anglii i Walii, (w angielskim prawie) istnieje „różnica pomiędzy poufnością a prawniczą tajemnicą zawodową. Krótko mówiąc, informacje poufne mogą zostać ujawnione, jeżeli jest to stosowne, ale prawnicza tajemnica zawodowa ma charakter bezwzględny i objęte nią informacje nie mogą zostać ujawnione. Poufne kontakty pomiędzy prawnikami a klientami w celu uzyskania i udzielenia porady prawnej mają charakter uprzywilejowany". https://www.sra.org.uk/solicitors/code-of-conduct/guidance/guidance/Disclosure-of-client-confidential-information.page
We Francji tajemnica zawodowa (*secret professionnel*) prawnika (*avocat*) jest kwestią *ordre public,* bezwzględną, bezterminową i obejmującą wszystkie typy spraw prawnych oraz wszelkie formy informacji (pisemne, elektroniczne, dźwiękowe, itd.), zob.: http://www.avocatparis.org/mon-metier-davocat/deontologie/secret-professionnel-et-confidentialite

[7] Frits Hondius, *A decade of international data protection*, w: Netherlands International Law Review, tom XXX (1983), str. 103 – 128 (niedostępne w internecie).

[8] Art. 12 Powszechnej deklaracji praw człowieka z 1948 roku, która była „macierzystym" instrumentem zarówno ICCPR, jak i ETPC (ale która sama w sobie nie stanowiła wiążącego traktatu), zgodnie z którym „Nie wolno ingerować samowolnie w czyjekolwiek życie prywatne, rodzinne, domowe, ani w jego korespondencję ...". ICCPR i ETPC opracowano równolegle w latach 1949-50 (przy czym ETPC, która była gotowa do podpisu pod koniec 1950 roku i weszła w życie w 1953 roku, ponad dwadzieścia lat przed ICCPR, która była gotowa do podpisu w 1966 roku i weszła w życie dopiero w 1976 roku).

[9] Np. ETPC, *Klass przeciwko państwu niemieckiemu*, wyrok z 6 września 1978 r.

[10] Np. ETPC, *Dudgeon przeciwko Zjednoczonemu Królestwu*, wyrok z 22 października 1981 r.

[11] Np. ETPC, *von Hannover przeciwko państwu niemieckiemu*, wyrok z 7 lutego 2012 r.

[12] Np. ETPC, *Halford przeciwko Zjednoczonemu Królestwu*, wyrok z 25 czerwca 1997 r.

Mimo, że art. 8 Europejskiej Konwencji Praw Człowieka (ETPC) był ostatnio coraz częściej interpretowany i stosowany, by chronić jednostki również pod kątem ich danych osobowych, a także w odniesieniu do gromadzenia, wykorzystywania i zatrzymywania ich danych, w szczególności przez państwowe i krajowe agencje bezpieczeństwa[13], w latach 70. i 80. XX wieku zakres, w jakim prawo do prywatnego życia mogło polegać na relacjach pomiędzy osobami fizycznymi oraz pomiędzy osobami fizycznymi a prywatnymi podmiotami (tak zwana kwestia „horyzontalnego oddziaływania praw człowieka" lub *Drittwirkung*) był w dalszym ciągu niejasny[14] – i nie został jeszcze w pełni rozstrzygnięty, jeżeli chodzi o przepisy prawne dotyczące tradycyjnych praw człowieka. W każdym bądź razie jednostki nie mogą na podstawie ETPC (lub ICCPR) dochodzić prawa do wniesienia skargi przeciwko innym osobom fizycznym, a mogą jedynie podjąć działania przeciwko odpowiedniej stronie państwowej za niezapewnienie im w odpowiednim prawie krajowym ochrony przed działaniami innych jednostek.

Podsumowując, przepisy i zasady dotyczące poufności i tajemnicy zawodowej oraz gwarancje praw człowieka obejmujące prywatność i życie prywatne nie chroniły i nie chronią odpowiednio jednostek przed niewłaściwym gromadzeniem i wykorzystaniem ich danych osobowych.

W efekcie ostatnio uznano osobne i odrębne prawo do „**ochrony danych osobowych"** („ochrony danych"), które omówiono poniżej. Ale oczywiście to nowe prawo *sui generis* musi być zawsze postrzegane jako blisko związane z tradycyjnymi prawami oraz takie tradycyjne prawa uzupełniające, co podkreśla w szczególności ETPC i ICCPR: celem ochrony danych jest zapewnienie pełnego i skutecznego stosowania tradycyjnych praw we względnie nowym kontekście cyfrowym.

1.1.2 „Ochrona danych"

Komputery zbudowano najpierw dla celów wojskowych w trakcie **II wojny światowej**. Brytyjscy łamacze kodów pod kierownictwem wielkiego Alana Turinga[15] zbudowali prymitywne wersje do odszyfrowywania niemieckich kodowanych komunikatów *Enigma* i *Lorenz*[16]. W Stanach Zjednoczonych firma IBM, pod przywództwem swojego pierwszego dyrektora generalnego Thomasa J. Watsona, wyprodukowała ogromne ilości urządzeń do przetwarzania danych dla celów militarnych i rozpoczęła eksperymenty z komputerami analogowymi[17]. Niemcy zaś wykorzystywali je do obliczania trajektorii pocisków rakietowych *V2*[18].

Potrzeba ochrony praw człowieka i swobód w demokracji w odniesieniu do zautomatyzowanego przetwarzania danych osobowych pojawiła się dopiero później, gdy w latach **60. XX wieku** komputery zaczęły być wykorzystywane w procesach zarządzania w sektorze publicznym i prywatnym. Ale ze względu na wysokie koszty komputerów i znaczną powierzchnię, jakiej w tym czasie wymagały, miało to miejsce wyłącznie w krajach rozwiniętych, i to tylko w przypadku dużych organów państwowych i spółek. Pierwsze zastosowanie komputerów związane było z wypłatą wynagrodzeń i należności dla dostawców, rejestracją pacjentów w szpitalach, spisem powszechnym i statystyką oraz aktami policyjnymi.

W świetle wyżej wspomnianych zmian pod koniec lat **60. I na początku lat 70. XX wieku** takie same debaty zaczęły toczyć w Niemczech (w szczególności w landzie Hessen w sprawie akt policyjnych), Norwegii, Szwecji i Francji (w szczególności ze względu na pamięć o nadużyciach rejestrów populacji i innych rejestrów publicznych przez okupantów nazistowskich w czasie II wojny światowej),

---

[13] Zob. arkusz informacyjny Rady Europy – Ochrona danych osobowych, 2018, dostępny na stronie: https://www.echr.coe.int/Documents/FS_Data_ENG.pdf. Przykładowa lista spraw prowadzonych przez Europejski Trybunał Praw Człowieka w odniesieniu do ochrony danych osobowych dostępna jest na stronie: https://www.coe.int/en/web/data-protection/echr-case-law. By zapoznać się z ogólniejszą dyskusją, zob: Lee A Bygrave, *Data Protection Pursuant to the Right to Privacy in Human Rights Treaties*, International Journal of Law and Information Technology, 1998, tom 6, str. 247–284, https://www.uio.no/studier/emner/jus/jus/JUR5630/v11/undervisningsmateriale/Human_rights.pdf

[14] Zob.: Hondius, o.c. (przypis 7, powyżej), str. 107, z nawiązaniem do Report by the Committee of Experts on Human Rights, Rada Europy (DH/EXP(70)15).

[15] Patrz: http://www.maths.manchester.ac.uk/about-us/history/alan-turing/

[16] Zob.: Chris Smith, *Cracking the Enigma code: How Turing's Bombe turned the tide of WWII*, 2 listopada 2017 r. http://home.bt.com/tech-gadgets/cracking-the-enigma-code-how-turings-bombe-turned-the-tide-of-wwii-11363990654704 Maszyna *Colossus,* wykorzystywana do odkodowywania komunikatów *Lorenz,* jest traktowana jako „pierwszy na świecie programowalny, elektroniczny komputer cyfrowy". Zob.: https://pl.wikipedia.org/wiki/Colossus

[17] Zob.: https://en.wikipedia.org/wiki/Thomas_J._Watson

[18] Zob.: Helmut Hoelzer's Fully Electronic Analog Computer used in the German V2 (A4) rockets (głównie w języku niemieckim), http://www.cdvandt.org/Hoelzer%20V4.pdf

Zjednoczonym Królestwie, Stanach Zjednoczonych itd., a także w OECD i Radzie Europy[19]. Na początku debaty te prowadzone były pomiędzy specjalistami podlegającymi obowiązkom etycznym (w Stanach Zjednoczonych w szczególności pomiędzy lekarzami i inżynierami informatykami, którzy jako pierwsi opracowali wytyczne dotyczące „uczciwych praktyk informacyjnych")[20] oraz pomiędzy politykami, którzy obawiali się ryzyka nadużyć lub niewłaściwego zastosowania oraz zabezpieczenia przetwarzanych automatycznie danych osobowych.

W **połowie i pod koniec lat 70. i na początku lat 80. XX wieku** kwestie te następnie zostały przekazane szerszej grupie odbiorców - we Francji pierwszym głównym katalizatorem było ujawnienie w 1974 roku przez informatorów planów rządowych zakładających stworzenie krajowej bazy danych wszystkich obywateli i rezydentów francuskich wraz z unikalnym numerem identyfikacyjnym dla każdego z nich, a także faktu istnienia spornych akt policyjnych[21]. W Niemczech, w ogólnie napiętym klimacie politycznym, istniała szeroka opozycja wobec proponowanego spisu powszechnego w 1983 roku[22]. Debaty te nie dotyczyły jedynie możliwości ryzyka naruszenia prywatności poprzez zastosowanie nowych technologii, ale także konsekwencji błędów danych i możliwej autorytarnej władzy stworzonej poprzez centralizowanie gromadzonych w różnych celach danych i/lub wykorzystywanie unikalnych identyfikatorów w powiązanych zbiorach. W Europie doprowadziło to do zapotrzebowania na konkretną, ustawowo umocowaną „ochronę danych" lub „informatykę i wolności", wzmocnionej rosnącym uznaniem tej potrzeby przez trybunały konstytucyjne i inne sądy najwyższe, oraz do przyjęcia instrumentów międzynarodowych (omówionych w pkt. 1.2 poniżej).

Zwrot „ochrona danych" (niemieckie ***Datenschutz***) został pierwotnie ukuty w tytule pierwszej ustawy w tym temacie, tj. ustawy o ochronie danych z 1970 roku (*Datenschutzgesetz*) w niemieckim landzie Hessen, opracowanej przez „ojca ochrony danych", profesora Spirosa Simitisa[23]. Jak wskazuje Burkert, tytuł ten był faktycznie „niewłaściwy, ponieważ [ustawa] nie chroniła danych, tylko prawa osób, których dane obsługiwano"[24].

Ale przyjął się i obecnie znany na całym świecie zwrot ten (Francuzi mówią także ***protection des données***) oznacza w skrócie „ochronę jednostek w związku z przetwarzaniem danych osobowych" (pełny zwrot zastosowano w tytułach Dyrektywy WE o ochronie danych z 1995 roku oraz unijnego Ogólnego rozporządzenia o ochronie danych z 2016 roku)[25]. Ale nawet ten pełniejszy zwrot nie wyjaśnia dokładnie znaczenia koncepcji w oczach i umysłach Europejczyków.

Ochrona danych obejmuje zarówno aspekty indywidualnej wolności, jak i aspekty społeczne.

W związku z tym we Francji (gdzie prawo stosuje wyrażenie „informatyka, akta i wolności" / „informatique, fichiers et libertés") ochrona danych jest postrzegana jako element dwoistych wymogów dotyczących jednostki i społeczeństwa oraz wymogów konstytucyjnych, zakładających, że:

Informatyka musi służyć każdemu obywatelowi. … Nie może zagrażać tożsamości człowieka,

---

[19] Rada Europy przyjęła swoje pierwsze uchwały w tych sprawach w 1973 i 1974 roku: Uchwała Komitetu Ministrów (73) 22 i (74) 29 (linki podano w przypisie 39 i 40 poniżej). Patrz: Uzasadnienie do Konwencji Rady Europy o ochronie danych z 1981 roku, par. 6 https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800ca434 Zasady przytoczone w tych uchwałach uwzględniono w Załączniku 1 do Podręcznika.

[20] Zob.: Robert Gellman, Fair Information Practices: A basic history, https://bobgellman.com/rg-docs/rg-FIPshistory.pdf Przez wiele lat, od lat 70. do lat 90. XX wieku, Gellman pracował w Izbie Reprezentantów nad amerykańskimi kwestiami prawnymi dotyczącymi prywatności.

[21] Zob.: artykuł w gazecie Le Monde z 21 marca 1974 r. „*SAFARI ou la chasse aux Français*" („SAFARI lub polowanie na Francuzów") http://rewriting.net/2008/02/11/safari-ou-la-chasse-aux-francais/. Nazwa bazy danych SAFARI to akronim „*système automatisé pour les fichiers administratifs et le répertoire des individus*" (zautomatyzowany system gromadzenia dossier administracyjnych i akt osób fizycznych), ale także dlatego że minister odpowiedzialny za projekt był fanem safari w Afryce. W kolejnych dniach rewelacja ta stała się przedmiotem artykułów we wszystkich innych gazetach, a rząd wstrzymał projekt kilka dni później, ustanawiając doraźną komisję do zbadania całego problemu i zaproponowania rozwiązań prawnych.

[22] Zob.: Marcel Berlinghoff, *Zensus und Boykott. Die Volkszählung vor 30 Jahren*, w: Zeitgeschichte-online, czerwiec 2013 r. https://zeitgeschichte-online.de/kommentar/zensus-und-boykott-die-volkszaehlung-vor-30-jahren

[23] *Hessisches Datenschutzgesetz (HDSG) 1970*, w mocy od 13 października 1970 r., *Gesetz- und Verordnungsblatt für das Land Hessen, Teil I*, 1970, Nr 41 (12 października 1970), str. 625ff, tekst oryginalny (w języku niemieckim) na stronie: http://starweb.hessen.de/cache/GVBL/1970/00041.pdf

[24] Herbert Burkert, Privacy-Data Protection: A German/European Perspective (bez daty, ok. 2000 r.), str. 46 http://www.coll.mpg.de/sites/www/files/text/burkert.pdf

[25] RODO stosuje zwrot „osoby fizyczne" zamiast „jednostki".

> **prawom człowieka, życiu prywatnemu ani wolnościom osobistym i publicznym**[26]
>
> (Art. 1 ustawy o informatyce, aktach i wolnościach z 1978 roku)

Francuska ustawa uzyskała status konstytucyjny, a decyzje sądów najwyższych we Francji oparte są na prywatności lub swobodzie, w zależności od analizowanej kwestii.

W Niemczech ochrona danych postrzegana jest przede wszystkim jako ochrona wynikająca z podstawowego (proto-) prawa do „[poszanowania] osobowości człowieka" (*das allgemeine Persönlichkeitsrecht*), gwarantowanego w art. 2(1) Konstytucji, w powiązaniu z art. 1(1). Na tej podstawie Trybunał Konstytucyjny w swoim słynnym wyroku *Census* z 1983 roku wysunął bardziej szczegółowe prawo do „**decydowania o wykorzystywaniu własnych danych**" (*informationelle Selbstbestimmung*)[27]. Jednak *Bundesverfassungsgericht* w dalszym ciągu wyraźnie i zdecydowanie wiązała to prawo jednostki z szerszymi i podstawowymi normami społecznymi[28]:

> Porządek społeczno-prawny, w którym obywatel nie wie już kto, co i kiedy o nim wie oraz w jakiej sytuacji, jest niezgodny z prawem do decydowania o wykorzystywaniu własnych danych. Osoba, która zastanawia się, czy nietypowe zachowanie jest za każdym razem odnotowywane i następnie przechowywane w rejestrze, wykorzystywane lub rozpowszechniane, będzie starała się nie zwracać na siebie w ten sposób uwagi. Osoba, która zakłada na przykład, że uczestnictwo w spotkaniu lub inicjatywie obywatelskiej jest oficjalnie rejestrowane i może rodzić dla niej ryzyko, może zdecydować się nie korzystać z odpowiednich podstawowych praw ([gwarantowanych] art. 8 i 9 Konstytucji). Ograniczyłoby to nie tylko możliwości rozwoju osobistego jednostki, ale także dobra wspólnego, ponieważ samostanowienie jest zasadniczym warunkiem koniecznym wolnego i demokratycznego społeczeństwa, opartego na zdolności i solidarności swoich obywateli.

Inne państwa europejskie, chociaż z gotowością zaakceptowały potrzebę ochrony danych i faktycznie często ją podkreślają w swoich konstytucjach jako prawo *sui generis*[29], nie wszystkie przyjęły niemiecką koncepcję decydowania o wykorzystywaniu własnych danych. Często bowiem uważały, że kładzie ona zbyt duży nacisk na aspekt wolności jednostki i niewystarczająco wzmacnia szersze aspekty społeczne[30]. W dalszym ciągu zasadniczo w Europie wszyscy zgadzają się, że, jak ujął to już Hondius w 1983 roku[31]:

> Celem ochrony danych jest zabezpieczenie sprawiedliwej i rozsądnej równowagi pomiędzy interesami jednostek a interesami społeczności [w odniesieniu do przetwarzania danych osobowych].

Państwa europejskie przyjęły stanowisko w celu zapewnienia takiej równowagi, należy stosować następujące **zasady regulacyjne**:

- gromadzenie oraz dalsze wykorzystywanie i ujawnianie danych osobowych powinno podlegać **prawu** (tj. **wiążącym regułom prawnym**, a nie dobrowolnym kodeksom lub niewiążącym wytycznym)[32];
- przepisy takie powinny mieć charakter **przepisów** „**zbiorczych**", które z zasady mają zastosowanie do wszystkich podmiotów publicznych i prywatnych przetwarzających dane

---

[26] *„L'informatique doit être au service de chaque citoyen. ... Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques."* Pominięte zdanie wskazuje, że „[Ochronę danych] należy wprowadzić w ramach współpracy międzynarodowej".

[27] BVerfG, 15.12.1983, BVerfGE Bd. 65, S. 1 ff. w sprawie „decydowania o wykorzystywaniu własnych danych", patrz § 151ff.

[28] *Idem*, § 154 (nasze tłumaczenie).

[29] Zob.: austriacka ustawa o ochronie danych z 1978 roku, zawiera w swoim pierwszym artykule zapis „konstytucyjny", na mocy którego ochrona danych stanowić ma konstytucyjnie chronione prawo. Ochrona danych jest także wyraźnie przewidziana w konstytucjach krajów, które wprowadziły demokrację w obecnej erze, takich jak Hiszpania (art. 18-4), Portugalia (art. 35), Grecja (art. 9A), Węgry (art. 59), Litwa (art. 22), Słowenia (art. 38), Słowacja (art. 19) lub które zmieniły swoją konstytucję, by odzwierciedlić potrzeby nowoczesnego społeczeństwa, takie jak Holandia (art. 10).

[30] Zob. np. blog *Informationelle Selbstbestimmung - (noch) kein neues Grundrecht*, 26 października 2017 r. w sprawie odmowy niższej izby szwajcarskiego parlamentu federalnego (*Nationalrat*), by podkreślić zasadę decydowania o wykorzystywaniu własnych danych w szwajcarskiej Konstytucji federalnej: https://www.humanrights.ch/de/menschenrechte-schweiz/inneres/person/datenschutz/informationelle-selbstbestimmung. Także w Holandii zasada ta nie została przyjęta w prawie ani przez sądy, nawet mimo tego, ze sąd najwyższy, *Hoge Raad*, działał pod wpływem orzecznictwa niemieckiego Trybunału Konstytucyjnego. Zob.: T. F. M. Hooghiemstra, Tekst en toelichting Wet bescherming persoonsgegevens (2001), ust. 4.3 (str. 18).

[31] Hondius, o.c. (przypis 7 powyżej), str. 108.

[32] Zob.: interpretacja koncepcji „prawa" w Europejskiej Konwencji Praw Człowieka (w szczególności art. 8 – 11) przez Europejski Trybunał Praw Człowieka.

osobowe (z uwzględnieniem wyjątków oraz modyfikacji tego typu zasad przewidzianych w zasadach szczególnych, jeżeli i gdy jest to konieczne, ale zawsze z poszanowaniem ich „zasadniczego znaczenia");

- prawo takie musi zawierać pewne **podstawowe przepisy prawa materialnego** (odzwierciedlające „**podstawowe" zasady ochrony danych** omówione w następnym punkcie) oraz przyznawać osobom, których dane dotyczą, **istotne prawa indywidualne** oraz
- zastosowanie takich przepisów powinno podlegać nadzorowi **specjalnych organów nadzorczych** (zazwyczaj zwanych **organami ochrony danych**).

1.2 Pierwsze przepisy, zasady i instrumenty międzynarodowe w sprawie ochrony danych[33]

1.2.1 Pierwsze ustawy o ochronie danych

„Europa zachodnia jest kolebką ochrony danych"[34]

Jak już wspomniano, pierwszą ustawą o ochronie danych na świecie była **przyjęta we wrześniu 1970 roku *Datenschutzgesetz* niemieckiego landu Hessen**[35]**.** Ustawa ta wprowadziła również pierwszy niezależny organ ochrony danych (chociaż ze względu na kwestie kompetencji państwowych, wyłącznie dla sektora publicznego i z ograniczonymi uprawnieniami mediacyjnymi w miejsce uprawnień egzekucyjnych).

W tej samej dekadzie, po ustawie o ochronie danych z Hessen, w Europie przyjęto krajowe (ogólnokrajowe) ustawy o ochronie danych w **Szwecji (1973)**, pierwszą **niemiecką federalną ustawę o ochronie danych (koniec 1977)** (która obejmowała przetwarzanie danych osobowych przez agencje federalne i sektor prywatny), **francuską ustawę o informatyce, aktach i wolnościach z 6 stycznia 1978 r.**, ustawy w **Austrii**, **Danii**[36] i **Norwegii (wszystkie w 1978 r.)** oraz w **Luksemburgu (1979)**. Chociaż niektóre z nich, jak na przykład niemiecka ustawa federalna, przewidywały osobne zestawy zasad dla sektora publicznego (federalnego) i prywatnego, w dalszym ciągu stanowiły przepisy „zbiorcze", ponieważ zasady dla obydwu sektorów oparte były na takich samych podstawowych zasadach i prawach, często wynikających z konstytucji[37].

1.2.2 Podstawowe zasady

Wprowadzone w Europie w 1970 roku ustawy opierały się w coraz większym stopniu na ogólnie akceptowanym (szeroko określonym) **zestawie „podstawowych" zasad i praw.** Były podobne do podstawowych zasad *Uczciwych praktyk informacyjnych* sporządzonych mniej więcej w tym samym

[33] W celu uzyskania danych historycznych, ze szczególnym uwzględnieniem projektu tworzonego równolegle do Wytycznych OECD z 1980 r. oraz Konwencji Rady Europy o ochronie danych z 1981 r., a także już wtedy pojawiających się różnic poglądów pomiędzy Europą a Stanami Zjednoczonymi, zob.: Frits Hondius, o.c. (przypis 7 powyżej), str. 103 – 128 oraz Uzasadnienie Konwencji Rady Europy, o.c. (przypis 19 powyżej), par. 14. Bardzo przydatny ogólny przegląd historycznych zmian w zakresie prywatności przedstawiono w rozdziale 4 zaktualizowanych Ram OECD w zakresie ochrony prywatności, zatytułowanym *Zmieniający się krajobraz prywatności: 30 lat po przyjęciu Wytycznych OECD w zakresie prywatności*, który omówiono bardziej szczegółowo poniżej (zob.: przypis 41 poniżej). Fascynujący osobisty raport na temat działań towarzyszących opracowaniu Wytycznych OECD oraz polityki (Europa vs. Stany Zjednoczone) i osobowości zaangażowanych w ten proces (Frits Hondius, Louis Joinet, Stefano Rodota i Spiros Simitis) sporządził Michael Kirby, Privacy Today: Something Old, Something New, Something Borrowed, Something Blue, Journal of Law, Information and Science, 2017 25(1), http://www.austlii.edu.au/au/journals/JILawInfoSci/2017/1.html

[34] Hondius, o.c. (przypis 7 powyżej), str. 104 z nawiązaniem do wcześniejszych ustaw podanych w tekście.

[35] Zob. przypis 23 powyżej. Więcej informacji na temat historii ochrony danych w Niemczech przedstawiono w: Herbert Burkert, o.c. (przypis 24 powyżej).

[36] W Danii wstępnie istniały dwie ustawy, jedna dla sektora prywatnego i jedna dla sektora publicznego, przyjęte tego samego dnia (ustawy nr 293 i 294 z 8 czerwca 1978 r.), przy czym obydwie w dalszym ciągu oparte były na tych samych szerokich zasadach. By zapoznać się z ogólnymi informacjami, patrz *Wprowadzenie* w: Peter Blume, Personregistrering, Kopenhaga, 1991. Pozostały one w mocy z różnymi zmianami do roku 2000, gdy wprowadzono nowe przepisy, by wdrożyć Dyrektywę WE o ochronie danych z 1995 roku.

[37] Odrębne państwowe przepisy o ochronie danych (Landesdatenschutzgesetze) obejmują państwowe sektory publiczne, ale opierają się na tych samych zasadach zakorzenionych w Konstytucji.

czasie w Stanach Zjednoczonych (chociaż praktyki te były mniej szczegółowe i nie zostały przewidziane w wiążącym prawie)[38].

Z kolei podstawowe zasady pierwszych ustaw w Europie odzwierciedlały w tej kwestii **najwcześniejsze (niewiążące) instrumenty europejskie** wydane przez Radę Europy (które z kolei stały się podstawą późniejszej i wiążącej Konwencji Rady Europy w sprawie ochrony danych).

- Uchwała Rady Europy z 1973 r. (73)22 w sprawie ochrony prywatności jednostek wobec elektronicznych banków danych w sektorze prywatnym, przyjęta przez Komitet Ministrów 26 września 1973 r.[39];
- Uchwała Rady Europy z 1974 r. (74)29 w sprawie ochrony prywatności jednostek wobec elektronicznych banków danych w sektorze publicznym, przyjęta przez Komitet Ministrów 20 września 1974 r.[40]

„Podstawowe" zasady zostały następnie uznane w **globalnych międzynarodowych, przy czym w dalszym ciągu niewiążących, instrumentach**, tj.:

- przyjętych przez OECD w 1980 roku Wytycznych w zakresie ochrony prywatności i przepływu danych osobowych przez granice[41] oraz
- wydanych w 1989 przez ONZ Wytycznych sprawie skomputeryzowanych archiwów danych osobowych, przyjętych przez Walne Zgromadzenie ONZ (UNGA).[42]

W celu zapoznania się z pełnym tekstem podstawowych zasad wynikających z wyżej wspomnianych czterech niewiążących instrumentów międzynarodowych z lat 70. i 80. XX wieku oraz amerykańskich zasad Uczciwych praktyk informacyjnych z 1973 roku, należy skorzystać z odnośników przytoczonych w przypisach.

W tym miejscu wystarczy zauważyć, że celem wszystkich zasad było rozwiązanie problemu nieodłącznie związanego z komputerami, który polega na tym, że ze względu na swój charakter komputery wprowadzają wiele nowych możliwości wykorzystania danych, w tym danych osobowych, bez zabezpieczeń oraz stosują ograniczenia stanowiące nieodłączny aspekt ich specyfiki. Innymi słowy, wszystkie podstawowe zasady mają zapobiegać nadużyciom ochrony danych osobowych, które na skutek nowych technologii stają się zbyt łatwo dostepne, chyba że zostaną odpowiednio powstrzymane. W tym sensie zasady te nie tracą na znaczeniu.

Zostało to zwięźle opisane w Wytycznych OECD.

[38] Zob.: pkt 1.3.4 poniżej.
[39] Dostępna na stronie: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680502830
[40] Dostępna na stronie: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804d1c51
[41] OECD, Rekomendacja Rady dotycząca Wytycznych w sprawie ochrony prywatności i przepływu danych osobowych przez granice, 23 września 1980 r.: https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm, w celu uzyskania informacji ogólnych, zob.z: Kirby, o.c. (przypis 33 powyżej). Należy zauważyć, że Wytyczne OECD zostały skorygowane w 2013 roku w kontekście stworzenia szerszych Ram OECD dotyczących prywatności, które także uwzględniają nowe zasady współpracy w zakresie egzekwowania przepisów o ochronie prywatności, które oparte były na wydanej w tej sprawie w 2007 roku rekomendacji, zob.: https://www.oecd.org/sti/ieconomy/privacy.htm. Nie wpływa to jednak na podstawowe zasady z lat 80. XX wieku.
[42] ONZ, Wytyczne sprawie skomputeryzowanych archiwów danych osobowych, rezolucja UNGA 44/132, 44 ONZ GAOR Supp. (nr 49), 211, dok ONZ A/44/49 (1989), https://www1.umn.edu/humanrts/instree/q2grcpd.htm. Należy zauważyć, że jest to pierwszy instrument, który uznaje potrzebę istnienia niezależnych organów ochrony danych.

Zasada ograniczenia zbierania

Powinno się ustanowić zasady zbierania danych osobowych. Wszelkie takie dane powinny być zbierane za pomocą uczciwych i rzetelnych środków oraz za wiedzą lub zgodą podmiotu danych, tam gdzie jest to właściwe.

Zasada jakości danych

Dane osobowe powinny być odpowiednie dla celu w jakim mają być użyte oraz, w stopniu niezbędnym dla realizacji tego celu, rzetelne, kompletne oraz aktualne.

Zasada określenia celu

Cele zbierania danych powinny być określone nie później niż w momencie ich zebrania, a późniejsze użycie ograniczone do realizacji tych celów lub innych zgodnych z nimi i określonych podczas każdej zmiany celu.

Zasada ograniczenia użycia

Dane osobowe nie powinny być ujawniane, udostępniane, ani używane w żaden inny sposób dla celów innych niż określone zgodnie [poprzednią zasadą], z wyjątkiem przypadków:

a) zgody podmiotu danych lub

b) działania na mocy prawa.

Zasada zabezpieczeń

Dane osobowe powinny być odpowiednio zabezpieczone przed ryzykiem w rodzaju utraty danych, nieupoważnionego dostępu, zniszczenia, użycia, modyfikacji lub ujawnienia danych.

Zasada jawności

Powinna istnieć ogólna zasada jawności ustaleń, praktyk i polityk dotyczących danych osobowych. Dostępne powinny być sposoby ustalania istnienia i istoty danych osobowych, jak również głównego celu ich użycia oraz tożsamości i siedziby administratora danych.

Zasada udziału jednostki

Jednostka powinna mieć prawo:

a) do otrzymania od administratora danych lub z innego źródła, potwierdzenia o posiadaniu lub nieposiadaniu przez administratora dotyczących jej danych;

b) do otrzymania dotyczących jej danych w rozsądnym terminie, bezpłatnie lub za umiarkowaną opłatą, w odpowiedni sposób oraz w formie dla niej zrozumiałej;

c) do uzyskania informacji o powodach odmowy realizacji żądania wynikającego z punktów (a) i (b) oraz mieć możliwość zakwestionowania takiej odmowy i

d) do zakwestionowania danych odnoszących się do niej, a w wypadku uznania jej racji, mieć prawo do usunięcia, korekty, uzupełnienia lub poprawienia danych.

Zasada rozliczalności

Administrator danych powinien być odpowiedzialny za przestrzeganie reguł wprowadzających w życie powyższe zasady.

Należy podkreślić, że zasady te (we wszystkich instrumentach) należy zawsze czytać i stosować łącznie, ponieważ tylko w ten sposób mogą zapewnić poważną ochronę przed niewłaściwym użyciem lub nadużyciem danych osobowych, takim jak błędy w zdygitalizowanych lub przechowywanych danych, gromadzenie większej liczby danych, niż jest to konieczne, lub przechowywanie ich przez okres dłuższy, niż jest to konieczne, wykorzystywanie danych w innych celach, kradzież lub ujawnianie danych innym w nielegalnych celach, utrata danych, hakerstwo, itp.

1.2.3 Konwencja Rady Europy o ochronie danych z 1981 r. i jej Protokół dodatkowy

Pierwszym wiążącym instrumentem międzynarodowym w obszarze ochrony danych była przyjęta w 1981 roku przez Radę Europy Konwencja o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, znana lepiej jako Konwencja o ochronie danych lub „Konwencja nr 108", zgodnie z jej numerem w serii traktatów europejskich[43]. Jako konwencja Rady Europy (a nie „konwencja europejska"), Konwencja o ochronie danych może być ratyfikowana - w oparciu o zaproszenie - także przez państwa niebędące członkami Rady Europy (art. 23). Do tej pory (sierpień 2018) Konwencja została ratyfikowana przez wszystkie 47 państw członkowskich Rady Europy oraz przez sześć krajów spoza Europy (Urugwaj [2013], Mauritius [2016], Senegal [2016], Tunezja [2017], Republika Zielonego Przylądka i Meksyk [2018])[44]. Dwa kolejne kraje nieeuropejskie zaproszono do przystąpienia do Konwencji: Argentynę i Burkina Faso[45]. W 2001 roku Konwencja została uzupełniona o Protokół dodatkowy[46].

Konwencja z 1981 roku oraz Protokół dodatkowy w skrócie opisano poniżej w czasie przeszłym, ponieważ niedawno w 2018 roku dokumenty te zostały fundamentalnie zmienione („zmodernizowane") w kolejnym protokole, który omówiono w pkt. 1.3. Należy jednak podkreślić, że skorygowana („zmodernizowana") Konwencja będzie miała zastosowanie wyłącznie do tych państw, które do niej przystąpiły. W przypadku pozostałych państw w mocy pozostaje tekst z 1981 roku (czytany łącznie z obowiązującą wersją Protokołu dodatkowego z 2001 roku).

Jako wiążący instrument międzynarodowy, Konwencja z 1981 roku (w przeciwieństwie do wcześniejszych niewiążących instrumentów) musiała uwzględniać i zazwyczaj uwzględniała bardziej precyzyjne **definicje** prawne głównych koncepcji zawartych w prawie ochrony danych, tj. „**danych osobowych**", „**administratora**" i „**przetwarzania**" (chociaż w późniejszych wiążących instrumentach musiały one zostać i zostały poszerzone i uzupełnione) (art. 2).

Główne, wyżej omówione, zasady ochrony danych - **zasada ograniczenia zbierania, zasada jakości danych, zasada określenia celu** i **Zasada ograniczenia użycia** - zostały określone w art. 5 Konwencji z 1981 roku (bez stosowania tych terminów - Konwencja wymienia te zasady łącznie pod nagłówkiem „Jakość danych"). **Zasada bezpieczeństwa danych** (zwana w Konwencji *Zasadą zabezpieczeń*) została wymieniona w art. 7, a **zasady jawności i zasada udziału jednostki** zostały określone w art. 8 (pod nagłówkiem „*Dodatkowe prawa osób, których dane dotyczą*")[47].

Konwencja dodała do tego specjalny artykuł o przetwarzaniu „**szczególnych kategorii danych"**, tj. „*danych osobowych ujawniających pochodzenie rasowe, poglądy polityczne, przekonania religijne lub inne, jak również danych osobowych dotyczących stanu zdrowia lub życia seksualnego"* oraz „*danych dotyczących skazujących wyroków karnych"* (art. 6). Artykuł ten przewiduje, że dane takie, powszechnie zwane „**wrażliwymi danymi**", „*nie mogą być przetwarzane automatycznie, chyba że prawo wewnętrzne zawiera odpowiednie gwarancje ochrony*".

UWAGA: potrzeba szczególnych zasad w odniesieniu do pewnych rodzajów danych była w tym czasie przedmiotem gorącej debaty. Niektórzy, w tym Simitis, uważali, że wszystkie dane mogą być wrażliwe, w zależności od kontekstu, podczas gdy niektóre z wymienionych danych mogą być w innym kontekście nieszkodliwe. Inni uważali, że tylko wrażliwe dane wymagają regulacji, ponieważ są z założenia niebezpieczne i mogą prowadzić do dyskryminacji. W końcu przeważyła propozycja złożona przez Louisa Joineta, francuskiego przedstawiciela i przewodniczącego Komitetu Rady Europy ds. opracowania

[43] Pełny tytuł: Rada Europy, Konwencja o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, otwarta da podpisu w Strasburgu 28 stycznia 1981 r. CETS nr 108, zob. link: http://prawo.sejm.gov.pl/isap.nsf/download.xsp/WDU20030030025/O/D20030025.pdf

[44] Zob.:https://www.coe.int/en/web/conventions/search-on-treaties/-/conventions/treaty/108/signatures?p_auth=qsJbzlEi

[45] *Idem*.

[46] Pełny tytuł: Rada Europy, Protokół dodatkowy do Konwencji o Ochronie Osób w związku z automatycznym przetwarzaniem danych osobowych dotyczący organów nadzorczych i transgranicznych przepływów danych, otwarty do podpisu w Strasburgu 8 listopada 2001 r. CETS nr 181, https://giodo.gov.pl/371/id_art/778/j/pl?fg. Protokół dodatkowy został ratyfikowany przez 36 z 47 państw członkowskich Rady Europy oraz przez sześć państw niebędących członkami (Republikę Zielonego Przylądka, Mauritius, Meksyk, Senegal, Tunezję i Urugwaj). Do przystąpienia zaproszono Burkina Faso. Zob.: https://www.coe.int/en/web/conventions/search-on-treaties/-/conventions/treaty/181/signatures?p_auth=yDDCP83k

[47] Ponieważ stosowanie podstawowych zasad stanowi główne zabezpieczenie jednostek: prawa osób, których dane dotyczą, uzupełniają te zasady, gdyż w indywidualnych przypadkach pozwalają na większą kontrolę ze strony jednostki.

projektu[48], i uregulowano wszystkie dane osobowe, z uwzględnieniem wyższego poziomu ochrony dla wrażliwych danych.

Jednocześnie Konwencja pozwalała państwom, które ją przyjęły, zastosować **wyjątki i ograniczenia** co do większości wymogów Konwencji (jednak nie do wymogów dotyczących bezpieczeństwa danych) dla „***ochrony państwa, interesów finansowych państwa lub dla utrzymania porządku i bezpieczeństwa publicznego oraz zwalczania przestępczości***" lub „***ochrony osoby, której dane dotyczą, albo praw lub wolności innych osób"***, pod warunkiem że odstąpienie takie „jest dopuszczalne, jeżeli przewiduje to prawo wewnętrzne strony" „jako środek ***konieczny*** [*i* ***proporcjonalny***] w społeczeństwie demokratycznym" , by chronić te interesy (art. 9(2))[49].

Poza nadaniem mocy prawnej podstawowym zasadom ochrony danych (z uwzględnieniem szczególnych zasad dotyczących wrażliwych danych) oraz prawom osób, których dane dotyczą, Konwencja z 1981 roku potwierdziła także dwa z innych wyżej wspomnianych europejskich **wymogów regulacyjnych:**

- Zobowiązała strony Konwencji do stosowania jej postanowień w **wiążących zasadach prawnych.** Mogły one przyjąć formę ustawy, rozporządzeń lub postanowień administracyjnych oraz mogły zostać uzupełnione niewiążącymi wytycznymi lub kodeksami, ale same główne zasady musiały mieć formę „wiążących środków"[50].
- Zobowiązała strony Konwencji do stosowania swoich przepisów w szerokim ujęciu **do (wszystkich) „zautomatyzowanych zbiorów danych osobowych, jak i automatycznego przetwarzania danych osobowych w sektorze publicznym i prywatnym"** (art. 3 ust. 1)). Innymi słowy, przynajmniej co do zasady, zobowiązała do przyjęcia **przepisów „zbiorczych"[51].**

Jednak Konwencja z 1981 roku nie wymagała jeszcze od stron ustanowienia niezależnego **organu ochrony danych.** Nie poruszała jeszcze także kwestii, która wkrótce stała się istotna w świetle coraz większego transgranicznego przepływu danych, tj. **potrzeby ograniczenia przepływu danych przez granicę,** by zapobiec obchodzeniu prawa materialnego i negowaniu zasadniczych praw osoby, której dane dotyczą, poprzez nakładanie zasad mających zapewnić, że ochrona będzie przestrzegana także po opuszczeniu przez dane terytorium państwa posiadającego odpowiednie przepisy o ochronie danych.

Konwencja z 1981 roku przewidywała raczej jedynie, że państwa będące stronami Konwencji:

> nie będą, uzasadniając to wyłącznie ochroną prywatności, zabraniać przepływu danych osobowych przez granice na terytorium innej strony lub uzależniać tego przepływu od wydania specjalnego zezwolenia (art. 12(2)) –
>
> chyba że ich ustawodawstwo przewiduje ostrzejsze zasady dla odpowiednich kategorii danych osobowych lub przepływ do drugiej strony odbywa się z zamiarem obejścia prawa w pierwszym z państw (art. 12(3)).

Innymi słowy, Konwencja z 1981 roku nie zajmowała się kwestią przepływu danych osobowych do państw niebędących jej stroną.

W końcu można zauważyć, że Konwencja miała zastosowanie wyłącznie do „zautomatyzowanych zbiorów danych osobowych oraz automatycznego przetwarzania danych osobowych" (art. 3 ust. 1, zob. także art. 1). Innymi słowy, **ręcznie prowadzone zbiory danych,** w tym „ręcznie uporządkowane zbiory

[48] Louis Joinet był do czasu przejścia na emeryturę starszym sędzią francuskim oraz członkiem doraźnej komisji ds. opracowania projektu francuskiej ustawy o ochronie danych z 1978 roku, zanim został pierwszym dyrektorem francuskiego organu ochrony danych (CNIL). Został wysoce zasłużonym francuskim przedstawicielem w Komitecie ONZ ds. Praw Człowieka, odpowiadającym za opracowanie Wytycznych ONZ (przypis 42 powyżej). Zob.: https://fr.wikipedia.org/wiki/Louis_Joinet; http://www.liberation.fr/societe/2013/12/18/louis-joinet-le-hessel-de-la-justice_967496

[49] Zgodnie z prawem Europejskiego Trybunału Praw Człowieka (ETPC) wymóg proporcjonalności stanowi element wyraźnie sformułowanego wymogu konieczności (w społeczeństwie demokratycznym), podczas gdy w prawie UE - w szczególności w Karcie Praw Podstawowych UE - te dwie koncepcje traktowane są jako osobne (chociaż w dalszym ciągu blisko powiązane) zasady. Zob.: art. 52 Karty Praw Podstawowych.

[50] Uzasadnienie do Konwencji Rady Europy, o.c. (przypis 19 powyżej), par. 39.

[51] Podlega to postanowieniu, że państwo będące stroną Konwencji może oświadczyć, że „nie będzie stosować niniejszej konwencji do niektórych kategorii zautomatyzowanych zbiorów danych osobowych" (art. 3 ust. 2 pkt a).

danych", nie były jeszcze przedmiotem jej przepisów (chociaż państwa będące stronami Konwencji mogły poszerzyć jej stosowanie o tego typu zbiory danych, art. 3 ust. 2 pkt c).

Dwa z wymienionych braków skorygowano w Protokole dodatkowym dotyczącym organów nadzorczych i transgranicznych przepływów danych[52], który, jak wskazuje tytuł, wymaga ustanowienia **niezależnych organów ochrony danych uprawnionych do prowadzenia dochodzenia oraz podejmowania interwencji, a także do wszczynania postępowań prawnych** (art. 1) oraz nałożenia **stosowanego z zasady zakazu przekazywania danych osobowych do kraju, który nie zapewnia „odpowiedniego poziomu ochrony"** (art. 2). Protokół dodatkowy został przyjęty przede wszystkim, by zbliżyć przepisy Konwencji do przepisów wynikających z ówcześnie obowiązującej Dyrektywy WE o ochronie danych z 1995 roku, którą omówiono w pkt. 1.3 poniżej.

Całkiem niedawno, w maju 2018 roku, Konwencja z 1981 roku została dodatkowo „**zmodernizowana**", by uzgodnić ją z najnowszym prawem UE o ochronie danych oraz ogólnymi (globalnymi) zmianami w obszarze ochrony danych, co omówiono bardziej szczegółowo w pkt. 1.4.3.

W ramach Rady Europy kwestiami ochrony danych dodatkowo zajmuje się szereg organów, w tym Zgromadzenie Parlamentarne Rady Europy (PACE), Komitet Konsultacyjny, znany jako „T-PD", ustanowiony na mocy Konwencji nr 108, którego głównym zadaniem jest codzienne monitorowanie zmian dotyczących ochrony danych oraz opracowywanie projektów wytycznych i zaleceń sektorowych oraz innych w tym obszarze, a także Komitet Ministrów Rady Europy (COM lub CM), który następnie przyjmuje w szczególności tego typu propozycje. Organy te wydały pomiędzy sobą wiele opinii, rekomendacji i badań, za każdym razem w nawiązaniu do Konwencji[53].

Ponadto istnieje wzajemna zależność pomiędzy Konwencją o ochronie danych a Europejską Konwencją Praw Człowieka, a Europejski Trybunał Praw Człowieka coraz częściej wskazuje na Konwencję o ochronie danych i wyżej wspomniane typy dokumentów w swojej własnej interpretacji art. 8 Konwencji Praw Człowieka (który gwarantuje prawo do życia prywatnego), podczas gdy PACE, Komitet Konsultacyjny i Komitet Ministrów opierają się w swojej pracy w tym obszarze na orzecznictwie Trybunału[54].

1.3 Europejskie prawo o ochronie danych w latach 90. XX wieku i w pierwszych latach XXI wieku

1.3.1 Ochrona danych we Wspólnocie Europejskiej

Informacje ogólne

Przez pewien czas Wspólnota Europejska (ówczesna nazwa Unii Europejskiej) uważała[55], że Konwencja Rady Europy o ochronie danych z 1981 roku zapewniała w tym obszarze wystarczającą ochronę. Jednak pod koniec dekady stało się jasne, że Konwencja nie doprowadziła do szerokiej lub szeroko zharmonizowanej ochrony danych osobowych we Wspólnocie, gdyż do września 1990 roku została ratyfikowana przez zaledwie siedem państw członkowskich WE (z czego jedno faktycznie jeszcze nie przyjęło odpowiednich przepisów), a prawo tych państwach członkowskich różniło się znacząco w

[52] Zob.: przypis 46 powyżej.

[53] Patrz: http://website-pace.net/en_GB/web/apce/documents (dokumenty PACE). Należy zauważyć, że dokumenty te mogą obejmować znacznie więcej kwestii niż ochrona danych, ale można je wyszukać pod hasłem „ochrona danych". https://www.coe.int/t/dghl/standardsetting/dataprotection/Documents_TPD_en.asp (dokumenty T-PD); https://www.coe.int/t/dghl/standardsetting/dataprotection/legal_instruments_en.asp (dokumenty COM dotyczące ochrony danych).

[54] Zob.: Rada Europy Factsheet – personal data protection (przypis 13, powyżej) i *Annex 1 – Jurisprudence* do dokumentu roboczego sporządzonego przez Grupę Roboczą UE ds. Art. 29, Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees) (WP237), przyjęty 13 kwietnia 2016 r., który wymienia 15 istotnych wyroków Trybunału dotyczących ochrony danych (i pięć wyroków Trybunału Sprawiedliwości UE), http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp237_en.pdf

[55] W momencie wprowadzenia pakietu omówionych w tym punkcie propozycji Komisji (wrzesień 1990) Komisja w dalszym ciągu była „Komisją Wspólnot Europejskich" (liczba mnoga). Zwrot „Wspólnota Europejska" (liczba pojedyncza) zaczął być stosowany dopiero w 1992 roku na podstawie Traktatu z Maastricht do czasu wejścia w życie Traktatu Lizbońskiego w 2009 roku. Jednak dla uproszczenia będziemy w tym punkcie nawiązywać ogólnie do Wspólnoty Europejskiej, a w kolejnym punkcie 1.4 oraz w części drugiej i trzeciej do Unii Europejskiej.

istotnych aspektach[56]. W tym czasie jedynie Włochy posiadały ustawę o ochronie danych w odniesieniu do pracowników, Hiszpania nie posiadała zbiorczego prawa, mimo że ochrona danych w jej konstytucji stanowiła jedno z fundamentalnych praw, itd.

Taka różnorodność wpasowała się ówczesne założenie Wspólnoty Europejskiej, by zharmonizować wszystkie rodzaje zasad i przepisów w celu uproszczenia procesu otwierania rynku wewnętrznego, który miał zapewniać swobodny przepływ towarów, usług, kapitału i osób. A konkretnie, w trakcie międzynarodowej konferencji organów ochrony danych, która miała miejsce w 1989 roku w Berlinie zgromadzeni przedstawiciele zostali poinformowani przez Komisję Europejską o konieczności harmonizacji zasad dla sektora telekomunikacyjnego. Pokazało to, że posiadanie właściwie stosowanych i silnych przepisów o ochronie danych we wszystkich państwach członkowskich nabrało istotnego znaczenia[57].

W efekcie, w odpowiedzi na apel europejskich organów ochrony danych we wrześniu 1990 roku Komisja Europejska przedstawiła ambitny zestaw propozycji mający na celu zabezpieczenie danych osobowych w całym pierwszym filarze WE[58]. Pakiet ten obejmował propozycje dwóch dyrektyw pierwszego filaru, tj.[59]:

---

[56] Komisja Wspólnot Europejskich, Komunikat w sprawie ochrony jednostek w związku z przetwarzaniem danych osobowych we Wspólnocie oraz w sprawie bezpieczeństwa informacyjnego, COM(90) 314 final – SYN287 i 288, Bruksela, 13 września 1990 r. *Wprowadzenie*. Cały dokument jest dostępny w internecie w doskonałych archiwach Centrum Własności Intelektualnej i Prawa Informacyjnego Uniwersytetu w Cambridge na stronie https://resources.law.cam.ac.uk/cipil/travaux/data_protection/3%2013%20September%201990%20Communication.pdf. Zob. w szczególności par. 6 – 8.

[57] Na konferencji w Berlinie Spiros Simitis, Komisarz ds. Ochrony Danych w niemieckim landzie Hessen (oraz inicjator pierwszej na świecie ustawy o ochronie danych w tym państwie), publicznie wezwał Jacquesa Fauveta, ówczesnego przewodniczącego francuskiego organu ochrony danych - CNIL (oraz wcześniej dyrektora gazety „Le Monde"), by napisał do swojego wieloletniego przyjaciela Jacquesa Delorsa, ówczesnego Prezesa Komisji Europejskiej, by ten podjął inicjatywę harmonizacji przepisów o ochronie danych we WE.

[58] Traktat o Unii Europejskiej, podpisany w Maastricht 7 lutego 1992 r. („Traktat z Maastricht"), przewidywał strukturę trzech filarów pod jednym frontonem. Pierwszy filar składał się z pierwotnej Europejskiej Wspólnoty Gospodarczej (EWG), Europejskiej Wspólnoty Węgla i Stali (EWWiS) i Europejskiej Wspólnoty Energii Atomowej (EWEA) (chociaż każdy z nich zachował osobowość prawną), a następnie obejmował utworzony jednolity rynek w 1993 r. Drugi i trzeci filar obejmowały odpowiednio wspólną politykę zagraniczną i bezpieczeństwa (WPZiB) oraz współpracę w dziedzinie wymiaru sprawiedliwości i spraw wewnętrznych (WSiSW). Filary zostały formalnie zniesione na mocy traktatu lizbońskiego, ale nadal istnieją odrębne instrumenty dla poszczególnych obszarów (por. Omówienie zakresu RODO w części drugiej, sekcja 2.3 poniżej). Patrz: strona internetowa ośrodka badawczego CVCE Uniwersytetu Luksemburga na temat wydarzeń historycznych w procesie integracji europejskiej (1945–2014), w szczególności strona „Pierwszy filar Unii Europejskiej": https://www.cvce.eu/en/education/unit-content/-/unit/02bb76df-d066-4c08-a58a-d4686a3e68ff/4ee15c10-5bdf-43b1-9b5f-2553d5a41274. Dyrektywa w sprawie ochrony danych z 1995 r. oraz inne dyrektywy omówione w niniejszym punkcie zostały wydane w czasie, gdy pierwszy filar nadal obowiązywał i zostały wydane tylko odnośnie tego filaru. Środki ochrony danych w pozostałych dwóch filarach zostały krótko omówione w podrozdziałach 1.3.4 i 1.3.5 poniżej, a zasady ochrony danych dla samych instytucji UE zostały pokrótce omówione w podrozdziale 1.3.6.

[59] Komisja Wspólnot Europejskich, Komunikat w sprawie ochrony jednostek w związku z przetwarzaniem danych osobowych we Wspólnocie oraz w sprawie bezpieczeństwa informacyjnego (przypis 56 powyżej). Pakiet ten obejmował cztery dodatkowe propozycje, tj.:

- projekt **uchwały** przedstawicieli państw członkowskich, która poszerzałaby stosowanie zasad zawartych w ogólnej dyrektywie do zbiorów danych prowadzonych przez organy publiczne, do których główna Dyrektywa o ochronie danych nie miałaby jako tako zastosowania; uchwały tej nigdy nie przyjęto, ale można ją uznać za genezę zasad ochrony danych dotyczących egzekwowania prawa i spraw sądowych, które niedawno zgromadzono w Dyrektywie w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy ścigania (Dyrektywa UE 2016/680 (nieomawiana w niniejszym Podręczniku, zob. uwaga w polu „O Podręczniku" na str. 1);
- projekt **deklaracji** Komisji w sprawie stosowania standardów ochrony danych ustalonych w głównej Dyrektywie o ochronie danych w stosunku do zbiorów danych prowadzonych przez instytucje Komisji, która ostatecznie doprowadziła do przyjęcia Rozporządzenia (WE) 45/2001 (*idem*);
- **rekomendacja w sprawie decyzji Rady** dotycząca przystąpienia Wspólnoty Europejskiej do Konwencji Rady Europy o ochronie danych, co do dzisiaj nie miało miejsca, ponieważ UE, która nie jest państwem członkowskim, nie może przystąpić do Konwencji; naprawiono to jednak w „zmodernizowanej" Konwencji Rady Europy o ochronie danych, która zostanie omówiona poniżej w pkt. 1.4.3,
- **propozycja decyzji Rady** w sprawie przyjęcia planu działania dotyczącego bezpieczeństwa informacyjnego, która doprowadziła do podjęcia szerokich działań w tym obszarze przez UE, z uwzględnieniem ustanowienia w 2004 roku Europejskiej Agencji Bezpieczeństwa Sieci i Informacji (ENISA) oraz przyjęcia kompleksowej strategii bezpieczeństwa cybernetycznego i informacji, które nie są przedmiotem niniejszego Podręcznika, ale informacje na temat których można znaleźć tutaj:

- **ogólnej dyrektywy WE** „*dotyczącej ochrony jednostek w związku z przetwarzaniem danych osobowych*", która po długim procesie legislacyjnym została główną Dyrektywą WE o ochronie danych, Dyrektywa 95/46/WE, omówiona poniżej w pkt. 1.3.2 oraz
- dodatkowo zaproponowanej **zależnej dyrektywy WE** „*dotyczącej ochrony danych osobowych w kontekście publicznych cyfrowych sieci telekomunikacyjnych, w szczególności cyfrowej sieci usług zintegrowanych (ISDN) oraz publicznych cyfrowych sieci komórkowych"*, która stała się Dyrektywa o ochronie danych telekomunikacyjnych, Dyrektywa 97/66/WE przyjęta w grudniu 1997 roku, następnie zastąpiona Dyrektywą 2002/58/WE, zwaną Dyrektywą o e-prywatności, którą omówiono poniżej w pkt. 1.3.3.

Zanim przystąpimy do omówienia tych dwóch dyrektyw, należy zapoznać się z ich charakterem i nieodłącznymi ograniczeniami.

Charakter i ograniczenia dyrektyw WE

Omawiając główne instrumenty UE dotyczące ochrony danych, w tym w szczególności dwie wyżej wymienione dyrektywy, należy pamiętać o trzech sprawach. Po pierwsze, każdy instrument prawny UE (lub wcześniej WE) z założenia ogranicza się do spraw mieszczących się w zakresie prawa UE (wcześniej WE). Niektóre sprawy, głównie działania państw członkowskich w odniesieniu do **bezpieczeństwa narodowego**, (prawie) w całości mieszczą się poza zakresem prawa UE (wcześniej WE), [60] przez co nie ma do nich zastosowania żaden z instrumentów prawnych UE (lub WE) (z uwzględnieniem powyższych dyrektyw lub RODO albo jakichkolwiek przyszłych zasad unijnych dotyczących ochrony danych, bez względu na ich formę). Zostało to wyraźnie potwierdzone w dyrektywach (i RODO): patrz art. 3(2) Dyrektywy o ochronie danych z 1995 roku oraz art. 1(3) Dyrektywy o e-prywatności (i art. 2(2)(a) RODO)[61].

Po drugie, niżej omówione dyrektywy WE ograniczały się - jako dyrektywy WE - do spraw w ramach tzw. **pierwszego filaru**[62] i ze względu na swój charakter dyrektyw WE nie miały zastosowania do czynności w ramach drugiego i trzeciego filaru, dla których sporządzono osobne instrumenty o ochronie danych, które zostały krótko omówione w sekcjach 1.3.4 i 1.3.5, a które nie zostały szczegółowo wyjaśnione w pierwszym wydaniu Podręcznika. Wystarczy wspomnieć, że *przekazywanie lub udostępnianie danych osobowych* przez podmioty podlegające dyrektywom (w tym zarówno podmioty sektora prywatnego, jak i organy państwowe działające zgodnie z prawem pierwszego filara (WE)) organom ścigania lub krajowym agencjom bezpieczeństwa było (a w przypadku Dyrektywy o e-prywatności w dalszym ciągu jest) przedmiotem tych instrumentów (ponieważ tego typu ujawnienie stanowiło w rozumieniu tych dyrektyw „przetwarzanie" przez te podmioty), nawet jeżeli *uzyskanie (otrzymanie) i dalsze przetwarzanie* ujawnionych danych było albo przedmiotem innych instrumentów (w tym, w szczególności w odniesieniu do egzekwowania prawa, do niedawna Decyzji ramowej Rady 2008/977/JHA i obecnie Dyrektywy z 2016 roku o ochronie danych osobowych przez organy ścigania), albo nie było przedmiotem prawa unijnego (lub prawa WE) w ogóle (tj. gdy zajmowały się tym krajowe

---

https://europa.eu/european-union/about-eu/agencies/enisa_pl
ec.europa.eu/geninfo/query/index.do?QueryText=bezpieczeństwo+cybernetyczne&op=Wyszukiwanie&swlang=pl&form_build_id=form-63nwYS2o-jarlv1KZmEMs0vwCzrcJGTf38woUjV5lkE&form_id=nexteuropa_europa_search_search_form
W celu zapoznania się z odrębnymi propozycjami wymienionymi w Komunikacie Komisji (oraz dodatkowymi dokumentami dotyczącymi procesu legislacyjnego), skorzystaj z linków na stronie: https://www.cipil.law.cam.ac.uk/projectseuropean-travaux/data-protection-directive

[60] Używamy zwrotu „(prawie) w całości" z dwóch powodów. Przede wszystkim coraz trudniej jest - w szczególności w odniesieniu do terroryzmu (który sam stanowi raczej źle zdefiniowaną koncepcję) - rozgraniczyć działania prowadzone przez państwa w odniesieniu do ich własnego bezpieczeństwa narodowego od działań podejmowanych w ramach prawa karnego lub prawa dotyczącego ochrony „bezpieczeństwa międzynarodowego", „bezpieczeństwa publicznego" lub „porządku publicznego", a wszystkie te aspekty bezpieczeństwa podlegają obecnie w większym lub mniejszym stopniu co najmniej częściowo prawu UE. Po drugie, nawet jeżeli działania podejmowane przez agencje państw członkowskich odpowiedzialne za bezpieczeństwo narodowe nie mieszczą się w zakresie prawa UE, blisko powiązane działania organów ścigania i prywatnych podmiotów (np. gromadzenie i ujawnianie danych przez banki w ramach przepisów o praniu brudnych pieniędzy lub gromadzenie i ujawnianie rejestrów pasażerów przez linie lotnicze agencjom państw członkowskich) często są przedmiotem prawa UE (w szczególności unijnego prawa o ochronie danych). Zob. drugi punkt w tekście.

[61] W celu uzyskania informacji na temat ograniczeń dotyczących zakresu unijnego Ogólnego rozporządzenia o ochronie danych, zob. Część druga, pkt 2.3, *Kluczowe elementy RODO*, w szczególności pkt 2.3.1, Postanowienia ogólne.

[62] Zob. przypis 67 poniżej.

agencje bezpieczeństwa)[63].

Po trzecie, dyrektywa z definicji nie ma zastosowania bezpośrednio w porządkach prawnych państw członkowskich: nie ma „bezpośredniej skuteczności". Jej postanowienia państwa członkowskie muszą raczej „**przetransponować**" na swoje prawo krajowe, a w tym zakresie często miały (i w dalszym ciągu mają) znaczną **swobodę** działania. Na pewno było tak w przypadku dwóch niżej omówionych dyrektyw, co, jak wspomniano w części drugiej, doprowadziło do znacznych rozbieżności pomiędzy przepisami krajowymi państw członkowskich wdrażającymi („transponującymi") postanowienia dyrektyw. Była to faktycznie jedna z podstawowych przyczyn wyboru formy (bezpośrednio obowiązującego) rozporządzenia RODO, jako następcy Dyrektywy o ochronie danych z 1995 roku (nawet mimo to, że, jak zobaczymy w tej części, Rozporządzenie to w dalszym ciągu pozwala na różne wdrożenie w wielu aspektach)[64].

1.3.2 Główna Dyrektywa WE o ochronie danych z 1995 roku

Informacje ogólne

Jak zauważono powyżej, na początku lat 90. XX wieku Komisja Wspólnot Europejskich (taka była jej ówczesna nazwa)[65] stanęła przed dylematem. Z jednej strony ochrona danych była coraz częściej uznawana w UE jako konstytucyjnie chronione prawo i wymagała ograniczeń co do wykorzystania i przepływu danych osobowych[66]. Z drugiej strony, rozwój **rynku wewnętrznego,** w ramach tak zwanego „pierwszego filara" Wspólnoty[67], wymagał swobodnego przepływu związanych z transakcjami handlowymi danych, w tym danych osobowych. Aby uzyskać kwadraturę koła, Komisja zaproponowała przyjęcie dla pierwszego filaru dwóch dyrektyw. W tym punkcie omówimy główną dyrektywę, tj. Dyrektywę 95/46/WE[68].

Cel i przedmiot Dyrektywy o ochronie danych z 1995 roku:

Biorąc pod uwagę powyższe dylematy, Wspólnota Europejska nadała dyrektywie dwa powiązane cele,

---

[63] W celu uzyskania informacji na temat podobnych spraw poruszonych w związku z unijnym Ogólnym rozporządzeniem o ochronie danych, patrz: Część druga, w szczególności pkt 2.2 *Status i podejście RODO: harmonizacja ze specyfikacjami na poziomie krajowym.*

[64] Zob.: Część druga, w szczególności pkt 2.2 *Status i podejście RODO: elastyczna harmonizacja.*

[65] Zob. przypis 67 poniżej.

[66] Ochrona danych jest obecnie wyraźnie uznawana jako prawo *sui generis* w art. 8 Karty Praw Podstawowych UE (CFR), niezależne od prawa (chociaż oczywiście w powiązaniu z prawem) do życia prywatnego i rodzinnego oraz prywatności, które chronione jest art. 7. CFR została ogłoszona zaledwie w 2000 roku, ale nie zyskała pełnej skuteczności prawnej do czasu wejścia w życie Traktatu z Lizbony w dniu 1 grudnia 2009 roku. Zob. link: https://pl.wikipedia.org/wiki/Karta_praw_podstawowych_Unii_Europejskiej. Innymi słowy, gdy przedłożono propozycje dyrektyw, Karta nie miała jeszcze pełnej mocy prawnej. Jednak nawet przed sporządzeniem Karty lub nadaniem jej mocy prawnej prawa podstawowe uzyskały już we Wspólnotach Europejskich status quasi konstytucyjny, patrz: Francesca Ferraro i Jesús Carmona, Fundamental Rights in the European Union – The role of the Charter after the Lisbon Treaty, European Parliament Research Service, Bruksela, marzec 2015, ust. 2*: EU Fundamental rights prior to the Lisbon Treaty*, http://www.europarl.europa.eu/RegData/etudes/IDAN/2015/554168/EPRS_IDA(2015)554168_EN.pdf. W związku z powyższym projekty Dyrektywy o ochronie danych z 1995 roku w dalszym ciągu prawidłowo umieszczały ochronę danych osobowych jako podstawowe prawo i fundament proponowanego instrumentu.

[67] Traktat o Unii Europejskiej podpisany w Maastricht 7 lutego 1992 roku („Traktat z Maastricht") zakładał strukturę opartą na trzech filarach w ramach jednego frontonu. Pierwszy filar obejmował pierwotną Europejską Wspólnotę Gospodarczą (EWG), Europejską Wspólnotę Węgla i Stali (EWWS) oraz Europejską Wspólnotę Energii Atomowej (EWEA) (chociaż każda z nich zachowała swoją własną osobowość prawną). Drugi i trzeci filar obejmowały odpowiednio wspólną politykę zagraniczną i bezpieczeństwa oraz współpracę w obszarach sprawiedliwości i spraw wewnętrznych. Filary zostały formalnie zniesione na mocy Traktatu Lizbońskiego, ale w dalszym ciągu wydawane są osobne instrumenty dla różnych obszarów (patrz: dyskusja na temat zakresu RODO w części drugiej, pkt 2.3). Patrz: strona internetowa ośrodka badawczego University of Luxembourg, Historical events in the European integration process (1945 – 2014), w szczególności strona „*The first pillar of the European Union*: https://www.cvce.eu/en/education/unit-content/-/unit/02bb76df-d066-4c08-a58a-d4686a3e68ff/4ee15c10-5bdf-43b1-9b5f-2553d5a41274. Zobacz także wpis w Wikipedii na temat Trzech filarów Unii Europejskiej, dostępny pod adresem: https://en.wikipedia.org/wiki/Three_pillars_of_the_European_Union (Z bardzo przydatną osią czasu ilustrującą rozwój traktatów). Dyrektywa o ochronie danych z 1995 roku (oraz pozostałe dyrektywy omówione w tym punkcie) została wydana w momencie, gdy pierwszy filar jeszcze istniał, i została wydana wyłącznie dla tego filara.

[68] Pełny tytuł: Dyrektywa Parlamentu Europejskiego i Rady 95/46/WE z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych, OJ L 281 z 23.11.1995, str. 31-50, https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:31995L0046&from=pl.

tj. zapewnienie **wysokiego poziomu ochrony danych** w całym ówczesnym „pierwszym filarze" Wspólnoty („wysoki poziom", gdyż dyrektywa miała chronić prawa człowieka), jako warunek *sine qua non* dla **swobodnego przepływu danych osobowych** w ramach głównego elementu tego filaru, tj. wschodzącego w tym czasie **rynku wewnętrznego** (patrz: art. 1 Dyrektywy oraz motyw 10 i w szczególności 11).

Podstawowe elementy Dyrektywy o ochronie danych z 1995 roku:

Poniżej wymieniono **podstawowe elementy** Dyrektywy o ochronie danych z 1995 roku w porównaniu do Konwencji z 1981 roku (uwaga: nowe elementy lub elementy zawierające istotne, nowe aspekty oznaczono jako *NOWE – chociaż należy zauważyć, że często stanowią one rozszerzenie rozwiązań, które zostały już zaproponowane lub wspomniane w preambule do Konwencji. Opis kluczowych elementów Dyrektywy z 1995 roku ma stanowić przegląd części podstawowych aspektów podejścia do ochrony danych w UE, które zostało w pełni ponownie potwierdzone w Ogólnym rozporządzeniu o ochronie danych z 2016 roku i w związku z tym wyjaśnione w niniejszym Podręczniku. Natomiast zasadniczo nowe elementy wprowadzone poprzez Rozporządzenie zostaną omówione w części drugiej. Najważniejszymi innowacjami jest wymóg niezależnych organów ochrony danych oraz środki zapewniające ciągłą ochronę danych przekazywanych do krajów trzecich (tj. spoza UE/EOG).

*NOWE Definicje:

Dyrektywa rozszerzyła podstawowe **definicje** zawarte w Konwencji z 1981 roku i dodała nowe. A konkretnie, wyjaśniła (w ramach definicji „danych osobowych"), kiedy jednostki powinny być uznawane za „***możliwe do zidentyfikowania***" (przez „każdego") oraz (w osobnej definicji) kiedy ręcznie prowadzony zbiór danych należy uznać za wystarczająco „***uporządkowany***", by podlegał postanowieniom Dyrektywy. Zakresem Dyrektywy objęto „ręcznie uporządkowane zbiory danych", by uniknąć obchodzenia zasad poprzez stosowanie tego typu zbiorów.

Dyrektywa określiła ***nieco zmodyfikowaną definicję „administratora"*** oraz dodała ***obejmującą wszystkie aspekty definicję „przetwarzania danych osobowych"*** i definicje koncepcji „***przetwarzającego", „osoby trzeciej" i „odbierającego dane".*** Dodała również definicję „***zgody osoby, której dane dotyczą"***, która określa warunki, jakie należy spełnić przed uznaniem jakiejkolwiek wnioskowanej zgody za ważną - zgoda, by była ważna, musi być ***dobrowolna, konkretna i świadoma*** oraz w pewien sposób ***wyrażona*** (art. 2(h))[69].

Konwencja z 1981 roku zawierała cztery definicje, natomiast Dyrektywa osiem (lub dziewięć, jeżeli liczyć osobno definicję „możliwej do zidentyfikowania osoby" w ramach definicji „danych osobowych").

Zasady ochrony danych:

Dyrektywa w znacznym stopniu powtarzała zasady ochrony danych zawarte w Konwencji z 1981 roku, ale wprowadziła pewne wyjaśnienia, z uwzględnieniem tego, że cel przetwarzania danych osobowych musi być nie tylko „określony" i „legalny" (co już przewidywał art. 5(b) Konwencji), ale także „jednoznaczny" (art. 6(1)(b)), a także wspominała „[d]alsze przetwarzanie danych w celach historycznych, statystycznych lub naukowych" (art. 6(1)(c) i (e)).

*NOWE Podstawy prawne przetwarzania

Główną nowością w Dyrektywie z 1995 roku było to, żeby osiągnąć większą harmonizację pomiędzy przepisami państw członkowskich, określała ona w art. 7 **wyczerpującą listę „kryteriów legalności przetwarzania danych**", które później nazwano „**podstawami prawnymi**" **przetwarzania danych osobowych**. Zgodnie z Dyrektywą przetwarzanie (niewrażliwych) danych osobowych było dopuszczalne wyłącznie wtedy, gdy (w skrócie):

(a) osoba, której dane dotyczą, ***jednoznacznie*** wyraziła na to **zgodę** (która oczywiście musiała być „***dobrowolna, konkretna i świadoma****" oraz* ***wyrażona,*** art. 2(h), wspomniany powyżej) lub

[69] Zgoda taka musi mieć formę „konkretnego i świadomego, dobrowolnego **wskazania przez osobę, której dane dotyczą na to, że wyraża przyzwolenie** na przetwarzanie odnoszących się do niej danych osobowych".

(b) przetwarzanie było **konieczne** dla realizacji umowy, której stroną jest osoba, której dane dotyczą, lub w celu podjęcia działań na życzenie osoby, której dane dotyczą, przed zawarciem umowy (np. dla celów kontroli kredytowej); lub

(c) przetwarzanie jest **konieczne** do wypełnienia dla wykonania **zobowiązania prawnego**, któremu administrator danych podlega; lub

(d) przetwarzanie danych jest **konieczne** dla ochrony **żywotnych interesów osób, których dane dotyczą**; lub

(e) przetwarzanie danych jest ***konieczne*** dla realizacji **zadania wykonywanego w interesie publicznym lub dla sprawowania władzy publicznej** przekazanej administratorowi danych lub osobie trzeciej, przed którą ujawnia się dane; lub

(f) przetwarzanie danych jest ***konieczne*** dla potrzeb wynikających z **uzasadnionych interesów** administratora danych lub osoby trzeciej, lub osobom, którym dane są ujawniane, z wyjątkiem sytuacji, kiedy interesy takie podporządkowane są interesom lub podstawowym prawom i wolnościom osoby, której dane dotyczą i które gwarantują ochronę na podstawie art. 1(1). [tak zwane „uzasadnione interesy" lub kryterium „równowagi"/podstawa prawna].

Upraszczając, w większości przypadków przetwarzanie niewrażliwych danych osobowych było dopuszczalne albo na podstawie prawa, umowy lub zgody osoby, której dane dotyczą, albo na podstawie uzasadnionego interesu administratora, nad którym nie przeważały interesy lub podstawowe prawa i wolności osób, których dane dotyczą.

Konwencja o ochronie danych z 1981 roku nie zawierała tego typu wykazu.

*NOWE <u>Konkretne zasady dotyczące przetwarzania wrażliwych danych</u>

Dyrektywa z 1995 roku w znacznej mierze wymieniała takie same **główne „szczególne kategorie danych",** zazwyczaj zwanych „**wrażliwymi danymi**", jak te przewidziane w Konwencji z 1981 roku, z niewielkimi zmianami, tj.[70]:

> dane osobowe ujawniające pochodzenie rasowe lub etniczne, opinie polityczne, przekonania religijne lub *filozoficzne*, *przynależność do związków zawodowych*, jak również ... dane dotyczące zdrowia i życia seksualnego.

Jednak zamiast jedynie przewidywać, że dane takie *„nie mogą być przetwarzane automatycznie, chyba że prawo krajowe zapewnia odpowiednie zabezpieczenia*" (Konwencja Rady Europy, art. 6), Dyrektywa w art. 8(1) określiła **stosowany z zasady zakaz** przetwarzania tego typu wrażliwych danych, z zastrzeżeniem ograniczonej liczby **wyjątków**. Główne wyjątki dotyczyły **szczególnie restrykcyjnych podstaw prawnych** przetwarzania wrażliwych danych. Było to (w skrócie):

- przetwarzanie bez wyrażonej dobrowolnie, konkretnej i świadomej, ale także ***wyraźnej zgody*** osoby, której dane dotyczą, chyba że prawo krajowe w szczególnych okolicznościach zabrania przetwarzania takich danych nawet za zgodą udzieloną przez osobę, której dane dotyczą (art. 8(2)(a));
- przetwarzanie jest konieczne do wypełniania obowiązków i uprawnień administratora danych w dziedzinie prawa pracy (o ile prawo krajowe przewiduje „odpowiednie środki zabezpieczające" (art. 8(2)(b));
- przetwarzanie jest konieczne dla ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby, w przypadku gdy osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do udzielenia zgody (art. 8(2)(c));
- przetwarzanie jest „dokonywane w ramach legalnej działalności wspartej odpowiednimi gwarancjami przez fundację, stowarzyszenie lub inną instytucję nienastawioną na osiąganie zysku, której cele mają charakter polityczny, filozoficzny, religijny lub związkowy, pod warunkiem że przetwarzanie danych odnosi się wyłącznie do członków tej instytucji lub osób mających z nią regularny kontakt w związku z jej celami oraz, że dane nie zostaną ujawnione osobie trzeciej bez zgody osób, których dane dotyczą (art. 8(2)(d));

[70] Konwencja z 1981 roku nie zawierała odwołania do danych „etnicznych", nawiązywała do „wierzeń religijnych i innych" (a nie „przekonań religijnych lub filozoficznych") oraz nie wspominała przynależności do związków zawodowych.

- przetwarzanie dotyczy (wrażliwych) danych, „które są podawane do wiadomości publicznej przez osobę, której dane dotyczą" (art. 8(2)(e), pierwsza część zdania) oraz
- przetwarzanie (wrażliwych) danych osobowych jest „konieczne do ustalenia, wykonania lub ochrony roszczeń prawnych" (art. 8(2)(e), drugi fragment zdania).

W szczególności, wykaz ten nie uwzględnia kryterium „**uzasadnionego interesu**" lub „**równowagi**" - wrażliwe dane, już na podstawie Dyrektywy, nie mogłyby być *z zasady* przetwarzane, gdyby leżało to w uzasadnionym interesie administratora lub osoby trzeciej, a nad interesem takim nie przeważałyby podstawowe prawa i interesy osoby, której dane dotyczą.

Jednak Dyrektywa przewidywała także, że stosowany z zasady zakaz przetwarzania wrażliwych danych (uwaga: jakiegokolwiek rodzaju wrażliwych danych) nie ma zastosowania *„w przypadku gdy przetwarzanie danych **wymagane** jest do celów **medycyny prewencyjnej, diagnostyki medycznej**, świadczenia **opieki** lub **leczenia**, lub też **zarządzania opieką zdrowotną",*** pod warunkiem że odbywało się to zgodnie z obowiązkiem zachowania tajemnicy zawodowej (art. 8(3)). Należy zauważyć, że dotyczy to wszelkiego rodzaju wrażliwych danych, ale oczywiście dane takie mogą być w dalszym ciągu w stosownym przypadku wykorzystywane w takich celach (np. informacje o pochodzeniu etniczym mogą być konieczne przy pewnych chorobach, takich jak anemia sierpowata, a przekonania religijne osoby mogą być potrzebne przy pewnych formach leczenia, jak transfuzja krwi w przypadku Świadków Jehowy).

Ponadto, chociaż wyżej wymienione zasady były jako takie ścisłe, Dyrektywa zawierała znacznie szerszą klauzulę (art. 8(4)), która pozwalała państwom członkowskim na ustalenie **dodatkowych wyłączeń**, tj. na pozwolenie na przetwarzanie (wszelkiego rodzaju) wrażliwych danych inaczej niż w oparciu o podstawy wymienione w art. 8(2) albo na mocy prawa, albo na podstawie decyzji swoich krajowych organów nadzorczych (organ ochrony danych) „***ze względu na istotny interes publiczny***", pod warunkiem że ustanowiono ustalone przez państwo członkowskie „***odpowiednie środki zabezpieczające***".

Dyrektywa wprowadzała także nieco bardziej restrykcyjne podejście do przetwarzania **danych osobowych dotyczących wyroków skazujących** (art. 8(5)) oraz **krajowych numerów identyfikacyjnych lub innych „identyfikatorów ogólnego stosowania"** (art. 8(7)), przy czym szczegóły regulacji w sprawie tego typu przetwarzania pozostawiała państwom członkowskim.

Również, mimo większego nacisku niż w przypadku Konwencji z 1981 roku na potrzebę **zrównoważenia ochrony danych i wolności wypowiedzi i informacji**, pozostawiała konkretne metody w tym zakresie państwom członkowskim (art. 9).

*NOWE Informowanie osób, których dane dotyczą

Konwencja o ochronie danych z 1981 roku wymagała jedynie pewnej ogólnej przejrzystości w sprawie „*istnienia zautomatyzowanego zbioru danych osobowych, podstawowych celów jego utworzenia, a także tożsamości, miejsca zamieszkania lub siedziby administratora tego zbioru*" (art. 8(a)).

Z kolei art. 10 i 11 Dyrektywy o ochronie danych z 1995 roku określa bardziej szczegółowo **informacje, jakie powinny zostać przekazane przez administratora osobom, których dane dotyczą**, *z własnej inicjatywy administratora,* gdy dane osobowe zostały uzyskane od takich osób lub od osób trzecich. Szczegóły, które należy przekazać obejmowały w obydwu przypadkach ***tożsamość administratora*** oraz ***cele przetwarzania. Dalsze informacje*** (z uwzględnieniem informacji na temat tego, czy dane są obowiązkowe czy dobrowolne oraz informacji na temat ich ujawnienia) należało przekazać, o ile było to konieczne w celu zagwarantowania rzetelnego przetwarzania (patrz: art. 10(c) i 11(1)(c)).

*NOWE Prawa osób, których dane dotyczą

Konwencja o ochronie danych z 1981 roku wymagała już, by osoby, których dane dotyczą, uzyskały prawo dostępu do swoich danych na życzenie w rozsądnych odstępach czasu, prawo do sprostowania lub usunięcia danych, które były niepoprawne lub zostały przetworzone z naruszeniem zasad ochrony danych, oraz prawo do zastosowania środków prawnych, jeżeli powyższe prawa nie zostały zapewnione (art. 8(b) – (d)).

Dyrektywa potwierdziła pierwsze dwa prawa, ale dodała **istotny dodatkowy szczegół.** Potwierdziła, że

prawo dostępu obejmuje prawo do „uzyskania" danych przez osobę, której dane dotyczą, (co już przewidywała Konwencja), ale dodała, że dane takie należy przekazać w *„zrozumiałej formie"* oraz że należy także przekazać *„posiadane informacje o **źródłach** [danych]"* (art. 12(a) drugi podpunkt). Poza sprostowaniem i usunięciem wprowadzono *„**blokowanie**"* (chociaż bez zdefiniowania tej koncepcji)[71] (art. 12(b)). Przewidziano także, że o ewentualnym sprostowaniu, blokowaniu i usunięciu należy zawiadomić ***osoby trzecie***, którym dane zostały ujawnione (art. 12(c)).

Wprowadzono również nowe prawa: **ogólne prawo do sprzeciwu** z „ważnych i uzasadnionych przyczyn" co do przetwarzania „przynajmniej" w odniesieniu do przetwarzania w celu realizacji zadania wykonywanego w interesie publicznym lub sprawowania władzy publicznej albo w oparciu o kryterium „uzasadnionego interesu"/"równowagi", pod warunkiem że sprzeciw taki jest „uzasadniony" (art. 14(a)); bardziej konkretne i silniejsze **prawo do sprzeciwu co do przetwarzania danych dla celów marketingu bezpośredniego** (w tamtych czasach głównie poprzez przesyłki reklamowe, przed narodzinami Internetu i spamów), które należało zawsze szanować, bez konieczności jakiegokolwiek uzasadnienia ze strony osoby, której dane dotyczą (art. 14(b)); oraz **prawo do nieobjęcia decyzją o w pełni zautomatyzowanym przetwarzaniu w oparciu o profilowanie**[72], które niesie za sobą skutki prawne lub inne istotne skutki (z zastrzeżeniem ważnych, ale ściśle wyszczególnionych ***wyłączeń***) (art. 15). W tym ostatnim przypadku należy zauważyć, że art. 12(a), podpunkt trzeci, przewidywał, że osoby, których dane dotyczą, posiadały także **nowe** prawo do uzyskania (w kontekście wniosku o udzielenie dostępu) **informacji na temat „logiki"** związanej z automatycznym przetwarzaniem dotyczących ich danych, „przynajmniej" w przypadku zautomatyzowanego procesu decyzyjnego opartego na profilowaniu.

Prawa wynikające z dyrektywy z 1995 r., które zostały przeniesione i dodatkowo wzmocnione w RODO, stają się coraz ważniejsze w związku z podejmowaniem decyzji opartych na „sztucznej inteligencji".

*NOWE Poufność i bezpieczeństwo danych

Konwencja z 1981 roku po prostu przewidywała, że należy podjąć „odpowiednie środki bezpieczeństwa", aby zabezpieczyć dane osobowe przed „przypadkowym zniszczeniem lub zniszczeniem bez zezwolenia albo przypadkowym zagubieniem, jak również aby zapobiec niepowołanemu dostępowi do danych oraz ich zmienianiu lub rozpowszechnianiu bez upoważnienia" (art. 7).

Dyrektywa znacząco poszerzyła tą kwestię poprzez nałożenie przede wszystkim **obowiązku poufności** na każdą osobę uczestniczącą w przetwarzaniu danych osobowych (art. 16), następnie przewidując, że administrator jest zobowiązany wdrożyć *„odpowiednie środki techniczne i organizacyjne w celu ochrony danych osobowych przed przypadkowym lub nielegalnym zniszczeniem lub przypadkową utratą, zmianą, niedozwolonym ujawnieniem lub dostępem, szczególnie wówczas, gdy przetwarzanie danych obejmuje transmisję danych w sieci, jak również przed wszelkimi innymi nielegalnymi formami przetwarzania*" (art. 17(1), z uwzględnieniem dalszych szczegółów). To ostatnie postanowienie zostało zaczerpnięte z niemieckiej federalnej ustawy o ochronie danych z 1977 roku.

Wskazano także istotne nowe wymagania co do angażowania przez administratora podmiotu przetwarzającego do przetwarzania danych w imieniu administratora, z uwzględnieniem wymogu *„wystarczających gwarancji*" w odniesieniu do bezpieczeństwa i poufności oraz wymogu szczegółowej pisemnej umowy pomiędzy administratorem i przetwarzającym (art. 17(2) – (4)).

*NOWE Ograniczenia dotyczące przekazywania danych za granicę

Jak wspomniano w pkt. 1.2.3, Konwencja z 1981 roku - w pierwotnie przyjętej formie - nie wymagała od państw będących jej stronami wprowadzenia **zakazu eksportu danych osobowych z ich własnego terytorium do państwa, które nie zapewniało podobnej ochrony.** Zajmowała się jedynie przepływem danych osobowych pomiędzy stronami Konwencji. Wprowadzenie takiego zakazu (z zastrzeżeniem ograniczonych wyłączeń), który wynikał z prawa i doświadczeń Francji oraz Danii, stanowiło więc istotny

[71] Odpowiednią koncepcję **„ograniczenia przetwarzania"** zdefiniowano w RODO, jako *„oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania"* (art. 4(3) RODO).

[72] Pełne brzmienie *„decyzją, która wywołuje skutki prawne, które jej dotyczą lub mają na nią istotny wpływ, oraz która oparta jest wyłącznie na zautomatyzowanym przetwarzaniu danych, którego celem jest dokonanie oceny niektórych dotyczących ją aspektów o charakterze osobistym, jak np. wyniki osiągane w pracy, zdolność kredytowa, wiarygodność, sposób zachowania itp."* Przepis ten zaczerpnięto bezpośrednio z francuskiej ustawy o ochronie danych z 1978 roku, art. 2 i 3.

nowy element Dyrektywy z 1995 roku.

Dyrektywa w szczególności przewidywała, że będące jej przedmiotem dane osobowe mogły być z zasady przekazywane wyłącznie do krajów trzecich, które zapewniają taki poziom ochrony, jaki można uznać za „**odpowiedni**" w rozumieniu Dyrektywy (art. 25(1)), oraz że to Komisja Europejska ustala (poprzez tak zwaną „**decyzję stwierdzającą odpowiedni poziom ochrony**"), czy sytuacja taka dotyczy konkretnego kraju trzeciego (art. 25(2))[73]. Komisja posunęła się dalej, by ustalić „odpowiedni poziom ochrony" nie tylko w odniesieniu do krajów trzecich jako całości, ale także w odniesieniu do **sektorów** w poszczególnych krajach (np. wstępnie przepisy dla organów sektora publicznego w Kanadzie) oraz specjalnych **programów** wprowadzonych w niektórych krajach (tj. systemu „*Safe Harbor*" w Stanach Zjednoczonych, zastąpionego później systemem „*Privacy Shield*").

Stosowany z zasady zakaz przekazywania danych do krajów trzecich (lub sektorów w tych krajach) nieposiadających odpowiedniej ochrony podlegał ograniczonej liczbie **wyłączeń** określonych w art. 26(1) Dyrektywy, z których większość była podobna do podstaw prawnych przetwarzania w ogóle, tj. (w skrócie):

(a) osoba, której dane dotyczą, ***jednoznacznie*** wyraziła **zgodę** na przekazanie danych (która oczywiście musiała być „***dobrowolna, konkretna i świadoma***" *oraz* ***wyrażona*** art. 2(h), o którym mowa była wcześniej), lub

(b) przekazanie danych było **konieczne** dla realizacji umowy, której stroną jest osoba, której dane dotyczą, lub w celu podjęcia działań na życzenie osoby, której dane dotyczą, przed zawarciem umowy (np. dla celów kontroli kredytowej);

(c) przekazanie danych było ***konieczne*** w celu zawarcia lub wykonania **umowy** pomiędzy administratorem a osobą trzecią zawartej w interesie osoby, której dane dotyczą (np. rezerwacja hotelu);

(d) przekazanie danych jest ***konieczne*** lub ***prawnie wymagane*** w oparciu o **istotny interes publiczny** lub w celu ustalenia, wykonania lub ochrony **roszczeń prawnych;**

(e) przekazanie danych jest ***konieczne*** dla ochrony **żywotnych interesów osoby, której dane dotyczą,** lub

(f) dane są przekazywane z **ogólnie dostępnego rejestru** (z zastrzeżeniem warunków mających zastosowanie do dostępu do takiego rejestru w ogóle).

Ponadto państwa członkowskie mogły **zezwolić** na przekazanie danych, jeżeli administrator zaleci „***odpowiednie zabezpieczenia***" odnośnie do ochrony prywatności oraz podstawowych praw i wolności osoby, której dane dotyczą (art. 26(2)), np. w formie ***doraźnych klauzul w sprawie przekazywania danych***, a Komisja **ma prawo** zatwierdzić pewne „***standardowe klauzule umowne***" dotyczące przekazywania danych, które zapewniałyby taką ochronę (art. 26(4)).

Szereg organów ochrony danych (oraz w okresie ich tworzenia Grupa Robocza Art. 29) także przyjrzało się tak zwanym ***Wiążącym regułom korporacyjnym,*** tj. regułom wydawanym przez przedsiębiorstwa międzynarodowe lub grupy przedsiębiorstw, które regulowały wykorzystanie i przepływ danych osobowych w ramach takich przedsiębiorstw lub grup[74]. Pomimo wahań po stronie niektórych organów

[73] Zwrot „odpowiednia ochrona" wybrano, ponieważ zwrot „równoważny" był już zastrzeżony w prawie WE (a potem UE) do relacji pomiędzy zasadami wśród państw członkowskich, chociaż na podstawie prawa międzynarodowego byłyby „równoważny w skutkach". W swoim wyroku w sprawie *Maximillian Schrems przeciwko Komisarzowi ds. Ochrony Danych,* wyrok Trybunału Sprawiedliwości UE w sprawie C-363/14, 6 grudnia 2015 r. Trybunał stwierdził, że zwrot „odpowiednia ochrona" należy rozumieć jako faktycznie wymagający „zasadniczo równoważnej" ochrony w państwie trzecim: zob. par. 96 wyroku, ale było to oczywiście wiele lat przed przyjęciem Dyrektywy z 1995 roku (lub Protokołu dodatkowego z 2001 roku do Konwencji z 1981 roku, o którym mowa w dalszej części tekstu).

[74] Grupa Robocza Art. 29 zajmowała się Wiążącymi regułami korporacyjnymi w wielu dokumentach roboczych i rekomendacjach, z uwzględnieniem:

- Dokumentu roboczego: w sprawie przekazywania danych osobowych do krajów trzecich (Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers), przyjętego przez Grupę Roboczą Art. 29 3 czerwca 2003 r. (WP74);
- Dokumentu roboczego w sprawie opracowania przykładowej listy kontrolnej do zatwierdzenia wiążących reguł korporacyjnych (Working Document Establishing a Model Checklist Application for Approval of Binding Corporate Rules), przyjętego przez Grupę Roboczą Art. 29 3 czerwca 2003 r. (WP108);
- Rekomendacji 1/2007 w sprawie standardowego wniosku o zatwierdzenie wiążących reguł korporacyjnych dotyczących przekazywania danych osobowych (Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data), przyjętej przez Grupę Roboczą Art. 29 10 stycznia 2007 r. (WP133);

ochrony danych, pomysł ten został formalnie uwzględniony w RODO (jak zauważono w części drugiej Podręcznika).

Ograniczenia dotyczące przekazywania danych osobowych do krajów trzecich niezapewniających odpowiedniej ochrony przewidywały działania wymagane poza terytorium Europy. W szczególności hiszpańskie i francuskie organy ochrony danych wykorzystały to, by promować przyjęcie odpowiednich przepisów w swoich odpowiednich globalnych strefach językowych, tj. odpowiednio w Ameryce Łacińskiej oraz krajach francuskojęzycznych, w szczególności w Afryce.

Uwaga: jak zauważono w pkt. 1.2.3 wymóg „odpowiedniej ochrony" przekazu danych został wprowadzony dla Konwencji z 1981 roku w Protokole dodatkowym z 2001 roku do Konwencji w celu uzgodnienia przepisów Konwencji w tym względzie z przepisami wynikającymi z Dyrektywy WE z 1995 roku (zob. art. 2(1) Protokołu dodatkowego), chociaż dotyczy to oczywiście państw będących stronami pierwotnej Konwencji, które przystąpiły także do Protokołu[75].

*NOWY Kodeksy postępowania (i proces certyfikacji)

Kolejnym nowym elementem wprowadzonym przez Dyrektywę było jej nawiązanie do **kodeksów postępowania**, których celem jest *„usprawnienie procesu prawidłowego wprowadzania krajowych przepisów przyjętych przez Państwa Członkowskie na mocy niniejszej dyrektywy, uwzględniając szczególne cechy różnych sektorów"* (art. 27(1)), chociaż posunięto się jedynie do „zachęcania" do tworzenia tego typu kodeksów (*idem*), wymagając, by państwa członkowskie przewidziały ocenę ***projektu kodeksów krajowych*** (art. 27(1)), chociaż posunięto się jedynie do „zachęcania" do tworzenia tego typu kodeksów (idem), wymagając, by państwa członkowskie przewidziały ocenę ***projektu kodeksów krajowych*** (art. 27(3)).

W praktyce bardzo niewiele kodeksów zostało zatwierdzonych lub nawet przedłożonych do zatwierdzenia. Pierwszy opracowany przez europejskie stowarzyszenie marketingu bezpośredniego (FEDMA) projekt europejskiego kodeksu praktyk dotyczących wykorzystania danych osobowych w marketingu bezpośrednim został przekazany Grupie Roboczej Art. 29 w 1998 roku, ale ostateczna wersja została zatwierdzona dopiero w 2003 roku[76]. Projekt Kodeksu postępowania dla dostawców usług w chmurze, sporządzony przez roboczą grupę sektorową w 2013 roku i faktycznie podlegający dwóm Dyrekcjom Generalnym UE (Dyrekcji Generalnej ds. Sieci Telekomunikacyjnych oraz Dyrekcji Generalnej ds. Sprawiedliwości) został przekazany Grupie Roboczej Art. 29 w styczniu 2015 roku, ale nie został przez nią zatwierdzony w opinii w sprawie projektu i w dalszym ciągu traktowany jest jako „sprawa w toku"[77].

- Dokumentu roboczego zawierającego tabelę elementów i zasad, jakie należy uwzględnić w wiążących regułach korporacyjnych, przyjętego przez Grupę Roboczą Art. 29 24 czerwca 2008 r. (WP153);
- Dokumentu roboczego określającego ramową strukturę wiążących reguł korporacyjnych, przyjętego przez Grupę Roboczą Art. 29 24 czerwca 2008 r. (WP154);
- Dokumentu roboczego w sprawie często zadawanych pytań dotyczących wiążących reguł korporacyjnych, przyjętego przez Grupę Roboczą Art. 29 24 czerwca 2008 r., ze zmianami przyjętymi 8 kwietnia 2009 r. (WP155);
- Dokumentu roboczego 02/2012 zawierającego tabelę elementów i zasad, jakie należy uwzględnić w wiążących regułach korporacyjnych podmiotu przetwarzającego, przyjętego przez Grupę Roboczą Art. 29 6 czerwca 2012 r. (WP195);

Zob. także:

- Opinia 02/2014 wymogów dotyczących wiążących reguł korporacyjnych przekazywanych krajowym organom ochrony danych w UE oraz transgranicznych reguł prywatności przekazywanych Agentom ds. Rozliczalności PEC CBPR (Opinion on a referential for requirements for Binding Corporate Rules submitted to national Data Protection Authorities in the EU and Cross Border Privacy Rules submitted to APEC CBPR Accountability Agents), przyjęta 27 lutego 2014 r. (WP212).

[75] Zob. przypis 46 powyżej. Należy zauważyć jednak, że nie jest jasne, czy zwrot „odpowiednia" w tym artykule Protokołu można lub należy interpretować zgodnie z wyrokiem w sprawie *Schrems* (przypis 73 powyżej), a tym samym czy Protokół dodatkowy faktycznie osiągnął ten cel.

[76] Tekst Kodeksu: https://www.fedma.org/wp-content/uploads/2017/06/FEDMACodeEN.pdf. Opinia Grupy Roboczej Art. 29 nr 3/2003 w sprawie europejskiego kodeksu postępowania FEDMA dotyczącego wykorzystywania danych osobowych w marketingu bezpośrednim, zatwierdzająca kodeks (WP77, przyjęta 13 czerwca 2003 roku) dostępna jest na stronie http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp77_en.pdf.

[77] Zob.: https://ec.europa.eu/digital-single-market/en/news/data-protection-code-conduct-cloud-service-providers (19 lipca 2013 r. - informacje ogólne i podstawowe dokumenty) https://ec.europa.eu/digital-single-market/en/news/data-protection-code-conduct-cloud-service-providers (12 października 2015 - najnowsze dostępne informacje na tej stronie). Opinia Grupy Roboczej Art. 29 nr 02/2015 w sprawie Kodeksu postępowania C-SIG dotyczącego chmur obliczeniowych (WP232, przyjęta 22 września 2015 roku) dostępna jest na stronie http://ec.europa.eu/justice/article-29/documentation/opinion-

Chociaż Dyrektywa z 1995 r. wyraźnie tego nie wspomina, Komisja Europejska zachęcała także do tworzenia programów certyfikacyjnych.[78] Komisja zapewniała wstępne finansowanie dla grupy organów ochrony danych oraz ekspertów pod kierownictwem organu ochrony danych w Schlewig-Holstein w celu ustanowienia **pan-unijnego programu certyfikacyjnego, *europejskiego systemu etykiet prywatności*** (EuroPriSe), w ramach którego produkty i usługi obejmujące wykorzystanie danych osobowych można ocenić i, jeżeli uznano je za zgodne z Dyrektywą (oraz w stosownym przypadku innymi regulacjami UE w sprawie ochrony danych, takimi jak Dyrektywa o e-prywatności, o której mowa w kolejnym punkcie), i następnie przyznać im certyfikat potwierdzający taką zgodność (chociaż, ponieważ Dyrektywa nie tworzy formalnych podstaw takiego programu, certyfikaty oczywiście nie mają mocy prawnej).[79]

*NOWY Zasady dotyczące „odpowiedniego prawa"

Jak powinno jasno wynikać z różnych zapisów w powyższych różnych punktach, zgodnie z Dyrektywą państwa członkowskie miały znaczącą swobodę w ustalaniu dokładnego sposobu transponowania postanowień Dyrektywy, a wiele z jej przepisów pozwalało im przyjąć takie zasady, jakie uznały w konkretnym kontekście za stosowne. Doprowadziło to do poważnego braku harmonizacji[80] i było jednym z podstawowych powodów, dlaczego dla instrumentów następujących po Dyrektywie wybrano formę rozporządzenia.[81]

Trudności wynikające z takich rozbieżności w pewnym zakresie złagodziło istotne postanowienie Dyrektywy o ochronie danych z 1995 roku w sprawie „odpowiedniego prawa". Postanowienie to (art. 4) skutecznie określiło trzy różne zasady dla sektora prywatnego:

(1) administratorzy, którzy posiadają siedzibę w jedynym tylko państwie członkowskim muszą przestrzegać przepisów o ochronie danych takiego państwa w odniesieniu do przetwarzania danych, którymi administrują, i które „odbywa się w kontekście prowadzenia przez [danego] administratora działalności gospodarczej" (art. 4(1)(a), pierwszy fragment zdania);

(2) administratorzy, którzy posiadają siedzibę w więcej niż jednym państwie członkowskim [czytaj: posiadają przedsiębiorstwa w więcej niż jednym państwie członkowskim] muszą zapewnić, że „każde z tych przedsiębiorstw wywiązuje się z obowiązków przewidzianych w odpowiednich przepisach prawa krajowego" (niekoniecznie kraju, w którym dane przedsiębiorstwo posiada siedzibę) (art. 4(1)(a), drugi fragment zdania);

(3) administratorzy, którzy nie posiadają siedziby we Wspólnocie (UE), muszą przestrzegać przepisów państwa członkowskiego, na terytorium którego „wykorzystują środki, zarówno zautomatyzowane, jak i inne" (art. 4(12)(c)) oraz administratorzy tacy muszą na danym terytorium „wyznaczyć przedstawiciela" (art. 4(2))[82].

Warto zauważyć, że zasady te nie tylko umożliwiły państwom członkowskim zabezpieczenie swoim **obywatelom** prawa do ochrony danych przed naruszeniem przez podmiot spoza ich terytorium lub spoza UE. Zamiast tego, zgodnie z wszystkimi trzema zasadami ochroną należało objąć **dane dotyczące**

---

recommendation/files/2015/wp232_en.pdf. By uzyskać więcej danych i stanowisk w świetle RODO, zapoznaj się z pismem Grupy Roboczej Art. 29 do Dostawców Infrastruktury w Chmurze w Europie z 6 lutego 2018 roku dostępnym na stronie http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=615033.

[78] Gdy na początku lat 90. XX wieku wzrastało wykorzystanie internetu na świecie, francuski organ ochrony danych zaproponował innym unijnym organom ochrony danych oraz Komisji Europejskiej, by potraktować programy certyfikacyjne jako bardzo skuteczny sposób radzenia sobie z usługami internetowymi tworzonymi poza Europą, ale w tym czasie niczego w tym kierunku nie uczyniono.

[79] Zob. https://www.european-privacy-seal.eu/EPS-en/about-europrise

[80] Zob. zlecone przez UE badanie przeprowadzone przez Douwe Korffa, Report on an EU study on the implementation of the [1995] data protection directive, 2002, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1287667 –

[81] Zob. Część druga, pkt 2.1 oraz tekst pod pierwszym nagłówkiem "*Rozporządzenie …*" w pkt. 2.2 poniżej.

[82] Zastosowanie tej trzeciej zasady skomplikowało wykorzystanie różnych słów w różnych (ale równie prawnie autentycznych) wersjach językowych. Pierwotny projekt dyrektywy sporządzono w języku francuskim i stosowano zwrot *moyens*, który w języku angielskim oznacza *means.* Zwrot stosowany w innych oficjalnych językach pochodzących od łaciny był jego językowym odpowiednikiem i także oznaczał „means". Oficjalna niemiecka wersja także stosowała ten sam zwrot – *Mittel.* Jednak *w* tekście angielskim mowa jest o „*equipment*" (sprzęcie), co zostało powielone w wersji holenderskiej (*middlen*). Doprowadziło to do ograniczenia w Zjednoczonym Królestwie i Holandii stosowania tej zasady do sytuacji, w których administrator spoza UE/EOG *posiadał na własność* lokalny element sprzęt w UE/EOG, podczas gdy inne kraje utrzymywały, że nawet obecność smartfonu w UE/EOG wystarczy, by uznać, że administrator „wykorzystuje" takie urządzenie do celów tranzytu danych będących przedmiotem Dyrektywy. Patrz: dyskusja na temat „właściwego prawa" w odniesieniu do Dyrektywy o e-prywatności w pkt. 1.3.3 poniżej

wszystkich jednostek („osób fizycznych") przetwarzane przez odpowiednich administratorów, ***bez względu na to, czy osoby, których dane dotyczą, były w UE, czy nie, oraz bez względu na to, czy były obywatelami lub rezydentami UE, czy nie***, zgodnie z zasadą *uniwersalności praw człowieka*[83].

Zasady te były trudne do stosowania w praktyce (w szczególności w odniesieniu do administratorów spoza UE/EOG)[84], ale przewidywały przynajmniej pewne wytyczne co do sposobu traktowania różnych przepisów w różnych państwach członkowskich, które w teorii mogłyby mieć zastosowanie do poszczególnych transnarodowych operacji przetwarzania danych osobowych. Konwencja o ochronie danych z 1981 roku nie zawierała żadnego postanowienia, którego celem byłoby unikanie „kolizji prawnej".

Jeśli chodzi o sektor publiczny, określenie prawa właściwego było w praktyce prostsze: wszystkie instytucje i organy publiczne, w tym placówki dyplomatyczne, podlegały wyłącznie przepisom o ochronie danych w swoim państwie członkowskim.

*NOWE Organy nadzorcze

Kolejną nowością w Dyrektywie z 1995 roku, w porównaniu do Konwencji z 1981 roku,[85] był wymóg, by wszystkie państwa członkowskie wyznaczyły:

> jeden lub więcej organów publicznych odpowiedzialnych za kontrolę stosowania na ich terytorium przepisów przyjętych przez Państwa Członkowskie na mocy niniejszej Dyrektywy
>
> (art. 28(1), pierwsze zdanie).

By skutecznie spełniać swoje zadanie, takie „**organy nadzorcze**", w praktyce znacznie częściej zwane ***organami ochrony danych*** lub ***OOD*** (po kilka w federalnych państwach członkowskich), musiały otrzymać szerokie uprawnienia ***dochodzeniowe, interwencyjne*** *i* ***kierowania*** (z uwzględnieniem uprawnień do nakazania zablokowania, usunięcia lub zniszczenia danych albo zakazania przetwarzania) (art. 28(3), pierwszy i drugi podpunkt) oraz musiały być w stanie „*w sposób całkowicie niezależny przy wykonywaniu powierzonych im funkcji*" (art. 28(1), drugie zdanie). Wymóg niezależności jest także wymogiem demokracji i praworządności. Ponieważ wymagania dotyczące niezależności nie zostały wyraźnie wspomniane w dyrektywie, Komisja musiała uciec się do działań sądowych przeciwko kilku państwom członkowskim, by tę sprawę wyjaśnić. Rezultaty takich spraw sądowych znalazły odzwierciedlenie w bardziej dopracowanych postanowieniach RODO.

Wprowadzono obowiązek ***konsultowania się*** z organami nadzorczymi przy opracowywaniu środków i przepisów dotyczących ochrony danych (art. 28(2)), a także możliwość „***brania udziału w postępowaniu sądowym***" w związku z rzekomym naruszeniem krajowych przepisów o ochronie danych (art 28(3), trzeci podpunkt).

Były one także odpowiedzialne za zawiadomienie i „kontrolę wstępną", co zostanie omówione w następnym punkcie.

Co istotne, poza bardziej formalnymi środkami prawnymi, które wskazano w kolejnym punkcie, organy ochrony danych miały prawo „**rozpatrywać skargi [czytaj: rozwiązywać reklamacje] zgłaszane przez dowolną osobę** lub przez stowarzyszenie ją reprezentujące" w związku z ochroną danych (art. 28(4)).

Organy ochrony danych, które na poziomie UE (do 25 maja 2018 r.) współpracowały z „**Grupą Roboczą Art. 29"** omówioną w poprzednim punkcie, stały się głównymi obrońcami praw ochrony danych w UE

---

[83] Zob. Douwe Korff, Maintaining Trust in a Digital Connected Society, raport sporządzony dla Międzynarodowego Związku Telekomunikacyjnego (ITU), maj 2016 r. pkt 2.3, *Universality of human rights*: http://www.itu.int/en/ITU-D/Conferences/GSR/Documents/ITU_MaintainingTrust_GSR16.pdf.

[84] Zob. Douwe Korff, *Der EG-Richtlinienentwurf über Datenschutz und "anwendbares Recht"*, w: Recht der Datenverarbeitung, rok 10 (1994), tom nr 5- 6, str. 209 ff; *The question of "applicable law"*, w: Compliance Guide 3 – Interim report (część nowej brytyjskiej ustawy o ochronie danych z 1998 roku, Information & Compliance Programme), Privacy Laws & Business, listopad 1999 r.

[85] Przewidywały to już niewiążące Wytyczne ONZ przyjęte w 1990 roku (patrz: przypis 41). Jak zauważono w pkt. 1.2.3 spoczywający na państwach obowiązek ustanowienia niezależnych organów nadzorczych, w formie bliskiej postanowieniom Dyrektywy o ochronie danych z 1995 roku, wprowadzono dla Konwencji z 1981 roku w Protokole dodatkowym z 2001 roku do Konwencji w celu uzgodnienia przepisów Konwencji w tym względzie z przepisami wynikającymi z Dyrektywy WE z 1995 roku (patrz: art. 1 Protokołu dodatkowego), chociaż dotyczy to oczywiście państw będących stronami pierwotnej Konwencji, które przystąpiły także do Protokołu (patrz: przypis 45).

(nawet pomimo istniejących w dalszym ciągu różnych uprawnień i różnej skuteczności w ramach przepisów krajowych przyjętych w celu wdrożenia Dyrektywy).

*NOWE Zawiadamianie i „kontrola wstępna"

*NOWE *Zawiadomienie:*

Aby osiągnąć **ogólną przejrzystość** przetwarzania danych osobowych oraz pomóc zapewnić pełną zgodność z przepisami w tym zakresie, Dyrektywa o ochronie danych z 1995 roku przewidywała także szeroki system **zawiadamiania** o operacjach przetwarzania danych osobowych (art. 18, patrz: art. 19 - szczegóły treści zawiadomienia) oraz wymagała, by zgłoszone informacje wpisano do **rejestru**, który powinien być ***ogólnie dostępny*** (art. 21(2)). Oparto to na podstawie pierwszego systemu tego typu przyjętego w Szwecji w 1973 roku i następnie wprowadzonego przez wiele innych państw członkowskich UE.

Jednak, dając alternatywy dla zawiadomienia, Dyrektywa zezwalała państwom członkowskim na ***uproszczenia*** lub ***odstąpienia*** od ogólnego obowiązku zawiadomienia (głównie) w dwóch „równorzędnych" sytuacjach, tj.[86]:

- jeżeli w przypadku „nieryzykownego" przetwarzania[87] organ ochrony danych państwa członkowskiego wydał „***uproszczone normy***" określające podstawowe parametry przetwarzania danych (tj. cele przetwarzania, dane lub kategorie danych podlegających przetwarzaniu, kategorię lub kategorie osób, których dane dotyczą, odbiorców lub kategorie odbiorców, którym dane mają zostać ujawnione, oraz okres przechowywania danych) (art. 18(2), pierwszy podpunkt), przy czym administratorzy, którzy formalnie zadeklarowali, że przestrzegają takich uproszczonych norm, byli **zwolnieni** z obowiązku zawiadomienia, lub
- jeżeli prawo państwa członkowskiego wymagało wyznaczenia niezależnego ***inspektora ochrony danych*** w ramach organizacji administratora, odpowiedzialnego za „zapewnienie w niezależny sposób wewnętrznego stosowania przepisów prawa krajowego przyjętych na mocy niniejszej dyrektywy oraz za prowadzenie rejestru operacji przetwarzania danych wykonywanych przez administratora danych i zawierających takie same informacje, jakie należałoby w innym przypadku zgłosić organowi ochrony danych (art. 18(2), drugi podpunkt).

Pierwszy z wyjątków oparty był na francuskim systemie „*normes simplifiées*", a drugi na niemieckim systemie wymagającym wyznaczenia Inspektorów ochrony danych w ramach organizacji wszystkich administratorów publicznych i większości dużych administratorów sektora prywatnego[88]. W odniesieniu do obydwu alternatywnych systemów Dyrektywa przewidywała, że administratorzy (lub inny organ wyznaczony przez państwo członkowskie) powinni udostępnić ogółowi społeczeństwa takie same informacje, jakie zostałyby udostępnione poprzez rejestr zgłoszonych operacji (art. 21(3)).

*NEW *„Kontrola wstępna":*

Zgodnie z francuskim podejściem Dyrektywa z 1995 roku wymagała, by przetwarzanie danych, które stwarza „**określone zagrożenia dla praw i wolności osób, których dane dotyczą" („ryzykowne przetwarzanie"),** podlegało daleko idącemu wymogowi „**kontroli wstępnej**" (art. 20). Państwa członkowskie same miały ustalić, **jakiego rodzaju operacje przetwarzania** poddałyby temu daleko idącemu wymogowi (biorąc pod uwagę cel przetwarzania, rodzaje danych oraz skalę przetwarzania). Państwa członkowskie mogły także wybrać, **jak i przez kogo** taka kontrola byłaby wykonywana, w

[86] Pozostałe operacje, które można było zwolnić z obowiązku zawiadomienia to **rejestry publiczne,** przetwarzanie **rejestrów członków i stowarzyszeń nienastawionych na osiąganie zysku organizacji politycznych, religijnych, filozoficznych lub związkowych (podlegających pewnym gwarancjom)** oraz **ręcznie prowadzone zbiory danych** (art. 18(3) - (5)).

[87] Pełny tekst: „w przypadku kategorii operacji przetwarzania, co do których mało prawdopodobne jest, biorąc pod uwagę dane przeznaczone do przetworzenia, aby niekorzystnie wpłynęły na prawa i wolności osób, których dane dotyczą".

[88] Odpowiednio *behördliche*- i *betriebliche Datenschutzbeauftragten*, nie mylić z państwowymi i federalnymi organami ochrony danych, *Landes*- i *Bundesdatenschutzbeauftragten*. Należy zauważyć, że chociaż wiele państw członkowskich wprowadziło koncepcję inspektora ochrony danych w przepisach wdrażających dyrektywę, uczyniono to na różne sposoby, w różnym zakresie oraz z uwzględnieniem różnych zadań inspektora, a także różnych warunków jego nominacji. Jak zostało to omówione w części drugiej Podręcznika, RODO zawiera z kolei szczegółowe, zharmonizowane wytyczne dotyczące ich nominacji oraz powiązania z zasadą „rozliczalności".

szczególności:

- czy należy jej wymagać ***po złożeniu zawiadomienia*** wskazującego, że zgłoszona operacja ze względu na swój rodzaj wymaga takiej kontroli ze strony organu ochrony danych (francuskie podejście, które zastosowało także większość pozostałych państw członkowskich) lub
- czy przetwarzanie miało podlegać prawu lub uzupełniającemu instrumentowi legislacyjnemu ze strony organu ochrony danych w trakcie jego przygotowania lub Parlamentu w trakcie jego przyjmowania.

(Art. 20(2) i (3)).

Ze względu na różne opcje dopuszczone postanowieniami Dyrektywy, różne państwa członkowskie przyjęły (lub raczej zachowały) różne systemy w tym względzie, co oznaczało, że niektóre operacje podlegały zgłoszeniu lub kontroli wstępnej w niektórych państwach członkowskich, a w innych nie.

*NOWE Konkretne środki prawne i sankcje

Konwencja z 1981 roku przewidywała, że państwa będące stronami Konwencji powinny wprowadzić ***odpowiednie sankcje i środki prawne*** w związku z naruszeniem krajowych przepisów o ochronie danych, ale nie wyjaśniała, co oznacza sformułowanie „odpowiednie".

W przeciwieństwie do tego postanowienia Konwencji z 1981 roku, Dyrektywa z 1995 roku przewidywała, że osoby, których dane dotyczą, powinny mieć dostęp do **środków sądowych** w związku z (domniemanym) naruszeniem ich praw (niezależnie od prawa do wnoszenia skarg do właściwego krajowego organu ochrony danych, o czym mowa w poprzednim punkcie) (art. 22). Ponadto każdej osobie, która poniosła szkodę wskutek niezgodnej z prawem operacji przetwarzania danych lub innej czynności niezgodnej z Dyrektywą, przysługuje od administratora danych **odszkodowanie** (chyba że administrator jest w stanie udowodnić, że nie ponosi z tego tytułu odpowiedzialności) (art. 23)[89]. Poza tymi środkami prawnymi państwa członkowskie zostały także zobowiązane do wprowadzenia dalszych „odpowiednich środków" i „sankcji", bez względu na indywidualne roszczenia lub skargi (art. 24).

Jednak w wielu państwach członkowskich faktyczne kary, jakie można było nałożyć na mocy odpowiedniego prawa krajowego lub jakie były nakładane w praktyce, były względnie niskie[90].

*NOWE Grupa robocza Art. 29 i Komitet Art. 31

W końcu Dyrektywa o ochronie danych z 1995 roku ustanowiła dwa podmioty unijne nazwane na podstawie artykułów, na mocy których je utworzono:

- tak zwaną „**Grupę Roboczą Art. 29**" – to niezależna grupa składająca się z przedstawicieli organów ochrony danych państw członkowskich, a także EDPS (European Data Protection Supervisor, Europejski Inspektor Ochrony Danych) oraz przedstawiciela Komisji Europejskiej (odpowiedzialnego za sekretariat grupy i bez prawa głosu), której nadano zadanie przyczyniania się do bardziej zharmonizowanego stosowania Dyrektywy, w szczególności poprzez przyjmowanie rekomendacji i opinii (z własnej inicjatywy) oraz wydawanie opinii na temat wszelkich projektów kodeksów postępowania wypracowanych na poziomie UE; i z którą Komisja Europejska miała obowiązek konsultować wszelkie propozycje dotyczące *„praw i wolności osób fizycznych w odniesieniu do przetwarzania danych osobowych*" (tj. ochrony danych) oraz wszelkie projekty decyzji dotyczących zapewnienia odpowiedniej ochrony w krajach trzecich[91] oraz
- tak zwany „**Komitet Art. 31**", składający się z przedstawicieli rządów państw członkowskich,

[89] Zjednoczone Królestwo wstępnie próbowało ograniczyć je do szkód rzeczowych, ale ostatecznie uznano, że Dyrektywa wymaga, by osoby były w stanie uzyskać odszkodowanie za szkody niematerialne (cierpienie).

[90] Potrzeba wyższych kar stała się widoczna dopiero po pojawieniu się internetu, w znacznej mierze kontrolowanego przez podmioty spoza UE/EOG, w przypadku których istniało mniejsze prawdopodobieństwo, że będą przestrzegać unijnych zasad ochrony danych jedynie na podstawie ponaglenia ze strony unijnych organów ochrony danych. Znajduje to odzwierciedlenie w znacznie ostrzejszym postanowieniu RODO, które przewiduje, że organy ochrony danych mogą nakładać administracyjne kary pieniężne w wysokości do 10.000.000 euro lub 2% rocznych obrotów odpowiedniego podmiotu lub w szczególnie poważnych przypadkach do 20.000.000 euro lub 4% rocznych obrotów (art. 83 RODO).

[91] Więcej szczegółów przedstawiono w art. 30.

któremu przewodniczył przedstawiciel Komisji, do którego należało przekazywać do zaopiniowania wszystkie projekty środków, jakie miały zostać podjęte na mocy Dyrektywy; jeżeli Komitet wydał negatywną opinię, dany środek należało skierować do Rady, gdzie mógł zostać odrzucony kwalifikowaną większością głosów.[92]

Grupa Robocza art. 29 (WP29) wydała **liczne dokumenty i opinie robocze** na temat wyjątkowo szerokiego zakresu spraw dotyczących stosowania Dyrektywy o ochronie danych z 1995 roku oraz Dyrektywy o e-prywatności z 2002 roku (omówionej w pkt 1.3.3)[93]. Dokumenty te, a w szczególności formalne opinie, chociaż nie są prawnie wiążące, w dalszym ciągu mają wysoce autorytatywne znaczenie w odniesieniu do dyrektyw. Pomagają zapewnić faktycznie pełne i ścisłe stosowanie dyrektyw na „wysokim poziomie" oraz w pewnym zakresie łagodzą problemy wynikające z rozbieżności w przepisach państw członkowskich.

Uwaga: Następca Grupy Roboczej Art. 29, Europejska Rada Ochrony Danych (European Data Protection Board, EDPB) bazuje na pracy Grupy Roboczej Art. 29 - w pierwszym dniu swojego istnienia, tj. 25 maja 2018 roku, Rada potwierdziła zakres opinii Grupy Roboczej, które sporządzono w ramach przygotowań do RODO[94]. Obsługę jej sekretariatu zapewnia EDPS.

1.3.3 Dyrektywa o ochronie danych w sektorze telekomunikacyjnym z 1997 roku, dyrektywa WE o e-prywatności z 2002 roku i zmiany z 2009 roku w dyrektywie o e-prywatności

Informacje ogólne

Dyrektywa o ochronie danych w sektorze telekomunikacyjnym, zaproponowana w tym samym czasie, co Dyrektywa o ochronie danych z 1995 roku, została przyjęta 15 grudnia 1997 roku[95]. Jej relację z Dyrektywą o ochronie danych z 1995 roku wyjaśniono w art. 1(2), który stwierdza, że postanowienia dyrektywy „dookreślają i uzupełniają" główną dyrektywę. W szczególności zawarte w Dyrektywie z 1995 roku definicje dotyczące ochrony danych oraz wszystkie inne zasady miały zastosowanie również do administratorów danych i operacji przetwarzania podlegających Dyrektywie o ochronie danych w sektorze telekomunikacyjnym, chyba że określała ona bardziej szczegółowe zasady. Także w odniesieniu do konkretnych celów, funkcji lub usług (szczegółowy rachunek, identyfikacja numeru dzwoniącego, książki telefoniczne itp.: patrz poniżej) odpowiednie postanowienia stanowią interpretację i zastosowanie ogólnych zasad i praw przewidzianych w Dyrektywie z 1995 roku. Innymi słowy, Dyrektywa o ochronie danych w sektorze telekomunikacyjnym stanowiła *lex specialis* w stosunku do Dyrektywy o ochronie danych z 1995 roku, *lex generalis.*

Wdrożenie tej dyrektywy uległo opóźnieniu, miedzy innymi dlatego, że w 1999 roku Komisja przeprowadziła ogólny przegląd ram regulacyjnych dla komunikacji elektronicznej w świetle rozwoju nowych technologii i praktyk sektorowych. Jednym z efektów przeglądu była wystosowana w 2000 roku propozycja zastąpienia Dyrektywy o ochronie danych w sektorze telekomunikacyjnym nową dyrektywą dotyczącą ochrony danych w sektorze łączności elektronicznej[96]. Doprowadziło to do przyjęcia w lipcu 2002 roku Dyrektywy w o prywatności i łączności elektronicznej, Dyrektywa 2002/58/WE, ogólnie

[92] Więcej szczegółów przedstawiono w art. 31.

[93] Wszystkie dokumenty Grupy Roboczej Art. 29 przyjęte w okresie od 1997 roku do listopada 2016 roku można przejrzeć na archiwalnej stronie http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm. Aktualizacje oraz dokumenty przyjęte po listopadzie 2016 roku do czasu zlikwidowania Grupy Roboczej Art. 29 25 maja 2018 roku można znaleźć na stronie: http://ec.europa.eu/newsroom/article29/news-overview.cfm.

[94] Zob. przypis 215 poniżej.

[95] Pełny tekst: Dyrektywa 97/66/WE Parlamentu Europejskiego i Rady 15 grudnia 1997 roku w sprawie przetwarzania danych osobowych i ochrony prywatnych danych w sektorze telekomunikacyjnym, OJ L24, 30.01.1998, str. 1 – 8, https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:31997L0066&from=PL. Dyrektywa o ochronie danych w sektorze telekomunikacyjnym opierała się w znacznej mierze na pracy wykonanej w ramach Radę Europy w odniesieniu do rekomendacji w tej samej sprawie, co doprowadziło do przyjęcia Rekomendacji nr R (95) 4 Komitetu Ministrów Rady Europy do Państw Członkowskich w sprawie ochrony danych osobowych w obszarze usług telekomunikacyjnych, ze szczególnym uwzględnieniem usług telefonicznych, przyjętej 7 lutego 1995 roku, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168050108e oraz pracy organów ochrony danych w utworzonej w 1983 roku *Międzynarodowej Grupy Roboczej ds. Ochrony Danych w Sektorze Telekomunikacyjnym* („Grupa berlińska"), zob. https://www.dataprotectionauthority.be/berlin-group.

[96] Propozycja Dyrektywy Parlamentu Europejskiego i Rady dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej, Bruksela, 12.07.2000, COM(2000) 365 final.

zwanej „**Dyrektywą o e-prywatności**”[97]. Dyrektywa ta także podkreślała swój pomocniczy i uzupełniający charakter w stosunku do głównej Dyrektywy o ochronie danych z 1995 roku w takim samym zakresie, jak jej poprzedniczka (patrz: art. 1(2)).

W 2009 roku Dyrektywa z 2002 roku została zmieniona poprzez wprowadzenie osobnej dyrektywy, tj. dyrektywy 2009/136/WE[98], często zwanej **prawem dotyczącym plików cookies**, gdyż reguluje kwestie związane z tego typu plikami (chociaż dotyczy także innych spraw oraz przetwarzania danych). Poniżej opiszemy zasady, jakie zawarto w Dyrektywie z 2002 roku z uwzględnieniem zmian wprowadzonych dyrektywą z 2009 roku. W niniejszym Podręczniku będziemy zwięźle określać Dyrektywę o ochronie danych z 1995 roku „główną dyrektywą”, a Dyrektywę o e-prywatności „pomocniczą dyrektywą”.

W czasie, gdy opracowywano niniejszy Podręcznik (grudzień 2018 roku), Dyrektywa o e-prywatności była w dalszym ciągu w mocy, mimo że jej „macierzysty” instrument, tj. główna Dyrektywa o ochronie danych z 1995 roku została zastąpiona Ogólnym rozporządzeniem o ochronie danych. Następca Dyrektywy o e-prywatności, także raczej w formie rozporządzenia (a nie dyrektywy), jest na etapie przyjmowania (patrz: pkt. 1.4.2 poniżej). Ponieważ Dyrektywa o e-prywatności pozostaje obecnie w mocy, w dalszym ciągu poświęca się jej uwagę w tym wydaniu Podręcznika. Oczekując na przyjęcie proponowanego nowego rozporządzenia o e-prywatności, opiszemy w czasie teraźniejszym obecnie obowiązującą Dyrektywę o e-prywatności.

Cel, przedmiot i zakres Dyrektywy o e-prywatności z 2002 r. zmienionej w 2009 r.

Chociaż główna Dyrektywa o ochronie danych z 1995 roku miała szerokie zastosowanie do wszystkich form przetwarzania danych osobowych przez odpowiednie podmioty sektora publicznego i prywatnego działające w „pierwszym filarze” Wspólnoty Europejskiej, Dyrektywa o e-prywatności, jako instrument pomocniczy, ma znacznie węższy (szczegółowo określony) zakres. Zgodnie z zawartym w niej sformułowaniem ma ona zastosowanie do:

> przetwarzania danych osobowych w związku z dostarczaniem **publicznie dostępnych usług łączności elektronicznej w publicznych sieciach łączności** we Wspólnocie, *z uwzględnieniem publicznych sieci łączności wspomagających zbieranie danych i urządzenia identyfikacyjne.*
>
> (Artykuł 3, dodano podkreślenie; fragment pisany pochyłą czcionką dodano w 2009 roku)[99]

Zwrot „usługi łączności elektronicznej” został dokładnie i ściśle zdefiniowany w artykule 2(c) zmienionej Dyrektywy ramowej[100], w następujący sposób:

> „usługa łączności elektronicznej" oznacza usługę zazwyczaj świadczoną za wynagrodzenie, polegającą całkowicie lub częściowo na przekazywaniu sygnałów w sieciach łączności elektronicznej, w tym usługi telekomunikacyjne i usługi transmisyjne świadczone poprzez sieci nadawcze; nie obejmuje jednak usług związanych z zapewnianiem albo wykonywaniem kontroli treści przekazywanych przy wykorzystaniu sieci lub usług łączności elektronicznej. **Spod zakresu niniejszej definicji wyłączone są usługi społeczeństwa informacyjnego w rozumieniu art. 1 dyrektywy 98/34/WE[101], jeżeli nie polegają one całkowicie lub częściowo na przekazywaniu**

[97] Pełny tytuł: Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z 12 lipca 2002 dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej), OJ L201, 31.07.2002 r. str. 37 – 47, https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32002L0058&from=PL

[98] Pełny tytuł: Dyrektywa 2009/136/WE Parlamentu Europejskiego i Rady z 25 listopada 2009 roku zmieniająca dyrektywę 2002/22/WE w sprawie usługi powszechnej i związanych z sieciami i usługami łączności elektronicznej praw użytkowników, dyrektywę 2002/58/WE dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej oraz rozporządzenie (WE) nr 2006/2004 w sprawie współpracy między organami krajowymi odpowiedzialnymi za egzekwowanie przepisów prawa w zakresie ochrony konsumentów OJ L337, 18.12.2009 r. str. 11 – 36, https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32009L0136.

[99] W ramach zmian wprowadzonych w 2009 roku usunięto zawarte w pierwotnej wersji (z 2002 roku) Dyrektywy o e-prywatności odstępstwo dotyczące central analogowych.

[100] Pełny tytuł: Dyrektywa 2002/21/WE Parlamentu Europejskiego i Rady z 7 marca 2002 roku w sprawie wspólnych ram regulacyjnych sieci i usług łączności elektronicznej (dyrektywa ramowa), OJ L108, 24.04.2002 r. str. 33 – 50, https://eur-lex.europa.eu/legal-content/ga/TXT/?uri=CELEX:32002L0021.

[101] Pełny tytuł: Dyrektywa 98/34/WE Parlamentu Europejskiego i Rady z dnia 22 czerwca 1998 r. ustanawiająca procedurę udzielania informacji w zakresie norm i przepisów technicznych, OJ L 204, 21.07.1998 r. str. 37 – 48, https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX%3A31998L0034.

sygnałów w sieciach łączności elektronicznej (dodano podkreślenie).

Na podstawie postanowienia zawartego w artykule 3 oraz z definicji przewidzianych w tych instrumentach, Grupa Robocza Art. 29 wysunęła prosty wniosek, który wyrażono w Opinii Grupy Roboczej Art. 29 z 2011 roku w sprawie usług geolokacji na inteligentnych urządzeniach mobilnych (Opinion on Geolocation services on smart mobile devices)[102]: Dyrektywa o e-prywatności ma zastosowanie do dostawców usług łączności elektronicznej, takich jak operatorzy usług telekomunikacyjnych oraz dostawcy usług internetowych, ale nie do dostawców usług społeczeństwa informacyjnego[103].

(Jak zauważono ponadto w pkt. 1.4.2 poniżej, Komisja proponuje usunąć takie ograniczenie w proponowanym rozporządzeniu o e-prywatności, ale dopóki tak się nie stanie, oczywiście pozostaje ono w mocy).

W tym ograniczonym zakresie Dyrektywa o e-prywatności posiada takie same cele jak główna Dyrektywa: zapewnienie jednocześnie ***wysokiego poziomu ochrony danych osobowych*** (jednak szczególnie w tym sektorze) oraz umożliwienie ***swobodnego przepływu danych osobowych*** we Wspólnocie (w tym sektorze) (patrz: art. 1(1)). Miała ona zasadniczy wpływ na szybko rozwijający się i niezwykle istotny sektor łączności elektronicznej, zapewniając wyższy poziom ochrony danych w tym obszarze w UE, niż gdziekolwiek indziej na świecie.

Stwierdzając powyższe, pomimo wydawałoby się jasnego języka artykułu 3, kwestia dokładnego zakresu Dyrektywy o e-prywatności nie jest do końca jasna, ponieważ część z jej postanowień ma szersze zastosowanie, lub można je w ten sposób odczytywać oraz nie zawiera ona jasnego postanowienia dotyczącego odpowiedniego prawa. Nie pomniejszając powodzenia Dyrektywy o e-prywatności, należałoby w skrócie odnotować wyżej wspomniane dwuznaczności.

Dwuznaczność i brak spójności co do zakresu

Występuje, przede wszystkim, dwuznaczność co do materialnego zakresu stosowania:

Dyrektywa o e-prywatności**.**

Jak zauważyła również Komisja w swojej propozycji rozporządzenia o e-prywatności[104]:

> Konsumenci i przedsiębiorstwa coraz częściej polegają na nowych usługach internetowych umożliwiających komunikację interpersonalną, takich jak Voice over IP, instant messaging i internetowe usługi poczty elektronicznej, w miejsce tradycyjnych usług łączności. **Tego typu usługi łączności OTT *z zasady* nie podlegają aktualnym ramom Unii dotyczącym łączności elektronicznej Unii, w tym postanowieniom Dyrektywy o e-prywatności.**

Zlecone przez Komisję w 2013 badanie (Studium SMART) stwierdziło, że[105]:

> **przepisy krajowe dotyczące takich tematów, jak pliki cookies, ruch i dane dotyczące lokalizacji lub niezamówionych komunikatów, przyjęte zgodnie z Dyrektywą o e-prywatności, często mają inny zakres zastosowania niż przewidziano w art. 3 Dyrektywy o e-prywatności**, która ogranicza się wyłącznie do dostawców publicznie dostępnych usług łączności elektronicznej (tj. tradycyjnych firm telekomunikacyjnych. [Badanie pokazało], że ograniczenie zakresu Dyrektywy jedynie do

---

[102] Grupa Robocza Art. 29, Opinia 13/2011 w sprawie usług geolokacji w inteligentnych urządzeniach mobilnych (WP185, 16 maja 2011 roku), http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp185_en.pdf.

[103] Grupa Robocza Art. 29, Opinia 13/2011 w sprawie usług geolokacji w inteligentnych urządzeniach mobilnych (poprzedni przypis) ust. 4.2.1, *Zakres stosowania skorygowanej dyrektywy o e-prywatności*(str. 8 – 9). Jak wspomniano jeszcze dokładniej w Dokumencie roboczym Komisji (przypis 99 powyżej):
„By być przedmiotem Dyrektywy:
(1) usługa powinna stanowić usługę łączności elektronicznej,
(2) usługa powinna być oferowana w sieci łączności elektronicznej,
(3) usługa i sieć powinny być ogólnie dostępne oraz
(4) sieć lub usługa powinna być dostępna we Wspólnocie." (str. 20)
Jak zauważono w pkt. 1.4.2, Komisja proponuje usunąć takie ograniczenie w proponowanym rozporządzeniu o e-prywatności, ale dopóki tak się nie stanie, oczywiście pozostaje ono w mocy.

[104] Propozycja rozporządzenia o e-prywatności (przypis 175 poniżej), pkt 1.1, str. 1, podkreślenie dodano.

[105] Podsumowanie Komisji dotyczące ustaleń z Badania SMART (podkreślenie dodano).

dostawców usług łączności elektronicznej jest dwuznaczne i może prowadzić do nierównego traktowania, w przypadku gdy dostawców usług społeczeństwa informacyjnego korzystający z internetu w celu świadczenia usług łączności są z zasady z takiego zakresu wyłączeni.

Brakuje również jasności co do odpowiedniego prawa krajowego:

Do momentu, gdy Dyrektywa o e-prywatności zostanie zastąpiona proponowanym Rozporządzeniem o e-prywatności (co może nie mieć miejsca jeszcze przez jakiś czas), wyżej wymienione dwuznaczności i niejasności pozostaną, a skuteczność Dyrektywy o e-prywatności będzie w dalszym ciągu zagrożona.

Związek pomiędzy Dyrektywą o e-prywatności a RODO

Dyrektywa o e-prywatności była *lex specialis* w odniesieniu do *lex generalis* Dyrektywy z 1995 r. **i stąd też stanowi *lex specialis* wobec jej następcy: RODO. Odnośnie spraw szczegółowo regulowanych Dyrektywą o e-prywatności,** zastosowanie ma ta dyrektywa, nie zaś przepisy RODO.

Podstawy prawne RODO nie mają zatem zastosowania, gdy Dyrektywa o e-prywatności określa bardziej szczegółowe zasady do przetwarzania danych osobowych. Na przykład: artykuł 6 Dyrektywy o e-prywatności, który przewiduje konkretny wykaz podstaw prawnych dotyczących przetwarzania danych o ruchu, z uwzględnieniem danych o ruchu, które stanowią dane osobowe, ma zastosowanie, w efekcie czego artykuł 6 RODO nie ma zastosowania. Jednak we wszystkich innych sytuacjach związanych z przetwarzaniem danych osobowych zastosowanie ma RODO.

Taka sama sytuacja ma miejsce w odniesieniu do **podmiotów, które podlegają lub nie podlegają *„jednoznacznie postanowieniom Dyrektywy o e-prywatności*”.** Biorąc pod uwagę opinię Grupy Roboczej Art. 29, że Dyrektywa o e-prywatności zasadniczo ma zastosowanie do dostawców usług łączności elektronicznej, oznacza to, że podobnie (w sytuacjach innych niż w odniesieniu do szczególnych zasad przewidzianych w art. 5(3) i 13, które mają szersze zastosowanie) przetwarzanie wszelkich danych, w tym danych bardziej jednoznacznie podlegających Dyrektywie o e-prywatności (takich jak dane o ruchu) przez *podmioty inne niż dostawcy usług łączności elektronicznej* jest przedmiotem RODO, a nie Dyrektywy o e-prywatności, pomimo szczególnych postanowień tej dyrektywy dotyczących tego typu danych.

Innymi słowy:

- dostawcy usług łączności elektronicznej muszą przestrzegać postanowień Dyrektywy o e-prywatności w odniesieniu do wszelkich spraw, które są bardziej szczegółowo uregulowane w tej dyrektywie, oraz RODO w przypadku wszystkich innych spraw, oraz
- podmioty niebędące dostawcami usług łączności elektronicznej muszą przestrzegać postanowień art. 5(3) Dyrektywy o e-prywatności dotyczących dostępu do informacji na urządzeniach oraz art. 13 tej dyrektywy, jeżeli chodzi o niezamawiane komunikaty, a także RODO w odniesieniu do wszystkich innych spraw (tj. nie podlegają żadnym postanowieniom Dyrektywy o e-prywatności poza tymi dwoma artykułami).

Konkretne kwestie, w których pojawiają się wyżej opisane wątpliwości, omówiono w stosownym przypadku w pozostałych punktach tej części Podręcznika.

Kluczowe cechy Dyrektywy o e-prywatności[106]

Definicje

Ponieważ Dyrektywa o e-prywatności została wyraźnie stworzona jako *lex specialis* do *lex generalis* Dyrektywy o ochronie danych z 1995 roku, zawarte w Dyrektywie o ochronie danych z 1995 roku **definicje związane z ochroną danych** miały także zastosowanie w odniesieniu do Dyrektywy o e-

[106] Wiele ze wspomnianych wymogów Dyrektywy o e-prywatności zostało już zawartych w Dyrektywie o ochronie danych w sektorze telekomunikacyjnym z 1997 roku i zostało po prostu przeniesionych do Dyrektywy o e-prywatności, przy czym nie będziemy o tym za każdym razem wspominać. W przypadku gdy zastosowano oznaczenie „*NOWY”, oznacza to, że wprowadzono coś, czego nie poruszono (jeszcze) w Dyrektywie o ochronie danych z 1995 roku.

prywatności, co zostało wyraźnie wskazane w art. 2, pierwsze zdanie, Dyrektywy o e-prywatności. Jednak w chwili obecnej, gdy Dyrektywę o ochronie danych z 1995 roku zastąpiono RODO, wszelkie odwołania do definicji w tej dyrektywie należy interpretować jako odwołania do odpowiednich definicji w rozporządzeniu (pod pewnymi względami zaktualizowanymi i wzmocnionymi). Wspomniano o tym w szczególności poniżej w osobnym punkcie zatytułowanym „*Zgoda*”[107].

Poza tym, **definicje bardziej technicznych zwrotów dotyczących łączności elektronicznej** w Dyrektywie w sprawie wspólnych ram regulacyjnych sieci i usług łączności elektronicznej[108], która powstała w wyniku wyżej wspomnianego przeglądu, w punkcie zatytułowanym „*Postanowienia ogólne*” - ***usługa łączności elektronicznej***[109]***, publicznie dostępne usługi łączności elektronicznej, publiczna sieć łączności*** itd. - mają także zastosowanie do odpowiednich zwrotów technicznych stosowanych w Dyrektywie o e-prywatności. Dotyczy to zwrotu „**abonent**” (usługi łączności elektronicznej).

Ponadto w art. 2 Dyrektywa o e-prywatności dodaje szereg *NOWY **dalszych (nowych) definicji**, takich jak „***użytkownik***”, „***dane o ruchu***”, „***dane dotyczące lokalizacji***”, „***usługa tworząca wartość dodaną***” oraz „***naruszenie ochrony danych osobowych***” (patrz art. 2).

*ZMIANA Zgoda

Najistotniejsza zmiana w definicjach podstawowych koncepcji w RODO w porównaniu do definicji zawartych w Dyrektywie o ochronie danych z 1995 roku dotyczy definicji „**zgody**” jako podstawy prawnej przetwarzania danych osobowych.

> W szczególności art. 2(f) Dyrektywy o e-prywatności przewiduje że „zgoda” użytkownika lub abonenta, w rozumieniu tej dyrektywy, odpowiada zgodzie osoby, której dane dotyczą, w Dyrektywie o ochronie danych. Ponieważ wszystkie odwołania do Dyrektywy o ochronie danych trzeba interpretować jako odwołania do RODO, zgodę wynikającą z Dyrektywy o e-prywatności należy w związku z tym rozumieć obecnie w taki sam sposób, jak zgodę wynikającą z RODO, w którym definiowana jest ona jako:
>
> 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 (art. 4, ust. 11 RODO).
>
> Ponadto RODO w bardziej szczegółowy sposób objaśnia warunki jakie muszą zostać spełnione celem uznania zgody za ważną i określa między innymi co oznacza, że zgoda jest udzielana dobrowolnie oraz co może stanowić wyraźne działanie potwierdzające[110]. Europejska Rada Ochrony Danych (EDPB) wydała ponadto wytyczne dotyczące zgody[111].

1.1 Wymagania dotyczące zgody w Dyrektywie o e-prywatności

> Kilka kluczowych postanowień Dyrektywy o e-prywatności wymaga zgody użytkownika lub abonenta. Są to:
>
> - art. 5.3 w sprawie przechowywania i gromadzenia informacji z terminala;
> - art. 6 i 9 w sprawie ponownego wykorzystania danych o ruchu i danych dotyczących lokalizacji w ramach usług przynoszących wartość dodaną dla celów wprowadzania do obrotu usług łączności elektronicznej;
> - art. 12 w sprawie spisów abonentów oraz
> - art. 13 w sprawie niezamówionych komunikatów.
>
> W wyżej wspomnianych sytuacjach zgoda, by była ważna musi być „zgodą na mocy RODO”. Wynikająca z RODO definicja zgody ma tutaj bezpośrednie zastosowanie. W tym kontekście państwa członkowskie

[107] RODO dodatkowo jeszcze wyjaśnia koncepcję „danych osobowych” poprzez uściślenie, że osoba może być także „możliwa do zidentyfikowania” poprzez „identyfikator internetowy” (art. 4(1) RODO, art. 2(a) Dyrektywy o ochronie danych z 1995 roku). Należy to obecnie także wziąć pod uwagę przy stosowaniu Dyrektywy o e-prywatności.

[108] Zob. przypis 97 powyżej.

[109] Zwrot ten omówiono powyżej w punkcie zatytułowanym *„Cel, przedmiot i zakres Dyrektywy o e-prywatności”.*

[110] Zob. art. 7 i 8 RODO i związane z nimi motywy: 32 – 33 oraz 42 – 43.

[111] Wytyczne EDPB dotyczące zgody na mocy rozporządzenia 2016/679 (wp259rev.01). Wytyczne te przyjęte zostały przez Grupę Roboczą Art. 29 (WP29) w dniu 28 listopada 2017 r. oraz zmienione 10 kwietnia 2018 r. Następnie zostały one zatwierdzone przez następczynię WP29: Europejską Radę Ochrony Danych (EDPB). Uzupełniają one uprzednią opinię WP29 w sprawie definicji zgody (WP187, opinia, 15/2011).

> muszą zweryfikować, czy prawo krajowe transponujące postanowienia Dyrektywy o e-prywatności i krajowe praktyki egzekwowania prawa są zgodne z RODO.

Powyższe sytuacje omówiono bardziej szczegółowo w punktach poniżej.

Bezpieczeństwo

Art. 4(1) skutecznie powtarza wymóg bezpieczeństwa danych przewidziany w Dyrektywie o ochronie danych z 1995 roku, przewidując, że dostawcy usług łączności elektronicznej muszą „***podjąć właściwe środki techniczne i organizacyjne w celu zapewnienia bezpieczeństwa oferowanych przez siebie usług****”,* dodając jednocześnie że *„jeśli to konieczne*", *„wraz z dostawcą publicznej sieci komunikacyjnej w odniesieniu do bezpieczeństwa sieci”.* Podobnie jak w głównej Dyrektywie dodano, że poziom bezpieczeństwa musi być „***odpowiedni do stopnia ryzyka***", uwzględniając najnowocześniejsze osiągnięcia techniczne oraz koszty ich wprowadzenia. Art. 4(1a), wprowadzony w Dyrektywie z 2009 roku, dodaje, że:

> Bez uszczerbku dla dyrektywy 95/46/WE środki, o których mowa w ust. 1, muszą co najmniej:
>
> - zapewniać, aby do danych osobowych mógł mieć dostęp wyłącznie uprawniony personel w dozwolonych prawem celach,
> - chronić przechowywane lub przekazywane dane osobowe przed przypadkowym lub bezprawnym zniszczeniem, przypadkową utratą lub zmianą oraz nieuprawnionym lub bezprawnym przechowywaniem, przetwarzaniem, dostępem lub ujawnieniem oraz
> - zapewnić wdrożenie polityki bezpieczeństwa w odniesieniu do przetwarzania danych osobowych.

Zarówno Dyrektywa o e-prywatności (w art. 4), jak i RODO (w art. 32 – 34) przewidują obowiązek zapewnienia bezpieczeństwa, a także obowiązek zgłaszania naruszenia ochrony danych osobowych[112] odpowiednio właściwemu organowi krajowemu i organowi nadzorczemu [tj. organowi ochrony danych][113]. Obowiązki te będą współistnieć równolegle w ramach dwóch różnych aktów prawnych zgodnie z ich odpowiednimi zakresami zastosowania. Zgodnie z art. 95 RODO rozporządzenie to nie nakłada dodatkowych obowiązków na osoby fizyczne i prawne w odniesieniu do spraw, które podlegają konkretnym obowiązkom określonym w Dyrektywie o e-prywatności. Jednak, jako *lex specialis* w stosunku do RODO, Dyrektywa o e-prywatności nie powinna [także] prowadzić do stosowania niższego poziomu ochrony niż poziom ochrony przewidziany w RODO.

Art. 4(1) przewiduje także, że:

> właściwe organy krajowe muszą być w stanie kontrolować środki przyjęte przez dostawcę publicznie dostępnych usług łączności elektronicznej oraz wydawać zalecenia dotyczące najlepszych praktyk dotyczących poziomu bezpieczeństwa, do jakiego środki te powinny prowadzić.

Należy zauważyć, że „właściwe organy" nie muszą oznaczać krajowych organów ochrony danych. Patrz punkt zatytułowany „*Nadzór i egzekwowanie prawa*" poniżej.

*NOWY Zgłaszanie ryzyka

Artykuł 4(2) Dyrektywy o e-prywatności przewiduje, że:

> w przypadku **szczególnego ryzyka naruszenia bezpieczeństwa sieci**, dostawca publicznie dostępnych usług łączności elektronicznej musi **poinformować** abonentów o zaistniałym ryzyku i, w przypadku gdy ryzyko wykracza poza zakres **środków zaradczych**, które może podjąć dostawca usług, włącznie z wynikającymi z nich ewentualnymi **kosztami** (dodano pogrubienie).

Wymóg „zgłoszenia ryzyka" (który uwzględniono już w pierwotnym tekście z 2002 roku) należy odróżnić od bardziej złożonych wymogów dotyczących „zgłaszania naruszania danych", które omówiono w kolejnym punkcie i które zostały dodane w wersji dyrektywy z 2009 roku oraz mają zastosowanie dopiero po wystąpieniu naruszenia, a art. 4(2) wymaga zgłoszenia każdego ryzyka *możliwości*

[112] Wymagania dotyczące zgłaszania naruszenia danych omówiono w odpowiednim punkcie w dalszej części Podręcznika.

[113] W celu uzyskania informacji na temat innych organów uczestniczących w procesie egzekwowania Dyrektywy o e-prywatności, zapoznaj się z kolejnym cytatem w niniejszym podpunkcie oraz zawartymi w nim uwagami, a także dyskusją w ostatnim punkcie tej części.

wystąpienia naruszenia.

*NOWY Zgłaszanie naruszenia danych

Dyrektywa o e-prywatności (ze zmianami z 2009 roku) przewiduje, że poza wyżej omówionym wymogiem „zgłoszenia ryzyka", dostawcy usług łączności elektroniczną muszą ***zawiadomić „właściwy organ krajowy"*** o - czytaj *każdym faktycznym* - naruszeniu ochrony danych osobowych „*bez zbędnej zwłoki*" (art. 4(3) pierwszy akapit - należy zauważyć, że i tym razem nie musi to być organ ochrony danych).

W przypadku gdy (i tylko wtedy gdy) „*naruszenie danych osobowych* ***może wywrzeć niekorzystny wpływ na dane osobowe lub prywatność abonenta lub osoby fizycznej"*** dostawca jest zobowiązany również zawiadomić „***o takim naruszeniu abonenta lub osobę fizyczną"*** *„bez zbędnej zwłoki"* (art. 4(3) drugi akapit). Jednak tego typu powiadomienie abonenta lub osoby fizycznej nie jest wymagane:

> jeżeli dostawca wykazał zgodnie z wymogami właściwego organu, że wdrożył odpowiednie technologiczne środki ochrony oraz że środki te zostały zastosowane do danych, których dotyczyło naruszenie bezpieczeństwa. Tego rodzaju technologiczne środki ochrony muszą sprawiać, że dane stają się nieczytelne dla każdego, kto nie jest uprawniony do dostępu do nich. (art. 4(3) trzeci akapit)

Innymi słowy, abonenci i inne odpowiednie osoby fizyczne (w szczególności oczywiście osoby, których dane dotyczą, ale także podmioty prawne będące abonentami) nie muszą być informowane o naruszeniu danych obejmującym ich dane, jeżeli dostawca może udowodnić „właściwemu organowi", że dane (w szczególności dane, które mogły zostać niewłaściwie ujawnione lub udostępnione stronom trzecim) zostały uczynione **zupełnie „nieczytelnymi"** dla każdego, kto mógł uzyskać dostęp w wyniku naruszenia, poprzez zastosowanie odpowiednich technologicznych środków ochrony (co objaśniono w art. 4 Rozporządzenia Komisji 611/2013)[114].

Odwrotnie, „właściwy organ" może „wymagać" od dostawcy powiadomienia odpowiednich abonentów i innych odpowiednich osób fizycznych o naruszeniu danych, jeżeli dostawca tego nie uczynił, tj. ponieważ organ ten nie zgadza się z oceną dostawcy, że naruszenie danych nie miało niekorzystnego wpływu na dane osobowe lub prywatność takich abonentów lub osób fizycznych, albo ponieważ organ ten nie wierzy, by ujawnione dane były faktycznie w pełni „nieczytelne" dla nieupoważnionych odbiorców (np. ponieważ klucz dekodujący został lub mógł zostać także ujawniony albo metoda szyfrowania nie była wystarczająco rzetelna)[115] (art. 4(3), czwarty akapit).

Ostatni, piąty akapit art. 4(3) przewiduje, że:

> Powiadomienie skierowane do abonenta lub osoby fizycznej zawiera co najmniej opis charakteru naruszenia ochrony danych osobowych oraz dane punktów kontaktowych, w których można uzyskać więcej informacji; zawiera ono także informacje o zalecanych środkach mających na celu złagodzenie ewentualnych niekorzystnych skutków tego naruszenia danych osobowych. Powiadomienie właściwego organu krajowego zawiera ponadto opis konsekwencji naruszenia danych osobowych i opis proponowanych lub podjętych przez dostawcę środków mających zaradzić naruszeniu.

Dyrektywa o e-prywatności zmieniona Dyrektywą z 2009 roku określa także istotne **formalne**

---

[114] Pełny tytuł: Rozporządzenie Komisji (UE) nr 611/2013 z 24 czerwca 2013 r. w sprawie środków mających zastosowanie przy powiadamianiu o przypadkach naruszenia danych osobowych, na mocy dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady o prywatności i łączności elektroniczne, OJ L 173 z 26.06.2013, str. 2 – 8: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32013R0611. Rozporządzenie Komisji przyjęto na podstawie art. 4(5) Dyrektywy o e-prywatności, która nadawała uprawnienia do podejmowania „technicznych środków wykonawczych dotyczących okoliczności, formatu i procedur mających zastosowanie do wymogów informacyjnych i zgłoszeniowych, o których mowa w niniejszym artykule" (art. 4(55), w konsultacji z ENISA, Grupą Roboczą Art. 29 oraz EDPS, a także z udziałem wszystkich (innych) zainteresowanych stron.

[115] Na przykład słabe algorytmy, takie jak MD5 lub SHA1, uznawane są za przestarzałe, a dane szyfrowane przy ich użyciu nie mogą być już traktowane jako naprawdę „nieczytelne" (czytaj: niemożliwe do odszyfrowania). Zob. https://www.owasp.org/index.php/Cryptographic_Storage_Cheat_Sheet. Możliwa jest także sytuacja, w której naruszono dane w ramach łączności elektronicznej, przez co treść komunikatów została w pełni odszyfrowana przy użyciu takich silnych algorytmów, jak SHA-256, bez odszyfrowania metadanych. Należy zauważyć, że (co wskazano na wyżej podanej stronie internetowej) „klasyfikacja „silnego" algorytmu kryptograficznego może z czasem ulec zmianie".

wymagania umożliwiające wypełnienie powyższych nowych postanowień. Tak więc:

> Właściwe organy krajowe muszą mieć również możliwość **kontrolowania**, czy dostawcy spełniają swoje obowiązki związane z powiadamianiem określone w niniejszym ustępie, oraz nakładają odpowiednie **kary** w przypadku niewykonywania tych obowiązków.
>
> (art. 4(4) pierwszy akapit, drugie zdanie, dodano podkreślenie)

Skuteczność tego typu uprawnień dotyczących kontroli (inspekcji) oraz kar wspiera dodatkowy wymóg określony w drugim akapicie art. 4(4):

> Dostawcy prowadzą **rejestr naruszeń ochrony danych osobowych**, w tym faktów towarzyszących naruszeniom, ich skutków i podjętych działań naprawczych; rejestr ten musi być wystarczający, tak aby umożliwić właściwemu organowi krajowemu sprawdzenie zgodności z przepisami ust. 3. Rejestr zawiera wyłącznie informacje niezbędne do realizacji tego celu. (dodano podkreślenie)

Zmieniona Dyrektywa o e-prywatności przewiduje wydawanie „**wytycznych**" i „**instrukcji**" przez „właściwe organy krajowe" dotyczących „*okoliczności, w których dostawcy zobowiązani są do powiadamiania o naruszeniu danych osobowych, a także dotyczących form takiego powiadomienia oraz sposobu, w jaki ma być dokonane takie powiadomienie*" (art. 4(4) pierwszy akapit, pierwsze zdanie).

Wymagania zawarte w Dyrektywie o e-prywatności dotyczące zgłaszania naruszenia danych, ograniczone zakresem dyrektywy, zapowiadają bardziej ogólne wymogi dotyczące zgłaszania naruszenia danych, obecnie uwzględnione w Ogólnym rozporządzeniu o ochronie danych, które mają zastosowanie do każdej operacji przetwarzania danych osobowych i które omówiono poniżej w części 2, pkt 2.1. Można traktować je jako „zbędne"[116].

Specjalne wymagania dotyczące przetwarzania w konkretnych celach:

Zamiast powtarzać określone w głównej Dyrektywie o ochronie danych z 1995 roku ogólne zasady ochrony danych i listę podstaw legalnego przetwarzania, Dyrektywa o e-prywatności przewiduje ogólny wymóg poufności komunikacji oraz szereg konkretnych wymogów i warunków dotyczących określonych konkretnych danych lub operacji przetwarzania. Dyrektywa o e-prywatności dąży do stosowania zasad i praw przewidzianych w Dyrektywie o ochronie danych z 1995 roku w stosunku do tego typu konkretnych spraw w celu harmonizacji stosowania tego typu zasad i praw w państwach członkowskich, co zostało omówione w różnych punktach poniżej.

Po pierwsze jednak należy przypomnieć, że w zakresie w jakim Dyrektywa o e-prywatności określa konkretne podstawy prawne przetwarzania w konkretnych celach (także w niej określonych), bardziej ogólne podstawy prawne przetwarzania w różnych celach określonych w art. 5 i 6 RODO nie mają zastosowania[117]***.***

Tak więc tam, gdzie Dyrektywa o e-prywatności wymaga zgody - w odniesieniu do dostępu do informacji na urządzeniach (art. 5(3)) albo wysyłania niezamówionych komunikatów (art. 13) - lub określa zakres szczególnych podstaw prawnych i celów przetwarzania - w odniesieniu na przykład do przetwarzania danych o ruchu (art. 6) - podmiot, który takim zasadom podlega - w odniesieniu do art. 5(3) i 13 jest to każdy podmiot, a w odniesieniu do art. 6 są to dostawcy usług łączności elektronicznej - nie może polegać na żadnych innych podstawach ani zasadach określonych w RODO. W szczególności nie może on polegać na podstawach przetwarzania opartych na „zgodnych celach", o których mowa w art. 5(1)(b) RODO.

*NOWY ***Poufność komunikatów:***

Art. 5(1) Dyrektywy o e-prywatności podkreśla fundamentalne znaczenie poufności komunikatów, na którą nacisk kładzie wiele konstytucji, przynajmniej w odniesieniu do poczty i rozmów telefonicznych (chociaż zapis ten często jest obecnie wyraźnie lub w ramach interpretacji poszerzany o wszystkie formy

[116] Komisja Europejska, REFIT analysis of coherence of the e-Privacy Directive with the GDPR (Wykres – uwaga na temat art. 4.3, 4.4, 4.5 – Zgłaszanie naruszenia ochrony danych osobowych).
[117] Zob. podrozdział dotyczący „*Związku pomiędzy Dyrektywą o e-prywatności a RODO*" powyżej.

komunikacji)[118], przewidując, że państwa członkowskie muszą:

> zapewnić **poufność komunikacji i związanych z nią danych o ruchu** za pośrednictwem publicznie dostępnej sieci łączności i publicznie dostępnych usług łączności elektronicznej poprzez ustawodawstwo krajowe. W szczególności ***powinny zakazać słuchania, nagrywania, przechowywania lub innych rodzajów przejęcia lub nadzoru komunikatu i związanych z nim danych o ruchu przez osoby inne niż użytkownicy***, bez **zgody** zainteresowanych użytkowników, z wyjątkiem upoważnienia ... (dodano pogrubienie).

Jak wyjaśniają to zwroty „*słuchania, nagrywania [itp.] ... przez osoby inne niż użytkownicy*", postanowienie to nie ma zastosowania do dostawców usług łączności elektronicznej. Państwa członkowskie (z zastrzeżeniem poniższych odstępstw) muszą raczej - zgodnie z prawem krajowym - zakazać tego typu interwencji w prawo do poufności komunikatów **każdej osobie**, w tym zarówno agencjom państwowym, jak i podmiotom prywatnym, takim jak spółki.

Art. 5(1) wyjątkowo zezwala na „*techniczne przechowywanie, które jest niezbędne do przekazania komunikatu bez uszczerbku dla zasady poufności*". Kolejne odstępstwo przewiduje art. 5(2) w odniesieniu do rejestrowania komunikatów i danych o ruchu do celów zapewnienia dowodów transakcji handlowej lub łączności w działalności handlowej. Tak zwana Dyrektywa o zatrzymywaniu danych, którą krótko omówiono w pkt. 1.3.4 poniżej, przewidywała dodatkowe, ogólnikowe i obowiązkowe odstępstwo od zakazu przechwytywania i gromadzenia danych o łączności, ale została unieważniona przez Trybunał Sprawiedliwości, co zostało omówione w wyżej wskazanym punkcie.

> *NOWE ***Stosowanie plików cookies i innych inwazyjnych technologii:***

Zmieniona Dyrektywa o e-prywatności w art. 5(3) przewiduje, stosując dość techniczne sformułowania, że państwa członkowskie muszą zapewnić, by:

> **przechowywanie informacji lub uzyskanie dostępu do informacji przechowanej na terminalu abonenta lub użytkownika** było dozwolone wyłącznie pod warunkiem, że abonent lub użytkownik wyrazi **zgodę** po uzyskaniu **jasnej i wyczerpującej informacji** zgodnie z Dyrektywą 95/46/WE, w tym między innymi o celach przetwarzania.

Dyrektywa wyjaśnia w kolejnym zdaniu tego paragrafu, że:

> Nie stanowi to przeszkody dla technicznego przechowywania danych lub dostępu do danych jedynie w celu wykonania transmisji komunikatu za pośrednictwem sieci łączności elektronicznej lub gdy jest to szczególnie niezbędne dla dostawcy usługi społeczeństwa informacyjnego, wyraźnie zażądanej przez abonenta lub użytkownika w celu wykonania usługi.

Należy zauważyć, że zwroty „*jedynie w celu*" oraz „*gdy jest to szczególnie niezbędne*" podkreślają, że odstępstwo to należy stosować w bardzo wąskim zakresie.

Zwrot „*przechowywanie informacji lub uzyskanie dostępu do informacji przechowanej na terminalu abonenta lub użytkownika"* stosuje język techniczny na określenie technologii, które pozwalają na rozpoznanie odwiedzającego stronę internetową przez tę stronę oraz śledzenie go w trakcie korzystania z tej strony lub nawet stron internetowych. Głównym środkiem służącym temu celowi są tak zwane pliki „**cookies**" – to właśnie dlatego Dyrektywa z 2009 roku, która wzmocniła zasady w tym zakresie (jak omówiono poniżej), była wstępnie (i czasami w dalszym ciągu jest) ogólnie nazywana w unijnym „**prawem dotyczącym plików cookies**" (jak czyni to, na przykład, należąca do podmiotu prywatnego strona internetowa dotycząca tej kwestii[119]).

W rzeczywistości istnieje szereg plików cookies wynikających z zestandaryzowanych międzynarodowych narzędzi zwanych „RFC", przyjętych przez Grupę Zadaniową Inżynierii Internetu (Internet Engineering Task Force, IETF), które w języku potocznym mogą zostać nazwane jako obejmujące swoim zakresem od wysoce inwazyjnych „**śledzących pliki cookies stron trzecich**" po **nieinwazyjne**, które poprawiają

[118] Zob. szeroka interpretacja koncepcji „korespondencji" w art. 8 ETPC Europejskiego Trybunału Praw Człowieka w słynnej sprawie *Klass przeciwko Republice Federalnej Niemiec* (wyrok z 6 września 1978 r.) par. 41, w którym Trybunał uznał, że „*rozmowy telefoniczne … są kwestią <życia prywatnego> i <korespondencji> [w tym artykule]*".
[119] Zob. np. https://www.cookielaw.org/the-cookie-law/.

korzystanie ze stron internetowych bez śledzenia odwiedzających je użytkowników[120]; istnieją także inne inwazyjne technologie, takie jak „**flash cookies**", **metody przechowywania HTML5** oraz tak zwane „**evercookies**"[121]. Wszystkie z tych plików i technologii mieszczą się w definicji „*informacji przechowywanych w terminalu*" i tym samym (co jest trochę problematycznie) są zgodnie z Dyrektywą o e-prywatności traktowane tak samo[122].

Cel i znaczenie art. 5(3) objaśniono prostszym językiem w motywach (24) i (25) do Dyrektywy o e-prywatności, które wyjaśniają, że postanowienie to obejmuje znacznie więcej niż tylko pliki cookies. Warto więc przytoczyć te zapisy w całości:

> Wyposażenie terminali użytkowników sieci łączności elektronicznej oraz informacje przechowywane na tych urządzeniach stanowią część prywatnej sfery użytkowników podlegającej ochronie na mocy Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności. Programy określane mianem **spyware, błędy sieciowe, ukryte identyfikatory i inne podobne narzędzia mogą się znaleźć w terminalu użytkownika bez jego wiedzy w celu uzyskania dostępu do informacji, przechowania ukrytych informacji lub śledzenia czynności użytkownika i mogą w poważny sposób naruszyć jego prywatność**. **Stosowanie takich narzędzi powinno być dozwolone wyłącznie dla uzasadnionych celów, po powiadomieniu zainteresowanych użytkowników.** (pogrubienie dodane przez autorów Podręcznika)
>
> Jednakże takie narzędzia, **jak na przykład tak zwane „cookies"** stanowią prawnie dopuszczalne i użyteczne narzędzie, na przykład, w analizowaniu skuteczności projektu strony internetowej i reklamy oraz w sprawdzaniu tożsamości użytkowników prowadzących transakcje w systemie on-line. W przypadku gdy takie narzędzia, na przykład „cookies", są przeznaczone do prawnie dopuszczalnych celów, takich jak ułatwienie dostarczania usług społeczeństwa informacyjnego, ich wykorzystywanie powinno być dozwolone pod warunkiem że użytkownicy otrzymają wyraźną i dokładną informację zgodnie z dyrektywą 95/46/WE o celu „cookies" lub podobnego narzędzia w celu zapewnienia, że użytkownicy zostali zapoznani z informacją umieszczaną na użytkowanym przez nich terminalu. Użytkownicy powinni mieć możliwość odmówienia przechowywania „cookies" lub podobnego narzędzia w ich terminalu. Jest to szczególnie ważne w przypadku, gdy użytkownicy inni niż użytkownik początkowy mają dostęp do terminali, a przez to do danych zawierających informacje szczególnie chronione ze względu na prywatność i przechowywane na tym urządzeniu. Informacja i prawo do odmowy mogą być oferowane jednorazowo dla różnego rodzaju narzędzi instalowanych w terminalu użytkownika w czasie tego samego połączenia oraz mogą obejmować wszelkie dalsze korzystanie z tych narzędzi w trakcie kolejnych połączeń. Metody udostępniania informacji oferujące prawo do odmowy[123] lub wymagające zgody, powinny być jak najbardziej przyjazne dla użytkownika. Dostęp do niektórych treści zamieszczonych na stronach internetowych może być nadal uzależniony od świadomej akceptacji zastosowania „cookie" lub podobnego urządzenia, jeżeli służy ono prawnie dopuszczalnemu celowi. (pogrubienie dodane przez autorów Podręcznika).

Główna zmiana wprowadzona dyrektywą z 2002 roku polegała na tym, że zmieniono system obejmujący wykorzystanie technologii z takiego, w którym abonent lub użytkownik musiał zostać poinformowany i należało mu przyznać „prawo do odmówienia" w odniesieniu do plików cookies (itp.)[124], na obecny

---

[120] Zob. rekomendacje IETF na temat cookies (począwszy od RFC 2109 z 1997 roku), które zawierają przykładową koncepcję prywatności, ale także pewne przydatne obowiązkowe dane w ramach cookies. https://tools.ietf.org/html/rfc2109 (oryginał RFC 2109); https://tools.ietf.org/html/rfc2965 (RFC 2965, zastępująca RFC 2109, ale zachowująca ten sam spis danych) oraz https://tools.ietf.org/html/rfc6265 (RFC 6265 z 2011 r. ponownie zachowująca pierwotny spis, z uwzględnieniem jednak wprowadzenia dostępu stron trzecich do plików cookies - aktualnie obowiązująca rekomendacja). Patrz: strona na Wikipedii: https://en.wikipedia.org/wiki/HTTP_cookie. Angielska wersja strony zawiera wiele szczegółów na temat różnych rodzajów plików cookie: sesyjnych, trwałych, bezpiecznych, jedynie HTTP, tej samej strony, stron trzecich, super i zombie, a także podaje szczegółowe informacje techniczne.

[121] Zob. https://webcookies.org/doc/eu-web-cookies-directive.

[122] Może to ulec zmianie w ramach proponowanego nowego Rozporządzenia o e-prywatności, które mogłoby w odmienny sposób traktować różne technologie w zależności od ich względnej inwazyjności.

[123] By uzyskać informacje na temat zachowania możliwości skorzystania z prawa do odmowy, patrz kolejne dwa przypisy.

[124] Wersja oryginalna z 2002 roku, pierwsze zdanie art. 5(3):

> *Państwa członkowskie zapewniają, że korzystanie z sieci łączności elektronicznej w celu przechowywania informacji lub uzyskania dostępu do informacji przechowanej na terminalu abonenta lub użytkownika jest dozwolone wyłącznie pod warunkiem że abonent lub użytkownik otrzyma wyczerpującą **informację** zgodnie z dyrektywą 95/46/WE, między innymi o celach przetwarzania, oraz zostanie zaoferowane mu **prawo do niewyrażenia** zgody na takie przetwarzanie przez administratora danych.* (pogrubienie dodano)

system przewidziany w art. 5(3), w którym pliki cookies są dopuszczalne, pod warunkiem, że abonent lub użytkownik został nie tylko poinformowany, ale także udzielił swojej **twierdzącej, wyraźnej zgody** na warunkach dotyczących (ważnej) zgody określonych w głównej Dyrektywie o ochronie danych z 1995 roku[125], która definiowała zgodę jako:

> każde konkretne i świadome, dobrowolne wskazanie przez osobę, której dane dotyczą, na to, że wyraża przyzwolenie na przetwarzanie odnoszących się do niej danych osobowych (art. 2(h)).

Jednak biorąc pod uwagę fakt, że Dyrektywa z 1995 roku została zastąpiona RODO, pojawia się pytanie, czy należy teraz przyjąć, że konieczna jest **bardziej wymagająca forma przewidzianej w Rozporządzeniu zgody.** Jeżeli tak jest, zgoda na umieszczenie plików cookies oraz innych narzędzi tego typu powinna być obecnie oparta na:

> dobrowolnym, konkretnym, świadomym i **jednoznacznym** okazaniu woli, którym [abonent lub użytkownik], **w formie oświadczenia lub wyraźnego działania potwierdzającego**, przyzwala na [umieszczenie plików cookies lub wykorzystanie innych narzędzi][126]

Powinno to oznaczać, że stosowanie „z góry zaznaczanych" pól w odniesieniu do stosowania plików cookies, itp. nie spełnia już wymogów zgody przewidzianych w Dyrektywie o e-prywatności.

Istnieje jednak w dalszym ciągu kwestia dotycząca tego, że Dyrektywa o e-prywatności z zasady traktuje wszystkie pliki „cookies" i narzędzia śledzące w podobny sposób, nie rozróżniając ich na przykład na „cookies sesyjne" i „cookies stałe".

W praktyce postanowienie to wprowadziło w Internecie kulturę „bierz to lub odrzuć" (ang. „take it or leave it"), gdzie osoby odwiedzające stronę internetową zostały faktycznie zmuszone do wyboru opcji „Zgadzam się" (na umieszczenie zazwyczaj nieokreślonych rodzajów cookies), by uzyskać dostęp do strony (nawet w przypadku stron publicznych). W Badaniu SMART ustalono, że[127]:

> zasady dotyczące plików cookies i podobnych technologii mogły nie osiągnąć swojego celu, biorąc pod uwagę fakt, że użytkownicy otrzymują zbyt wiele komunikatów ostrzegających, których nie traktują we właściwy sposób.

Okaże się jeszcze, czy ta sytuacja ulegnie zmianie dzięki nowemu rozporządzeniu o e-Prywatności – jednakże poruszone kwestie w sposób oczywisty odnoszą się bezpośrednio do stosowania podstawowych zasad i praw w zakresie ochrony danych – łącznie z ograniczeniem celu, minimalizacją danych, ograniczeniem zatrzymywania danych, itd. Na przykład odnośnie kwestii takich jak okresy zatrzymywania danych odpowiednie dla różnych typów plików cookies (w zależności od ich przeznaczenia)[128], tego w jaki sposób odpowiednia zgoda (zgoda w rozumieniu RODO) winna być pozyskiwana celem użytkowania różnych rodzajów plików cookies oraz tego, jak osoby, których dane dotyczą, mogą wykonywać przysługujące im prawa, itd. – i w jaki sposób te kwestie mogą i powinny być wdrażane na podstawie zasad uwzględniania ochrony danych w fazie projektowania i domyślnej ochrony danych – zasady obecnie wyraźnie zapisanej w RODO.

*NOWE ***Ograniczenia dotyczące wykorzystania danych o ruchu i danych dotyczących lokalizacji:***

Art. 6 Dyrektywy o e-prywatności nakłada ostre ograniczenia dotyczące danych oraz ograniczenia dotyczące przetwarzania danych o ruchu i lokalizacji przez dostawców usług łączności elektronicznej. Z zasady, **dane o ruchu** (tj. dane przetwarzane i niezbędne do celów przekazywania komunikatu lub naliczania opłat za te usługi) mogą być przetwarzane i przechowywane wyłącznie przez dostawcę odpowiedniej usługi łączności elektronicznej dla celów ***transmisji*** komunikatów elektronicznych, ***naliczania opłat*** abonenta za łączność lub umożliwienia ***rozliczeń międzyoperatorskich*** (tj. płatności pomiędzy dostawcami z tytułu wzajemnego użytkowania sieci) (art. 6(1) i 6(2)). Przetwarzanie takie nie wymaga zgody abonenta ani użytkownika usługi, ponieważ jest wymagane w związku z jej wykonaniem.

---

[125] Zmiana ta nie znalazła odzwierciedlenia w motywach cytowanych w tekście, które nie zostały zmienione w porównaniu do oryginalnej Dyrektywy z 2002 roku i w dalszym ciągu nawiązują do „prawa do niewyrażenia", mimo że w Dyrektywie z 2009 roku zostało ono usunięte. W efekcie zwroty te stały się martwe.

[126] Zob. art. 4(11) RODO. Pogrubienie dodano.

[127] Zob. przypis powyżej).

[128] Niektóre strony internetowe określają okres zatrzymywania danych na 25 lat, co jest w sposób oczywisty nadmierne, bez względu na cel.

Gdy dane te nie są już potrzebne do celów wyżej wspomnianych usług, muszą zostać „usunięte lub uczynione anonimowymi" (art. 6(1))[129].

Dane o ruchu mogą być jedynie wykorzystywane do ***marketingu usług łączności elektronicznej*** lub w celu świadczenia ***usług tworzących wartość dodaną*** wyłącznie za **zgodą** abonenta lub użytkownika. Ponownie, oznacza to obecnie, że RODO ma pełne zastosowanie, należy przestrzegać wymogów RODO dotyczących ważnej zgody, tj. że odpowiednia zgoda musi zostać wydana w formie:

> dobrowolnego, konkretnego, świadomego i jednoznacznego okazania woli, którym [abonent lub użytkownik], w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na [wykorzystanie jego danych o ruchu w celach marketingowych przez dostawców usług łączności elektronicznej lub w celu świadczenia konkretnych usług tworzących wartość dodaną].

Dyrektywa o e-prywatności przewiduje również, że dostawca usług musi poinformować abonenta lub użytkownika swoich usług o rodzajach danych o ruchu, które są przetwarzane, oraz o okresie tego przetwarzania, a dla celów przetwarzania w oparciu o zgodę (tj. marketingu i usług tworzących wartość dodaną - patrz powyżej), informacje takie należy przekazać przed uzyskaniem takiej zgody (art. 6(4)).

W rezultacie Dyrektywa o e-prywatności przewiduje, że przetwarzanie danych o ruchu przez dostawcę usług łączności elektronicznej dla różnych **pomocniczych celów** związanych ze świadczeniem takich usług (***naliczanie opłat, zarządzanie ruchem, obsługa klienta, wykrywanie nadużyć finansowych, marketing i świadczenie usług tworzących wartość dodaną***) przez pracowników dostawcy lub pracowników przetwarzającego zatrudnionego przez dostawcę musi być **ograniczone zgodnie z zasadą „koniecznego dostępu"**, tj. każda z tych osób powinna uzyskać dostęp do danych o ruchu wyłącznie, wtedy, gdy jest to potrzebne do wykonania konkretnego zadania (art. 6(5)). Jednak „właściwe organy" [zewnętrzne]", takie jak organy rozstrzygające spory dotyczące rozliczeń lub płatności międzyoperatorskich, muszą oczywiście uzyskać dostęp do danych o ruchu w razie potrzeby (art. 6(6)).

Dyrektywa o e-prywatności wprowadza jeszcze ostrzejsze zapisy w odniesieniu do przetwarzania „**danych dotyczących lokalizacji innych niż dane o ruchu**", tj. danych przetwarzanych w sieci łączności elektronicznej, która wskazuje ***położenie geograficzne urządzenia końcowego użytkownika*** (jako takie, z reguły - telefon komórkowy), które ***nie są przetwarzane dla celów łączności elektronicznej lub w celu naliczania opłat z tego tytułu***. Takie dane mogą być przetwarzane wyłącznie wtedy, gdy uczyniono je ***anonimowymi***[130] lub w zakresie, w jakim mogą być wykorzystywane do świadczenia ***usług tworzących wartość dodaną*** za **zgodą** użytkowników lub abonentów takiej usługi (art. 9(1), pierwsze zdanie). Dostawca usług łączności elektronicznej ponownie musi **poinformować** użytkowników i abonentów o szczegółach przetwarzania przed uzyskaniem ich zgody (*idem,* drugie zdanie). Użytkownicy i abonenci powinni ponadto być w stanie odwołać swoją zgodę w dowolnym momencie (*idem,* trzecie zdanie) i/lub tymczasowo odłączyć śledzenie danej lokalizacji „w sposób prosty i wolny od opłat" (art. 9(2)). I ponownie przetwarzanie musi być ograniczone do pracowników dostawcy usług łączności elektronicznej lub pracowników dostawcy odpowiednich usług tworzących wartość dodaną (lub zatrudnionego przez nich przetwarzającego) (art. 9(3)).

*NOWE *Szczegółowe wykazy połączeń*

Abonenci muszą mieć prawo do otrzymywania **rachunków, które nie są szczegółowe** (art. 8(1)), a państwa członkowskie powinny także zapewnić **alternatywne, gwarantujące prywatność metody** dotyczące szczegółowych wykazów połączeń (art. 8(2), np. szczegółowe wykazy połączeń prezentujące jedynie kody kraju lub kody regionalne połączeń wychodzących), lub pomijać albo zasłaniać trzy ostatnie cyfry wybieranego numeru, by zapewnić zarówno prezentację fakturowanej kwoty, jak i ochronę prywatności użytkownika (który niekoniecznie jest abonentem albo członkiem rodziny).

*NOWE *Dzwonienie, identyfikacja i automatyczne przekazywanie rozmów*

Dostawcy usług łączności elektronicznej muszą oferować zarówno użytkownikowi wybierającemu, jak i odbierającemu połączenie (z uwzględnieniem użytkowników z UE [wcześniej WE] wykonujących

[129] W celu uzyskania informacji na temat problemów związanych z anonimizacją tego typu danych, patrz dyskusja w kontekście RODO w części drugiej, pkt 2.1.
[130] Zob. poprzedni przypis.

połączenie do krajów trzecich) **możliwość zablokowania wyświetlania identyfikacji rozmów przez odbiorcę połączenia**, ale osoby odbierające połączenie z niezidentyfikowanego numeru (z lub spoza UE/WE) muszą być w stanie **zablokować** połączenie, natomiast każdy musi za każdym razem mieć możliwość **wyłączenia** identyfikacji swojej własnej linii (art. 8(1) – (4)).

Dostawcy usług łączności elektronicznej muszą ponadto **podać tego typu możliwości do wiadomości publicznej** (i oczywiście w szczególności poinformować o nich swoich abonentów i użytkowników) (art. 8(6))[131].

Z zastrzeżeniem odpowiednich przepisów krajowych (oraz oczywiście ogólnych zasad konieczności i proporcjonalności, dostawcy usług łączności elektronicznej mogą **pominąć zablokowanie** wyświetlania identyfikacji rozmów przychodzących na wniosek abonenta ***w celu prześledzenia dokuczliwych lub złośliwych telefonów*** *(*by umożliwić dochodzenie reklamacji przez dostawców oraz policję, a także w celu dostarczenia dowodów w sprawach sądowych) lub udzielić wsparcia pogotowiu ratunkowemu i straży pożarnej ***do celów odpowiadania na połączenia alarmowe*** (art. 10(1) i (2)).

Abonent musi mieć także *„możliwość **zablokowania** w sposób prosty i wolny od opłat **automatycznego przekazywania połączeń** przez stronę trzecią do terminalu tego abonenta*" (art. 11).

Wszystkie powyższe opcje o charakterze obowiązkowym zostały wprowadzone do międzynarodowych norm technicznych, zatem mogą być w łatwy sposób stosowane praktycznie względem smartfonów, itd.

*NOWE ***Spisy abonentów***

W wyniku nacisków ze strony krajowych organów ochrony danych Dyrektywa o e-prywatności zawiera postanowienia, na mocy których abonenci muszą zostać poinformowani o zamiarze umieszczenia ich danych (tj. numeru telefonu stacjonarnego lub komórkowego) w ***spisie abonentów publicznie dostępnym lub uzyskiwanych w telefonicznej informacji o numerach*** oraz muszą być w stanie wycofać się z takich spisów (tj. „**wypisać się ze spisu”**) w sposób wolny od opłat oraz bez podawania przyczyny (art. 12(1) i (2))[132].

Prawa te stosuje się do abonentów będących osobami fizycznymi, ale państwa członkowskie muszą zapewnić również, że „uzasadnione interesy abonentów innych niż osoby fizyczne [tj. osoby prawne, takie jak spółki]" także „posiadają wystarczającą ochronę" (art. 12(4)).

Jeżeli spis ma być wykorzystywany dla *„**jakiegokolwiek celu ... innego niż przeszukiwanie danych do kontaktu** osób, na podstawie podania ich nazwiska oraz, w miarę potrzeb, minimalnej ilości innych danych identyfikacyjnych”*, np. jeżeli dane takie mają być wykorzystane dla celów ***marketingu bezpośredniego, oceny kredytowej*** [133] lub ***kampanii politycznej,*** abonenci muszą zostać poproszeni o **dodatkową zgodę** wyraźnie dotyczącą wykorzystania ich danych w tego typu innych celach (art.

[131] Opcje takie zostały pierwotnie opracowane przez krajowe organy ochrony danych. Co interesujące, opcje te - w przeciwieństwie do technicznych standardów dotyczących plików cookies - jak tylko usługi „identyfikacji dzwoniącego” itp. zostały wprowadzone na rynek w latach 80-tych XX wieku, zostały one zintegrowane w ramach międzynarodowych standardów technicznych dotyczących przekazywania transmisji telekomunikacyjnych (staromodne linie stacjonarne), a gdy pojawiły się telefony komórkowe, w ramach telefonów komórkowych umożliwiających aktywację wyżej wspomnianych opcji. Było to możliwe dzięki organom nadzoru we Francji i Niemczech, które poruszyły tego typu kwestie z negocjatorami telekomunikacyjnymi w Europie, którzy następnie naciskali na wprowadzenie kompletnego i łatwego w użyciu rozwiązania na poziomie globalnym poprzez normy GSM.

[132] Prowadzona przez organy ochrony danych bitwa o tego typu zabezpieczenia miała miejsce przed przyjęciem Dyrektywy telekomunikacyjnej z 1997 roku. W Niemczech skoncentrowano się na braku konieczności podawania powodu wykreślenia ze spisu numerów telefonów. We Francji główną kwestią było postanowienie, że wykreślenie takie powinno być darmowe. Tylko z tego powodu w czasie negocjacji w sprawie Dyrektywy telekomunikacyjnej Francja niemalże doprowadziła do odrzucenia całej dyrektywy. W rzeczywistości brak wpisu w spisie numerów telefonów prowadził w ówczesnych czasach do mniejszej liczby komunikatów, a tym samym mniejszych zysków operatorów telekomunikacyjnych, gdyż każda rozmowa telefoniczna była płatna, podczas gdy 20% abonentów wnioskowało o niewpisywanie ich numeru telefonu do spisu. Obecnie, w dobie internetu bardziej istotne jest, by użytkownicy nie byli nękani telefonami, jeżeli ich numery telefonu zostaną opublikowane.

[133] Zob. „**red-lining**” - praktyka różnego traktowania w ramach usług kredytowych, mieszkaniowych, ubezpieczeniowych i innych w zależności od adresu osoby oraz historii naruszeń w danym obszarze - praktyka ta została uznana za nielegalną w USA wiele lat temu. Zob. np. https://www.investopedia.com/terms/r/redlining.asp, także: *How Redlining's Racist Effects Lasted for Decades*, NY Times, 24 sierpnia 2017 r. https://www.nytimes.com/2017/08/24/upshot/how-redlinings-racist-effects-lasted-for-decades.html (wraz z mapami ilustrującymi tą praktykę).

12(3))[134].

*NOWE ***Komunikaty niezamówione***

Jak wspomniano w art. 1.3.2 powyżej, Dyrektywa o ochronie danych z 1995 roku daje już osobom, których dane dotyczą, bezwarunkowe **prawo sprzeciwu** wobec wykorzystywania którychkolwiek z ich danych osobowych dla celów marketingu bezpośredniego (art. 14(b) Dyrektywy z 1995 roku), tj. wszelkiego rodzaju marketingu handlowego, politycznego itp. Ówcześnie chodziło w dalszym ciągu głównie o marketing drogą pocztową. Dyrektywa o e-prywatności dodaje do tego wymóg uzyskania w tym celu **uprzedniej zgody** na stosowanie ***automatycznych systemów wywołujących bez ludzkiej ingerencji i faksów***[135] lub ***poczty elektronicznej*** (art. 13(1)). Wynika to z faktu, że wysyłanie komunikatów tą drogą jest znacznie tańsze niż tradycyjna poczta, a tym samym najprawdopodobniej będzie coraz powszechniej stosowane. Wymóg ten ma zastosowanie zarówno do osób fizycznych, jak i prawnych (jednostek i spółek itp.). Ponadto, co zauważono już wcześniej w punkcie zatytułowanym „*Cel, przedmiot i zakres Dyrektywy o e-prywatności*", postanowienie to ma zastosowanie do **każdego podmiotu**, który chce korzystać z tego typu środków, by wysyłać komunikaty w ramach marketingu bezpośredniego.

Jednak gdy klient przekazuje szczegółowe elektroniczne dane kontaktowe (numer telefonu lub adresy e-mail, itp.) spółce w kontekście sprzedaży produktu lub usługi, sprzedający może używać tych szczegółowych danych na potrzeby **wprowadzania na rynek swoich własnych produktów podobnych lub usług** dla tego klienta (tak zwany ***„proximity marketing***"), pod warunkiem że klientowi zaoferowano łatwy sposób sprzeciwienia się tego typu podejściu w każdym komunikacie (tj. pod warunkiem że zaoferowano mu możliwość ***rezygnacji*** (opt-out) z dalszego marketingu w każdym komunikacie) (art. 13(2)).

W przypadku innych form marketingu bezpośredniego (tj. marketingu innego niż marketing bezpośredni wykorzystujący inne środki inne niż automatyczne dzwonienie lub faks lub e-mail) państwa członkowskie mogą **wybrać** pomiędzy uprzednią zgodą (tj. ***możliwością akceptacji*** (opt-in), która jest oferowana w momencie gromadzenia danych osobowych) a modelem ***rezygnacji*** (opt-out) („poinformowany, ale nie wyraża sprzeciwu") (art. 13(3))[136]. Jednak w każdym przypadku zakazana jest praktyka wysyłania poczty elektronicznej do celów marketingu bezpośredniego „*zmieniająca lub zatajająca tożsamość nadawcy, w imieniu którego wysyłany jest komunikat lub bez aktualnego adresu, na który odbiorca może wysłać wniosek o zaprzestanie takich komunikatów*" (art. 13(4)).

Odstępstwa

Art. 15 Dyrektywy o e-prywatności wyjaśnia, że państwa członkowskie mogą ograniczyć różne prawa i obowiązki przewidziane dyrektywą na takiej samej podstawie, jak w przypadku szerokiej, przewidzianej w głównej Dyrektywie o ochronie danych z 1995 roku klauzuli derogacyjnej opartej na „**istotnych interesach publicznych**" (art. 13), tj. „gdy takie ograniczenia stanowią środki niezbędne, właściwe i proporcjonalne w ramach społeczeństwa demokratycznego do zapewnienia ***bezpieczeństwa narodowego*** (i.e. bezpieczeństwa państwa), ***obronności, bezpieczeństwa publicznego oraz zapobiegania, dochodzenia, wykrywania i karania przestępstw kryminalnych***" , do czego Dyrektywa o e-prywatności dodaje jedynie „lub ***niedozwolonego używania systemów łączności elektronicznej***". Podkreślone zwroty zostały wzmocnione w Dyrektywie o e-prywatności poprzez dodatkowy wyraźny zapis, że: Podkreślone zwroty zostały wzmocnione w Dyrektywie o e-prywatności poprzez dodatkowy wyraźny zapis, że:

> *„Wszystkie środki określone w niniejszym ustępie są zgodne z ogólnymi zasadami prawa wspólnotowego, w tym zasadami określonymi w art. 6 ust. 1 i 2 Traktatu o Unii Europejskiej"*

[134] Pozostaje kwestia, czy dotyczy to także „osób prawnych", ponieważ paragraf ten nie został wspomniany w czwartym paragrafie art. 12.

[135] Faks to urządzenie umożliwiające przesyłanie wizerunku (często wizerunku dokumentu) poprzez sieć telefoniczną. Obecnie jest rzadko stosowane. Zob. https://faxauthority.com/fax-history/.

[136] Unijny model rezygnacji („opt-out") wymaga poinformowania osoby, której dane dotyczą, o: (i) zamiarze wykorzystania jej danych dla celów marketingu bezpośredniego, (ii) jej prawie do rezygnacji z takiego marketingu oraz (iii) sposobie, w jaki można (prosto i bez opłat) z takiego prawa skorzystać. Należy zauważyć, że europejski model rezygnacji różni się znacząco od amerykańskiego, który nie wymaga informowania osób, których dane dotyczą, o tego typu szczegółach.

(art. 15(1), ostatnie zdanie)

Wspomniane artykuły Traktatu nawiązują odpowiednio do Karty praw podstawowych UE (ogłoszonej w 2000 roku, tj. po wejściu w życie Dyrektywy o ochronie danych z 1995 roku) oraz Europejskiej Konwencji Praw Człowieka.

Chociaż jest to mile widziane i wyraźne potwierdzenie istotnego unijnego wymogu konstytucyjnego o poszanowaniu podstawowych praw i wolności, oczywiście nie jest to niczym nowym - odpowiednie zasady prawa były już stosowane w praktyce (i prawie) także w momencie przyjęcia „macierzystej" dyrektywy, jako „ogólne zasady prawa wspólnotowego"[137].

Art. 15(1) przewiduje także, że by zabezpieczyć różne „istotne interesy publiczne" wymienione, ale podlegające istotnemu zastrzeżeniu co do poszanowania praw człowieka i ogólnych zasad prawa wspólnotowego:

> *„Państwa Członkowskie mogą, między innymi, uchwalić środki ustawodawcze przewidujące **przechowywanie danych przez określony czas** uzasadnione na podstawie zasad ustanowionych w niniejszym ustępie"*
>
> (art. 15(1), drugie zdanie)

Oryginalny tekst, uwzględniający **wyraźną zasadę ograniczenia prawa, skutecznie zakazującą masowego przetrzymywania danych,** jest istotny, biorąc pod uwagę późniejsze próby ustawodawcy europejskiego, by nałożyć dokładnie takie same obowiązki w ramach tak zwanej Dyrektywy o zatrzymywaniu danych, która została ostatecznie unieważniona przez Trybunał Sprawiedliwości, co omówiono w pkt. 1.3.4.

*RÓŻNICA ***Nadzór i egzekwowanie***

Zważywszy, że Dyrektywa o ochronie danych z 1995 roku została wprowadzona przez specjalistyczne i niezależne organy o ochronie danych i RODO jest egzekwowane przez te same organy, państwa członkowskie mogły przekazać odpowiedzialność za nadzór i egzekwowanie Dyrektywy o e-prywatności innemu organowi lub innym organom. Doprowadziło to do przypisania nadzoru różnym organom w państwach członkowskich w odniesieniu do różnych kwestii będących przedmiotem Dyrektywy o e-prywatności.

Komisja ustaliła, że „przyznanie kompetencji egzekucyjnych szerokiej grupie organów, które się często nakładają" również wydaje się „[hamować] efektywność zasad w sytuacjach transgranicznych"[138].

Stosowanie podstawowych elementów Dyrektywy o ochronie danych z 1995 roku:

W końcu, w ramach przeglądu zasad Dyrektywy o e-prywatności należy zauważyć, że Dyrektywa ta wyraźnie przewiduje, że wymogi Dyrektywy z 1995 roku dotyczące **środków zaskarżenia, odpowiedzialności i sankcji** (patrz pkt 1.3.2) mają także zastosowanie w odniesieniu do Dyrektywy o e-prywatności (art. 15(2)), że **Grupa Robocza Art. 29** (także omówiona w w/w punkcie) podejmuje zadania ustanowione w Dyrektywie z 1995 roku także w odniesieniu do Dyrektywy o e-prywatności (art. 15(3)) oraz że państwa członkowskie muszą zapewnić „skuteczne, proporcjonalne i odstraszające" kary za naruszenie Dyrektywy (art. 15a).

1.3.4. Narzędzia ochrony danych w Trzecim Filarze[139]

W okresie pomiędzy połową lat 90. a 2009 r. Unia Europejska powołała do życia szereg podmiotów, mając na celu usprawnienie współpracy między państwami członkowskimi w obszarze policji i prawa karnego („Sprawiedliwość i Sprawy Wewnętrzne", „Justice and Home Affairs", JHA) – tak zwanym „Trzecim Filarze" UE[140] - z których wszystkie koncentrują się na ustanowieniu ogólnounijnych baz danych

[137] Zob. przypis 63 powyżej.
[138] *Idem*.
[139] Aby uzyskać szczegółowe informacje na temat prawa w tym obszarze, zobacz sekcje historyczne w odpowiednich rozdziałach w: Steve Peers, (2016). Unijne prawo dotyczące wymiaru sprawiedliwości i spraw wewnętrznych: Tom I: Unijne prawo imigracyjne i azylowe (czwarte wydanie) i Tom II: Unijne prawo karne, prawo policyjne i prawo cywilne (czwarte wydanie), oba Oxford University Press, 2016.
[140] Zob. przypis 58 (UWAGA: nowy przypis dodany na s. 26 oryginału angielskiego; podrozdział 1.3.1).

osobowych oraz zasad i procedur dostępu do nich poprzez wymianę danych osobowych między państwami członkowskimi.

Znalazły się między nimi *Europol* (1998), *System Informacyjny Schengen, SIS-I*, (2001, zmodernizowany do *SIS-II* w 2013), *Eurojust* (2002), *Eurodac* (2003), *Wizowy System Informacyjny, VIS* (2004) oraz *System Informacji Celnej, CIS* (2009).

W tym okresie Rada przyjęła 123 instrumenty w obszarze JHA[141]. W 2005 r. Konwencja z Prüm została podpisana przez siedem państw członkowskich, zaś decyzją z 23 czerwca 2008 r. Rada Europy wyraziła zgodę na włączenie jej podstawowych postanowień w ramy prawne UE celem umożliwienia wymiany (między wszystkimi państwami członkowskimi UE) danych biometrycznych (DNA i odcisków palców) na szerszą skalę w walce z terroryzmem i przestępczością transgraniczną.

W 2008 r. Rada przyjęła nadrzędną decyzję ramową celem ustanowienia wspólnych zasad celem ochrony danych osobowych w obszarze JHA[142]. Mimo że wiele z przepisów decyzji ramowej z 2008 r. inspirowanych było Dyrektywą 95/46/WE oraz Konwencją Rady Europy, Peter Hustinx, ówczesny Europejski Inspektor Ochrony Danych, stwierdził jednakże: *„poziom ochrony pod względem zasięgu i treści był znacznie niższy"*[143]. Odnośnie zasięgu [Hustinx] zwrócił uwagę, że[144]:

> Decyzję stosuje się jedynie, gdy dane osobowe są przekazywane lub udostępniane innym państwom członkowskim i stąd [jej zakres] nie rozciąga się na przetwarzanie „krajowe" (tj. przetwarzanie przez lub wewnątrz państwa członkowskiego), inaczej niż w przypadku Dyrektywy 95/46/WE.

W roku 2009, po wejściu w życie Traktatu Lizbońskiego, który położył kres funkcjonowaniu struktury trzech filarów[145], rozpoczął się pięcioletni okres przejściowy, podczas którego unijne prawo dotyczące obszaru JHA miało zostać wpisane w stosowne unijne ponadnarodowe ramy prawne (patrz: podrozdział 1.4.2 poniżej)[146]. W 2018 r. Decyzja Ramowa z 2008 r. została zastąpiona nową decyzją (*idem*).

1.3.5 Ochrona danych w Drugim Filarze

W latach 1990-1993 dla „europejskiej współpracy politycznej" („European Political Cooperation") w sprawach zewnętrznych obowiązywał system nieformalny. W związku z wejściem w życie Traktatu z Maastricht w 1993 r. został on sformalizowany we „Wspólnej polityce zagranicznej i bezpieczeństwa" („Common Foreign and Security Policy", CFSP) – „Drugim Filarze" UE. Niemniej aż do czasu dalszego rozwinięcia CFSP w związku z Traktatem Lizbońskim z 2009 r. (który zniósł „strukturę filarową")[147], jak wspomina podrozdział 1.4.4 poniżej, nie istniały konkretne przepisy ochrony danych, które odnosiły się do przetwarzania danych osobowych w tym obszarze (inne niż przepisy krajów członkowskich w sprawie ochrony danych oraz Konwencja Rady Europy).

1.3.6. Ochrona danych w instytucjach Unii Europejskiej

Ogólne i spójne przepisy w zakresie ochrony danych, które odnosiłyby się do instytucji UE, nie istniały aż do 2001 r., kiedy to rozporządzenie (WE) 45/2001 jako pierwsze wprowadziło takie regulacje na podstawie art. 286 Traktatu o Unii Europejskiej, stawiającego ich wymóg[148].

Przepisy rozporządzenia z 2001 r. oparte były o istniejące wówczas regulacje Wspólnoty dotyczące

---

[141] Zob.Emilio De Capitani, Metamorphosis of the third pillar: The end of the transition period for EU criminal and policing law, EU Law Analysis blogspot, 10 lipca 2014 r. dostępne pod adresem: https://eulawanalysis.blogspot.com/2014/07/metamorphosis-of-third-pillar-end-of.html.

[142] Decyzja ramowa Rady 2008/977/WSiSW z dnia 28 listopada 2008 r. *w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych*, OJ L 350, 30 grudnia 2008 r. str. 60, dostępna pod adresem: https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex%3A32008F0977

[143] Peter Hustinx, EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation, str. 15, dostępny pod adresem: https://www.statewatch.org/news/2014/sep/eu-2014-09-edps-data-protection-article.pdf.

[144] *Idem*, w odniesieniu do motywu 7 i art. 1 Decyzji ramowej.

[145] Zob. przypis 58 (patrz komentarz wyżej) powyżej

[146] Zob. Protokół 37 do Traktatu Lizbońskiego oraz Emilio De Capitani, op. cit., (przypis 169 powyżej).

[147] Zob. ponownie przypis 58 powyżej (patrz: przypis 173 i komentarz).

[148] 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*, OJ L 8, 12 stycznia 2001 r. str. 1-22, dostępne pod adresem: https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32001R0045.

ochrony danych, które miały zastosowanie w państwach członkowskich, w szczególności o Dyrektywę o ochronie danych osobowych z 1995 r. oraz Dyrektywę o e-prywatności z 2002 r.

Rozporządzenie 45/2001 ustanowiło ponadto instytucję Europejskiego Inspektora Ochrony Danych jako niezależnego organu nadzorczego z uprawnieniem do monitorowania przetwarzania danych osobowych przez instytucje i organy Wspólnoty oraz wprowadziło wymóg wyznaczenia inspektorów ochrony danych (Data Protection Officer, DPO) przez te instytucje i organy.

1.4 Prawo o ochronie danych w przyszłości

Do końca pierwszej dekady XXI wieku stało się jasne, że zasadniczo przyjęte w XX wieku instrumenty o ochronie danych, omówione w pkt. 1.3, nie były już wystarczające - zostały wymyślone i opracowane przed wprowadzeniem masowego dostępu do internetu (lub przynajmniej ogólnoświatowej sieci), wszechobecnych komputerów (i urządzeń mobilnych), obszernych zbiorów danych, „internetu rzeczy" (Internet of Things, IoT), dogłębnego profilowania, opartego na algorytmach procesu decyzyjnego oraz sztucznej inteligencji (Artificial Intelligence, AI). Zarówno w UE, jak i w Radzie Europy opracowano więc nowe i zaktualizowane („zmodernizowane") instrumenty o ochronie danych, które omówiono poniżej.

1.4.1 Unijne ogólne rozporządzenie o ochronie danych

W 2012 roku Komisja Europejska zaproponowała przyjęcie Ogólnego rozporządzenia o ochronie danych (RODO)[149], by sprostać wyzwaniom nakładanym przez nowe technologie i usługi. Komisja postrzegała silną, wysokiego poziomu ochronę danych jako zasadniczy warunek zdobycia zaufania w środowisku internetowym, które samo w sobie jest kluczem do rozwoju gospodarczego, a nowy zaktualizowany system ochrony danych *lex generalis* miał odgrywać centralną rolę w Agendzie Cyfrowej dla Europy oraz ogólniej w Strategii Europa 2020[150].

Historia, status i podejście oraz kluczowe elementy RODO opisano bardziej szczegółowo w drugiej części Podręcznika. Wystarczy wspomnieć, że RODO znacząco **poszerza i wzmacnia główne zasady i reguły;** wyraźnie **dodaje dane genetyczne i biometryczne do listy wrażliwych danych** (co zostało zainspirowane pracami nad „zmodernizowaną" Konwencją Rady Europy o ochronie danych, którą omówiono poniżej w pkt. 1.4.3); ma na celu wprowadzenie **większej harmonizacji** przepisów o ochronie danych w państwach członkowskich UE (przynajmniej w obszarach, których dotyczy, tj. głównie w obszarze wcześniej zwanym „pierwszym filarem" Wspólnoty Europejskiej) zgodnie z istotnym nowym orzecznictwem Trybunału Sprawiedliwości, aczkolwiek z zastrzeżeniem szerokiego zakresu „klauzul szczegółowych" (tj. klauzul pozostawiających dokładniejsze uregulowanie niektórych kwestii prawu krajów członkowskich w ogólnych ramach nakreślonych przez RODO, traktaty unijne zgodne z interpretacją TSUE oraz konstytucyjne i prawne systemy państw członkowskich[151]; określa **silniejsze (i nowe) prawa osób, których dane dotyczą;** umożliwia **znacznie bliższą współpracę transgraniczną** pomiędzy organami ochrony danych państw członkowskich, a także powinna prowadzić do **lepszego, spójniejszego stosowania i egzekwowania** tych reguł.

Konkretniej, jak już wspomniano we Wprowadzeniu do niniejszego Podręcznika, RODO wprowadza (lub przynajmniej precyzuje) **obecnie podstawową i obowiązkową we wszystkich państwach członkowskich zasadę „rozliczalności"** i w wielu przypadkach (także w odniesieniu do wszystkich podlegających Rozporządzeniu organów państwowych) **wymaga** wprowadzenia instytucji

[149] Propozycja rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (ogólne rozporządzenie o ochronie danych) , COM(2012) 11 final, Bruksela, 25.01.2012 r. https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52012PC0011&from=PL. Jednocześnie Komisja zaproponowała osobny instrument o ochronie danych, Propozycję dyrektywy w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych (COM(2012) 10 final), ale dyrektywa ta nie jest przedmiotem niniejszego Podręcznika (patrz uwaga w polu „O podręczniku" na str. 1 Podręcznika).

[150] Propozycja RODO (poprzedni przypis), str. 1 – 2 (z odwołaniem do głównych dokumentów umieszczonych w Agendzie Cyfrowej i Strategii Europa 2020). Następcą Agendy Cyfrowej jest Strategia Jednolitego Rynku Cyfrowego („Strategia JRC").

[151] Zob. Część druga, podrozdział 2.2, poniżej, pod nagłówkiem *„[…] ale z <klauzulami szczegółowymi>"*.

wyznaczanych przez administratora lub podmiot przetwarzający inspektorów ochrony danych (**IOD**).

Jak wspomniano w części drugiej, obydwa te elementy są ze sobą powiązane – zgodnie z RODO inspektorzy ochrony danych to osoby, które będą w praktyce zapewniać przestrzeganie zasady rozliczalności przez organizacje i w ramach organizacji, do których należą.

1.4.2 Proponowane rozporządzenie UE o e-prywatności

Chociaż, jak zauważono w poprzednim ustępie, jednym z głównych celów proponowanego RODO było stawienie czoła wyzwaniom wynikającym z **braku zaufania (w szczególności konsumentów) w środowisku internetowym**, kolejne pięć lat zajęło komisji zaproponowanie nowego instrumentu, zastąpienie reguł dotyczących w większym stopniu tego środowiska, tj. omówionej w pkt. 1.3.4 Dyrektywy o e-prywatności (Dyrektywa 2002/58/WE) (która przez to pozostaje w mocy w nieco „osierocony" sposób).

Doprowadziło to w styczniu 2017 roku do propozycji zastąpienia także Dyrektywy o e-prywatności stosownym **rozporządzeniem**[152].

Propozycja ta znajduje się jeszcze na wczesnym etapie procesu legislacyjnego - w trakcie pisania (grudzień 2018), była w dalszym ciągu przedmiotem rozmów wewnętrznych w ramach Rady oraz znaczącej uwagi ze strony zarówno jej rzeczników (grup na rzecz wolności cywilnych, praw konsumentów i praw cyfrowych)[153], jak i przeciwników (z uwzględnieniem niektórych głównych amerykańskich gigantów internetowych, którzy wnioskują albo o zupełne wycofanie propozycji, albo o jej znaczące osłabienie)[154]. Dlatego też jest zbyt wcześnie, by omówić proponowane rozporządzenie w szczegółach. Niewątpliwie ostateczna wersja będzie - przynajmniej pod pewnymi względami - różnić się od propozycji.

W związku z powyższym w pierwszej edycji Podręcznika musi wystarczyć prosta prezentacja **kluczowych punktów propozycji Komisji**, określonych przez samą Komisję[155]:

> Propozycja rozporządzenia w sprawie wysokiego poziomu reguł prywatności w odniesieniu do wszystkich komunikatów elektronicznych obejmuje:
>
> - **Nowych graczy:** reguły prywatności [*i ochrony danych*] także w przyszłości będą miały zastosowanie do nowych [tak zwanych „*skrajnych*"] graczy świadczących usługi łączności elektronicznej, takich jak WhatsApp, Facebook Messanger i Skype. Zapewni to, że te popularne serwisy gwarantować będą taki sam poziom poufności komunikatów, jak tradycyjni operatorzy telekomunikacyjni.
> - **Silniejsze reguły:** wszystkie osoby i przedsiębiorstwa w UE korzystać będą z takiego samego wysokiego poziomu ochrony swoich komunikatów elektronicznych poprzez bezpośrednio obowiązujące rozporządzenie. Przedsiębiorstwa będą także korzystać z jednego zestawu reguł w całej UE[156].
> - **Treść łączności elektronicznej i metadane:** gwarantowana prywatność obejmuje treść łączności elektronicznej i metadane, np. czas połączenia i lokalizację. Metadane zawierają element wysokiej prywatności i muszą być anonimizowane lub usuwane,

---

[152] Propozycja rozporządzenia Parlamentu Europejskiego i Rady w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej i uchylające dyrektywę 2002/58/WE (rozporządzenie w sprawie prywatności i łączności elektronicznej), COM(2017) 10 final, Bruksela, 10.01.2017 r. https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52017PC0010&from=PL

[153] Zob. Otwarty list do państw członkowskich UE w sprawie reformy e-prywatności, wysłany przez dużą grupę organizacji pozarządowych 27 marca 2018 r. https://edri.org/files/eprivacy/20180327-ePrivacy-openletter-final.pdf.

[154] Zob. Corporate Europe Observatory, *Shutting down ePrivacy: lobby bandwagon targets Council*, 4 czerwca 2018 r. https://corporateeurope.org/power-lobbies/2018/06/shutting-down-eprivacy-lobby-bandwagon-targets-council.

[155] https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation (pogrubiona czcionka - oryginał, wyrazy w nawiasach kwadratowych i pochyłą czcionką oraz przypisy - dodano).

[156] Należy jednak zauważyć, że zależeć to będzie od zastosowanych w Rozporządzeniu o e-prywatności reguł niezawierających „elastycznych" klauzul „szczegółowych", takich jak te zawarte w RODO (patrz druga Część, pkt 2.1). Gdyby ostateczny tekst Rozporządzenia o e-prywatności miał zawierać takie „elastyczne" postanowienia (co jest bardzo prawdopodobne), należałoby - w szczególności dla środowiska internetowego, które jest ze względu na swój charakter transnarodowe - dodać postanowienie o „odpowiednim prawie".

jeżeli użytkownicy nie wyrazili zgody, chyba że dane te są niezbędne do naliczania opłat[157].

- **Nowe możliwości dla przedsiębiorstw:** gdy wydano zgodę na przetwarzanie danych - treści i/lub metadanych - pochodzących z łączności, tradycyjni operatorzy telekomunikacyjni będą mieli większe możliwości w zakresie świadczenia dodatkowych usług oraz rozwoju swoich przedsiębiorstw. Na przykład mogliby wyprodukować mapy uwagowe (heat maps) wskazujące obecność jednostek, które pomagałyby organom publicznym i firmom transportowym w realizacji nowych projektów infrastrukturalnych.
- **Prostsze zasady dotyczące plików cookies:** postanowienie dotyczące plików cookies, które doprowadziło do nadmiaru wymaganych zgód użytkowników internetowych, zostanie zoptymalizowane. Nowa zasada będzie bardziej przyjazna użytkownikowi, ponieważ ustawienia przeglądarki będą umożliwiać łatwą akceptację lub odmowę śledzenia plików cookies i innych identyfikatorów. Propozycja ta wyjaśnia także, że nie jest potrzebna zgoda na stosowanie niezakłócających prywatności plików cookies, które poprawiają korzystanie z internetu (np. zapamiętują historię koszyka zakupów), lub plików cookies stosowanych przez stronę do liczenia odwiedzających.
- **Ochrona przed spamem:** propozycja zabrania przesyłania niezamówionych komunikatów elektronicznych pocztą elektroniczną, SMSem i przy użyciu automatycznych systemów wywołujących. *W zależności od prawa krajowego* ludzie będą lepiej chronieni domyślnie lub będą w stanie skorzystać z listy zakazanych kontaktów, by nie otrzymywać marketingowych połączeń telefonicznych[158]. Marketerzy będą musieli wyświetlić swój numer telefonu lub stosować specjalny prefiks wskazujący na połączenie marketingowe.
- **Skuteczniejsze egzekwowanie:** za egzekwowanie zasad prywatności w Rozporządzeniu odpowiedzialne będą organy ochrony danych, na które odpowiedzialność taką już nałożyło Ogólne rozporządzenie o ochronie danych.

1.4.3. Dyrektywa z 2016 r. o ochronie danych w związku z przetwarzaniem ich przez organy ścigania (Law Enforcement Data Protection Directive of 2016, LEDPD; Dyrektywa o ochronie danych osobowych, DODO)

Wprowadzenie

Art. 10(1) Protokołu 36 do Traktatu Lizbońskiego przewidywał okres przejściowy, zanim znalazły zastosowanie pełne uprawnienia Komisji i Trybunału Sprawiedliwości w odniesieniu do aktów prawnych Unii w dziedzinie współpracy policyjnej oraz współpracy sądowej w sprawach karnych, które zostały przyjęte przed wejściem w życie Traktatu Lizbońskiego („wcześniejszy dorobek trzeciego filaru"). Ta faza przejściowa dobiegła końca 1 grudnia 2014 r.

W 2012 r. Komisja złożyła wniosek o sformułowanie dyrektywy w tym obszarze wraz z propozycją ogólnego rozporządzenia o ochronie danych (przedstawionego w rozdziale 1.4.1, powyżej i omówionego bardziej szczegółowo w części drugiej tego podręcznika)[159]. Niemniej, tak jak w przypadku RODO, dyrektywa o ochronie danych w związku z przetwarzaniem ich przez organy ścigania (określana również jako „dyrektywa w sprawie organów ścigania", „dyrektywa policyjna ochrony danych", czy też po prostu: „dyrektywa policyjna") została przyjęta dopiero w 2016 r. - tego samego dnia co RODO[160]. W

[157] Należy jednak zwrócić uwagę na podejmowane przez państwa członkowskie i Komisję próby zatrzymania lub ponownego wprowadzenia obowiązkowego zatrzymywania (meta)danych w ramach łączności elektronicznej: patrz pkt 1.3.4.

[158] Jest to dokładnie takie samo „elastyczne" postanowienie, jak to wspomniane w przypisie 179, i ilustruje potrzebę wprowadzenia zasady „odpowiedniego prawa", by wyjaśnić które z różnych reguł krajowych będą miały zastosowanie do transgranicznych przesyłek marketingowych.

[159] Zob. przypis 149 powyżej (UWAGA: w tej wersji: 146).

[160] 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*, OJ L 119, 4 maja 2016 r. str. 89-131,

przeciwieństwie jednak do RODO, które jako rozporządzenie jest zasadniczo stosowane bezpośrednio w porządkach prawnych państw członkowskich (aczkolwiek w tym przypadku ze znaczącą liczbą zapisów, które wymagają dalszego „dookreślenia" w prawie krajowym)[161], DODO, jako dyrektywy, nie stosuje się bezpośrednio (tj. nie wywiera ona „bezpośredniego efektu") lecz **musi być „przetransponowana" na prawo krajowe**. Należało tego dokonać w okresie dwóch lat od formalnego wejścia w życie dyrektywy, tj. do dnia 6 maja 2018 r. (zaledwie kilka tygodni przed rozpoczęciem stosowania RODO w dniu 25 maja 2018 r.).

Należy odnotować wydłużone terminy wprowadzenia w życie, określone w art. 61-63 dyrektywy, uzasadnione różnymi okolicznościami dotyczącymi dużej liczby operacji przetwarzania danych wchodzących w jej zakres, które będą omówione pokrótce na końcu rozdziału dotyczącego DODO, pod nagłówkiem *„Odroczona transpozycja"*.

W tym miejscu wystarczyć musi odnotowanie głównych cech charakterystycznych oraz wymogów DODO[162].

Dyrektywa w miejsce Decyzji Ramowej Rady

Pierwszą uwagą, jaką należy tu uczynić, jest ta, że wyznaczenie zasad przetwarzania danych w dyrektywie jest samo w sobie **znaczącym udoskonaleniem** w porównaniu z zawarciem ich w Decyzji Ramowej Rady, takiej jak ta z 2008 roku uchylona przez DODO[163]. Do dyrektywy mogą przed sądami krajowymi (oraz ostatecznie przed Trybunałem Sprawiedliwości)_odwoływać się jednostki w postępowaniach przeciwko organom państwa; dyrektywa podlega również władzy wykonawczej Komisji, która ma na celu zapewnienie właściwej transpozycji takich instrumentów w prawo krajowe.

Zakres DODO

i. Działania, które obejmuje

Odnośnie zakresu, DODO określa, co następuje:

Zakres

1. Dyrektywa ma zastosowanie do przetwarzania danych osobowych przez właściwe organy [do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, łącznie z ochroną przed zagrożeniami dla bezpieczeństwa publicznego i zapobieganiem takim zagrożeniom].
2. Dyrektywa ma zastosowanie do zautomatyzowanego przetwarzania danych osobowych oraz do przetwarzania ręcznego, jeżeli dane osobowe znajdują się lub mają się znaleźć w zbiorze danych.
3. Dyrektywa nie ma zastosowania do przetwarzania danych osobowych:
   a) w ramach działalności wykraczającej poza zakres prawa Unii;
   b) przez instytucje, organy i jednostki organizacyjne Unii[164].

Odnośnie „właściwego organu", szczegółowe rozgraniczenie między przetwarzaniem danych podlegającym DODO, a tym podlegającym RODO, musi zostać oszacowane przy wzięciu pod uwagę motywu 12. Wyjaśnia on, w ostatnim zdaniu, że przetwarzanie danych osobowych w związku z „innymi zadaniami", powierzonymi „właściwym organom", które *„niekoniecznie służą zapobieganiu przestępczości, prowadzeniu postępowań przygotowawczych, wykrywaniu i ściganiu czynów zabronionych, w tym ochronie przed zagrożeniami dla bezpieczeństwa publicznego i zapobieganiu takim*

dostępna pod adresem: https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32016L0680. Formalnie dyrektywa ta weszła w życie dzień po jej publikacji w Dzienniku Urzędowym, tj. 5 maja 2016 r. – ale, jak odnotowano w tekście, miała zastosowanie (poprzez transpozycję na prawo krajowe państw członkowskich) dwa lata po tym terminie, tj. od 6 maja 2018 r.

[161] Zob. Część druga, rozdział 2.2, poniżej.

[162] Jak zostało to wyjaśnione na początku tego podręcznika, mamy nadzieję rozwinąć problematykę ochrony danych w UE poza RODO w drugim wydaniu. Objęłoby ono przepisy DODO, które zostały tu jedynie pokrótce omówione.

[163] Zob. Steve Peers, The Directive on data protection and law enforcement: A Missed Opportunity? Statewatch Analysis blog, kwiecień 2012 r. dostępne pod adresem: https://www.statewatch.org/analyses/no-176-leas-data%20protection.pdf.

[164] Przetwarzanie, dokonywane przez instytucje, organy i jednostki organizacyjne Unii do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, podlega szczególnemu zestawowi przepisów, zawartych w Rozdziale IX nowego rozporządzenia […] w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii […], Rozporządzenie (UE) 2018/1725, jak zostało to pokrótce omówione w rozdziale 1.4.5 poniżej.

zagrożeniom", wchodzi w zakres RODO, nie zaś DODO.

Administrator musi zwrócić szczególną uwagę na to rozgraniczenie oraz na inne kwestie, takie jak zakres, w którym zbieranie i dalsze przetwarzanie danych osobowych w związku z „incydentami", co do których *nie jest jeszcze jasne*, czy doszło do naruszenia prawa, czy też w związku z podejmowaniem środków (łącznie ze „*środkami przymusu*") w trakcie demonstracji lub dużych imprez sportowych, które „mogą prowadzić do poważnego przestępstwa kryminalnego" (lub nie), podlega DODO – ponieważ odpowiedzi na te pytania mogą mieć znaczący wpływ na poziom ochrony danych, który musi zostać zapewniony, tj. pod względem informowania osób, których dane dotyczą, ograniczeń zatrzymywania danych, ograniczeń praw osób, których dane dotyczą, itd. Tymczasem inspektorzy ochrony danych, pracujący we właściwych organach, powinni wspierać organy w dokonywaniu tychże ustaleń celem zapewnienia odpowiedniego poziomu ochrony danych we wszystkich kontekstach.

Pojęcie "**bezpieczeństwa publicznego**" jest zazwyczaj używane w kontekście wyjątków od prawa unijnego, tj. by określić podstawy, które mogą zostać użyte do usprawiedliwienia działania, które w innym przypadku byłoby naruszeniem prawa Unii. Jak wskazuje Koutrakis, „Bezpieczeństwo publiczne ustanawia podstawę do wyjątków od wszystkich naszych wolności zgodnych z podstawowymi prawami Unii"[165]. Cytując dokument instruktażowy, stworzony na wniosek Komisji Rynku Wewnętrznego i Ochrony Konsumentów (IMCO) Parlamentu Europejskiego[166]:

> Ze wszystkich podstaw, na których opierają się wyjątki od swobodnego przepływu, **bezpieczeństwo publiczne jest najbliżej kojarzone z tym, co jest tradycyjnie rozumiane jako trzon suwerenności narodowej, to jest obszarem działalności, w którym państwo ma podstawowy obowiązek ochrony swojego terytorium i obywateli**. (podkreślenie dodane)

Przewodnim wyrokiem TSUE w kwestii „bezpieczeństwa publicznego" jest sprawa Campus Oil[167], w której Trybunał utrzymał, że krajowy środek – w tym wypadku krajowa kwota zaopatrzenia w olej rafinowany w Republice Irlandzkiej – jest usprawiedliwiony, gdyż olej rafinowany został uznany za:

> **mający fundamentalne znaczenie dla egzystencji państwa**, gdyż nie tylko jego świadczenia, ale również wszystkie jego instytucje, kluczowe usługi publiczne, a nawet przetrwanie jego mieszkańców, zależą od nich (par. 34, podkreślenie dodane).

Jasne jest zatem, że – z **jednej strony – pojęcie „bezpieczeństwa publicznego", tak jak używane jest ono w prawie UE – nie ogranicza się jedynie do kwestii związanych z działalnością przestępczą, lecz rozciąga się na kwestie takie jak ochrona „kluczowych usług publicznych" oraz środki mające na celu „przetrwanie mieszkańców [państwa]"; z drugiej jednak strony, nie jest ono tak szerokie jak „ład publiczny" – pojęcie używane często w prawie policyjnym i odnoszące się do spraw związanych z utrzymywaniem porządku podczas demonstracji, parad i uroczystości[168]. Kwestia, którą należy zabezpieczyć musi, zdaniem Rady, odnosić się do**[169]:

> autentycznego i wystarczająco poważnego zagrożenia, dotyczącego jednego z fundamentalnych interesów społecznych, takiego jak zagrożenie funkcjonowania instytucji i kluczowych usług publicznych oraz przetrwania ludności, jak również do ryzyka poważnego zaburzenia w stosunkach zagranicznych lub w pokojowym współistnieniu narodów, czy też ryzyka dla interesów militarnych.

Ocena dokładnych granic tego, co jest, a co nie jest (przestępczymi?) zagrożeniami dla „bezpieczeństwa publicznego", jest trudna do oszacowania w szczególnych okolicznościach. Kiedy jakieś zaburzenie ładu

---

[165] Panos Koutrakis, Public Security Exceptions and EU Free Movement Law, w: Koutrakis, P., Nic Shuibhne. N. oraz Sypris, P., (red.), Exceptions from EU Free Movement Law, 2016 (str. 190-217), dostępne pod adresem: http://openaccess.city.ac.uk/id/eprint/16192/ (w odniesieniu do art. 36 (dobra), art. 45(3) oraz 52 (osoby) oraz art. 65 TFUE (kapitał)).

[166] Public Security Exception in the Area of non-personal Data in the European Union, dokument instruktażowy na wniosek Komisji IMCO Parlamentu Europejskiego, przygotowany przez Kristinę Irion, PE 618.986, kwiecień 2018 r. str. 3, dostępny pod adresem: https://www.europarl.europa.eu/RegData/etudes/BRIE/2018/618986/IPOL_BRI(2018)618986_EN.pdf.

[167] Wyrok Trybunału z 10 lipca 1984 r. Campus Oil Limited and others v Minister for Industry and Energy and others, Case 72/83, ECR 1984 -02727, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:61983CJ0072&from=EN.

[168] Por. np. http://www.lokalepolitie.be/5371/contact/diensten/20-handhaving-openbare-orde (w języku holenderskim.

[169] Rada Unii Europejskiej, kartoteka międzyinstytucjonalna: 2017/0228 (COD), motyw 12(a) na str. 3, dostępna pod adresem: https://www.consilium.europa.eu/media/32307/st15724-re01en17.pdf.

publicznego, np. przerwa w lotach, będąca dziełem osób demonstrujących przeciwko wydaleniu ludzi poszukujących azylu, stanowi „zagrożenie dla kluczowej usługi publicznej”[170]? I kiedy ryzyko „zaburzeń w stosunkach zagranicznych” – np. demonstracja przeciwko wizycie głowy obcego państwa – jest wystarczająco „poważne”, by sklasyfikować je jako zagrożenie dla bezpieczeństwa publicznego? Jednakże to odpowiedzi na te pytania determinują kwestię, czy DODO stosuje się do przetwarzania danych osobowych w związku z tymi działaniami, czy też nie.

Podczas gdy wiele podmiotów – w szczególności z sektora publicznego, takich jak władze lokalne czy organy ochrony środowiska, usług społecznych czy opieki nad zwierzętami – otrzymuje część władzy publicznej i część uprawnień publicznych związanych z (pewnymi) przestępstwami i (pewnymi) zagrożeniami bezpieczeństwa publicznego, główne zadania tych organów nie będą związane z prowadzeniem postępowań przygotowawczych (itd.) w sprawie czynów zabronionych w ich właściwych kompetencjach czy też z zagrożeniami ładu publicznego (związanymi z przestępczością lub nie).

Inspektorzy ochrony danych w takich organach i instytucjach publicznych powinni drobiazgowo prześledzić, w jakim zakresie przetwarzanie danych osobowych przez ich własną organizację lub organizacje może być uznane za podlegające RODO i w jakim zakresie podlega LEDPD. Nie będzie to często prosta kwestia do wyjaśnienia, zaś inspektor ochrony danych powinien w związku z tym pracować nad tym razem z administratorem, działem prawnym i właściwym organem nadzorczym. Ponadto dane osobowe przetwarzane w ramach operacji przetwarzania, które podlegają LEDPD, muszą być przechowywane oddzielnie od danych osobowych przetwarzanych w ramach operacji, które podlegają przepisom RODO, wraz ze szczegółowymi przepisami i polityką w odniesieniu do tego, kiedy dane osobowe w jednej kategorii lub w jednym celu mogą być wykorzystywane do innej kategorii lub w innym celu[171].

Wreszcie pojawia się problem związany z granicą między działaniami państw członkowskich UE w obszarze „*zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych*” oraz „*ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom*”, z jednej strony, a z drugiej strony działaniami państw członkowskich dotyczącymi **bezpieczeństwa narodowego** i czynności agencji lub jednostek państw członkowskich zajmujących się kwestiami bezpieczeństwa narodowego,. W coraz większym stopniu zacierają się granice między tymi dwoma obszarami działań – pierwsza teoretycznie w pełni w ramach prawa UE, druga formalnie całkowicie bez prawa UE (zwłaszcza w odniesieniu do zbyt ograniczonych kategorii „terroryzm”, „cyberprzestępczość”, „cyberbezpieczeństwa” itp.)[172]. W rzeczywistości[173]:

> [I] W niektórych krajach same agencje stają się instrumentami hybrydowymi, a ich podwójną rolą jest walka z przestępczością i ochrona bezpieczeństwa narodowego.

[170] W Wielkiej Brytanii doszło do kontrowersji odnośnie kwestii ścigania i karania takich właśnie demonstrantów zgodnie z prawem antyterrorystycznym, tj. zgodnie z prawem „bezpieczeństwa publicznego”, nie zaś zgodnie z normalnym prawem karnym dotyczącym naruszenia miru domowego, patrz: https://www.theguardian.com/global/2019/feb/06/stansted-15-rights-campaigners-urge-judge-to-show-leniency. W sprawie wniesiono apelację.

[171] Zob. również omówiona poniżej podsekcja 1.4.6 dotycząca wymiany danych osobowych między różnymi podmiotami działającymi w różnych systemach ochrony danych w UE.

[172] Douwe Korff, Ben Wagner, Julia Powles, Renata Avila i Ulf Buermeyer, Boundaries of Law: Exploring Transparency, Accountability, and Oversight of Government Surveillance Regimes, sprawozdanie porównawcze obejmujące Kolumbię, Demokratyczną Republikę Konga, Egipt, Francję, Niemcy, Indie, Kenię, Mjanma, Pakistan, Rosję, RPA, Turcję, Zjednoczone Królestwo, Stany Zjednoczone, przygotowane dla World Wide Web Foundation, styczeń 2017 r., w szczególności sekcja 2.3.1, dostępne pod adresem: https://ssrn.com/abstract=2894490

[173] *Idem*, s. 27. Rozszerzenie roli policji na działania prewencyjne nie jest nowe. Zob. Ian Brown & Douwe Korff, Privacy & Law Enforcement, FIPR Study for the UK Information Commissioner, 2005, Paper 4, The legal framework, sekcja 3.1. Najnowsze zmiany, w szczególności w odniesieniu do zacierania się granic pomiędzy politykami a działaniami związanymi z bezpieczeństwem narodowym opisane są w: Douwe Korff, Protecting the right to privacy in the fight against terrorism, dokument tematyczny sporządzony dla Komisarza Rady Europy ds. Praw Człowieka w 2008 r. dostępny pod adresem: https://wcd.coe.int/ViewDoc.jsp?Ref=CommDH/IssuePaper (2008) 3.

> Doskonałym przykładem jest Federalne Biuro Śledcze (FBI)[174], ale również w Zjednoczonym Królestwie GCHQ współpracuje w coraz większym stopniu z organami ścigania[175].

Kwestia ta nie może zostać szczegółowo omówiona w tym miejscu, ale zostanie poruszona w sekcji poniżej 1.4.6, dotyczącej przekazywania danych osobowych przez administratora danych w obszarze objętym jedną z kategorii prawa o ochronie danych UE, administratorowi, który podlega innej kategorii prawa UE – lub, w przypadku krajowych agencji bezpieczeństwa, w ogóle nie podlega prawu unijnemu.

Z drugiej strony rozróżnienie między przetwarzaniem danych osobowych objętych LEDPD a przetwarzaniem danych osobowych przez instytucje, organy, urzędy i agencje UE jest jasne, a te ostatnie objęte są nowym rozporządzeniem przyjętym w 2018 r., jak zostało to omówione w sekcji 1.4.6 poniżej.

i. Podmioty objęte rozporządzeniem

Również w odniesieniu do zakresu zastosowania LEDPD definiuje „**właściwe organy**", o których mowa w art. 1 ust. 1, jako:

> (a) organ publiczny właściwy do 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; lub
>
> (b) inny organ lub podmiot, któremu prawo państwa członkowskiego powierza sprawowanie władzy publicznej i wykonywanie uprawnień publicznych do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom.
>
> (art. 3 ust. 7)

Jak już zauważono, może to wykraczać daleko poza policję i inne organy egzekwowania prawa działające na pierwszej linii, tak aby uwzględnić – w zależności od krajowego podejścia konstytucyjnego – organy publiczne na szczeblu lokalnym i regionalnym, agencje ds. zdrowia, bezpieczeństwa i pożytku społecznego, organy sprawujące nadzór nad instytucjami finansowymi, organy zajmujące się ochroną zwierząt, agencje ds. środowiska, organy celne i podatkowe, a także wiele innych organów – w przypadku gdy przyznano im „*władzę publiczną i uprawnienia publiczne*" w odniesieniu do czynów zabronionych lub zagrożeń dla bezpieczeństwa publicznego, które mogą pociągać za sobą prowadzenie działalności przestępczej w ramach ich kompetencji.

Jak już zauważono, przetwarzanie danych osobowych przez takie organy w odniesieniu do

---

[174] Na stronie internetowej FBI *« Addressing threats to the nation's cybersecutiry »* (*„Przeciwdziałanie zagrożeniom dla bezpieczeństwa narodowego*") wyraźnie stwierdza się, że FBI jest odpowiedzialne za ochronę bezpieczeństwa narodowego Stanów Zjednoczonych, jak również jest główną agencją ds. egzekwowania prawa, dodając, że „role *te wzajemnie się uzupełniają, gdyż zagrożenia dla bezpieczeństwa narodowego mogą pochodzić od organizacji terrorystycznych z państw narodowych oraz ponadnarodowych organizacji przestępczych; gdzie granice między nimi z czasem się zacierają.*" Zob.: www.fbi.gov/about-us/investigate/cyber/addressing-threats-to-the-nations-cybersecurity
FBI niedawno zmieniło arkusz informacyjny FBI, aby opisać swoją *„podstawową funkcję*", ponieważ nie jest to już *„egzekwowanie prawa*", ale obecnie *„bezpieczeństwo narodowe*". Zob. The Cable, 5 stycznia 2014 r. pod adresem: http://thecable.foreignpolicy.com/posts/2014/01/05/fbi_drops_law_enforcement_as_primary_mission#sthash.4DrWhlRV.dpbs W odniesieniu do zagrożeń, jakie niesie ze sobą takie zacieranie granic zob.: www.foreignpolicy.com/articles/2013/11/21/the_obscure_fbi_team_that_does_the_nsa_dirty_work
[przypis oryginalny]

[175] Zob. Computer Weekly, *„GCHQ and NCA join forces to police dark web",* 9 listopada 2015 r. pod adresem: http://www.computerweekly.com/news/4500257028/GCHQ-and-NCA-join-forces-to-police-dark-web
[przypis oryginalny]

działań niezwiązanych ze sprawami karnymi podlega RODO, a nie LEDPD, i tak samo może być w przypadku przetwarzania danych osobowych przez takie organy w związku z zagrożeniami dla bezpieczeństwa publicznego, które nie obejmują czynów zabronionych, takich jak burze lub powodzie czy epidemie, lub w związku z obsługą wydarzeń sportowych podczas których nie dochodzi do ewentualnych czynów zabronionych.

ii. Operacje przetwarzania objęte rozporządzeniem

W odniesieniu do środków wykorzystywanych do przetwarzania, zgodnie z innymi unijnymi instrumentami ochrony danych, LEDPD ma zastosowanie do:

> przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany oraz do przetwarzania w sposób inny niż zautomatyzowany danych osobowych stanowiących część zbioru danych lub mających stanowić część zbioru danych.

Innymi słowy, LEDPD ma zastosowanie do **wszelkiego rodzaju przetwarzania danych osobowych w sposób zautomatyzowany** oraz do przetwarzania wszystkich danych osobowych przechowywanych w manualnych **uporządkowanych zbiorach**, które wchodzą w jego zakres pod względem działalności i podmiotów.

Co ważne, w odróżnieniu od decyzji ramowej z 2008 r., omówionej wcześniej, w sekcji 1.3.6 powyżej, **LEDPD stosuje się** nie tylko do danych osobowych przekazywanych między państwami członkowskimi, ale **również do przetwarzania danych osobowych na użytek krajowy do celów egzekwowania prawa**. Jak podkreśla Komisja, dyrektywa powinna w związku z tym *„ułatwić współpracę policji i organów wymiaru sprawiedliwości w sprawach karnych w całej UE”*[176].

Swobodny przepływ danych między właściwymi organami w różnych państwach członkowskich

Chociaż dyrektywa *„nie wyklucza ustanowienia przez państwa członkowskie zabezpieczeń wyższych niż zabezpieczenia przewidziane w niniejszej dyrektywie”* (art. 1 ust. 3), każde państwo członkowskie, które ustanowiło takie wyższe standardy, nie może powoływać się na nie jako oznaczające „**ograniczenie lub zakazanie**” swobodnej wymiany danych osobowych między państwami członkowskimi, co stanowi sam cel dyrektywy (art. 1 ust. 2 lit. b)). Jeżeli natomiast państwo członkowskie przewiduje w swoim prawie „szczególne **warunki**” w odniesieniu do określonego przetwarzania (np. w celu profilowania) lub – przypuszczalnie – do przetwarzania określonych rodzajów danych (np. danych biometrycznych) – to państwo członkowskie może, ale rzeczywiście musi („musi”):

> zapewnić, by właściwy organ przesyłający informował odbiorcę takich danych osobowych o tych warunkach i o obowiązku ich przestrzegania.
>
> (art. 9 ust. 3)

Państwa członkowskie nie mogą jednak na mocy tego przepisu nakładać warunków na odbiorców w innym państwie członkowskim, którzy są zaangażowani w sprawy sądowe lub policyjne, innych niż mających zastosowanie do „podobnego przesyłania” w odniesieniu do tego rodzaju odbiorców krajowych (art. 9 ust. 4).

(W kwestii przekazywania danych osobowych do państw spoza UE, zob. poniżej).

Treść

Wiele przepisów w LEDPD jest bardzo podobnych do przepisów RODO, ale tylko do tego stopnia, aby odzwierciedlić szczególny kontekst egzekwowania prawa i zapobiegania zagrożeniom dla bezpieczeństwa publicznego.

[176] Komisja Europejska, Factsheet – How will the data protection reform help fight international crime? 30 kwietnia 2018 r. dostępny pod adresem: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en.

Definicje głównych pojęć w art. 3 — *„dane* osobowe", *„przetwarzanie*", *„ograniczenie przetwarzania", „profilowanie*", *„pseudonimizacja*", *„zbiór danych*", *„administrator ' 'podmiot przetwarzający*", *„odbiorca*", *„naruszenie ochrony danych* osobowych", *„dane genetyczne*", *„dane biometryczne*", *„dane dotyczące* zdrowia" – są w rzeczywistości identyczne z definicjami tych samych pojęć w RODO[177].

Zasady podstawowe, określone w art. 4, są również podobne. W szczególności zasada „**zgodności z prawem**", której brakowało w decyzji ramowej z 2008 r. - jest obecnie wyraźnie wymieniona podkreślona w art. 4 lit. a) i rozwinięta w art. 8 ust. 1 – z zasadą „przejrzystości" (która jest bezpośrednio powiązana z zasadą zgodności z prawem i rzetelności w RODO) w pewnym zakresie odzwierciedloną w art. 8 ust. 2 *(„prawo państwa członkowskiego regulujące przetwarzanie w zakresie stosowania niniejszej dyrektywy określa co najmniej powody przetwarzania, dane osobowe mają*ce *podlegać przetwarzaniu oraz cele przetwarzania*") oraz w przepisach dotyczących informowania osób, których dane dotyczą, oraz dotyczących udzielania dostępu do ich danych (chociaż w szczególnym kontekście LEDPD prawa te są objęte szerszymi ograniczeniami).

Zasada ograniczenia celu jest ograniczona w tym sensie, że dane osobowe gromadzone przez dowolne z wyżej wymienionych właściwych organów do celów egzekwowania prawa lub bezpieczeństwa publicznego mogą być wykorzystywane do innych celów, o ile jest to *„dozwolone* [każdym] *prawem Unii lub prawem państwa członkowskiego*" (art. 9 ust. 1 zdanie pierwsze), z zastrzeżeniem postanowienia zawartego w art. 9 u t. 1 zdanie drugie:

> Jeżeli przetwarzanie danych osobowych odbywa się w takich innych celach, zastosowanie ma rozporządzenie (UE) 2016/679 [RODO], chyba że przetwarzanie odbywa się w toku działalności nieobjętej prawem Unii[178].

Z powyższego wynika, że wszelkie dane dotyczące egzekwowania prawa udostępnione na podstawie takiego prawa „zezwalającego" muszą być ograniczone do tego, co jest „istotne" i „niezbędne" dla „zgodnego z prawem" celu, do którego dąży prawo zezwalające. **Co do zasady, ważną rolę odgrywa tu inspektor ochrony danych (IOD), działający odpowiednio na rzecz podmiotów ujawniających i odbierających.** Jednak w niektórych krajach prawo może po prostu stanowić, że niektóre dane dotyczące egzekwowania prawa muszą, w pewnych określonych okolicznościach (np. w przypadku uzyskania zgody urzędnika wyższego szczebla) zostać udostępnione organom niebędących organami ścigania[179].

Dyrektywa wymaga od państw członkowskich ustalenia **okresów zatrzymywania danych** w odniesieniu do danych przetwarzanych na podstawie dyrektywy (art. 5); oraz **wyraźnego rozróżnienia** między danymi osobowymi różnych **kategorii osób, których dane dotyczą**, takimi jak osoby podejrzane, osoby skazane za czyn zabroniony, ofiary, świadkowie itp. (art. 6); oraz przewiduje, że *„Państwa członkowskie zapewniają, by dane osobowe oparte na faktach były rozróżniane, tak dalece, jak to możliwe z danymi osobowymi opartymi na indywidualnych ocenach*" (art. 7 ust. 1).

Również LDPD (podobnie jak RODO) wymaga od **administratorów danych** zapewnienia **bezpieczeństwa z uwzględnieniem „stanu wiedzy technicznej",** kontekstu i celów

[177] Co dziwne, przy określeniu wszystkich wyżej wymienionych definicji koniecznie w identyczny sposób jak w RODO, LEDPD nie definiuje pojęcia „strona trzecia" – mimo że inna definicja („odbiorcy") wyraźnie wymienia strony trzecie.
[178] Zob. również art. 9 ust. 2. Jest to ponownie omówione w podsekcji 1.4.6 poniżej.
[179] Por. dyskusja na temat (proponowanej wówczas) szeroko zakrojonej wymiany danych na temat małoletnich w Wielkiej Brytanii między organami pomocy społecznej, oświatowymi i policyjnymi w Ross Anderson *i in.,* Children's Databases – Safety and Privacy: A Report for the Information Commissioner, raport przygotowany przez Foundation for Information Policy Research Zjednoczonego Królestwa (FIPR), 2006 r., który zawiera streszczenia: Douwe Korff, nie tylko odnośne przepisy prawne w zakresie ochrony danych obowiązujące w Zjednoczonym Królestwie (*Data Protection Rules and Principles Relating to Data Sharing*, s. 100 i nast.), ale także (w załączniku) przegląd *Regulation Elswhere in Europe* [uregulowania gdzie indziej w Europie], w szczególności w Niemczech i Francji, dostępne na stronie internetowej https://www.cl.cam.ac.uk/~rja14/Papers/kids.pdf.

przetwarzania danych (art. 29 ust. 1), oraz wymaga, aby administratorzy dokonali **oceny ryzyka** w tym zakresie, w celu ustalenia, jaki poziom bezpieczeństwa jest właściwy (art. 29 ust. 2). Ponadto (podobnie jak RODO) wymaga także bezpieczeństwa fizycznego i technicznego (*idem*) oraz nałożenia na pracowników **obowiązku zachowania poufności** (art. 23).

Podobnie jak w RODO, **naruszenia ochrony danych osobowych** muszą być zgłaszane organowi nadzorczemu w ciągu 72 godzin (lub jeżeli nie dokonano tego w tym okresie, opóźnienie musi być uzasadnione) (art. 30); a osoby, których dane dotyczą, należy o tym fakcie zawiadomić „*bez zbędnej zwłoki*", „*w przypadku gdy naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych*" (art. 31).

Zasady zawarte w LEDPD dotyczące przetwarzania **danych szczególnie chronionych** — tj. „danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe lub przynależność do związków zawodowych", danych genetycznych, danych biometrycznych (wykorzystywanych w celu jednoznacznego zidentyfikowania osoby fizycznej), „danych dotyczących zdrowia" i „danych dotyczących seksualności i orientacji seksualnej osoby fizycznej" – są sformułowane nieco inaczej niż te zawarte w RODO (art. 9)[180], ponieważ LEDPD zezwala na przetwarzanie takich danych:

> **wyłącznie wtedy,** jeżeli **jest to bezwzględnie niezbędne**, podlega **odpowiednim zabezpieczeniom** dla praw i wolności osoby, której dane dotyczą, oraz:
>
> (a) jest **dopuszczone prawem** Unii lub prawem państwa członkowskiego;
>
> (b) jest niezbędne dla ochrony **żywotnych interesów** osoby fizycznej, której dane dotyczą, lub innej osoby; lub
>
> (c) takie przetwarzanie dotyczy danych osobowych w **sposób oczywisty upublicznionych przez osobę, której dane dotyczą**.
>
> (art. 10 LEDPD, dodano podkreślenie)

Te dwa warunki odpowiadają wyjątkom w RODO (odpowiednio art. 9 ust. 2 lit. c) i e))[181].

W przypadku gdy państwo członkowskie powołuje się na inny warunek — **dopuszczenie na mocy prawa** — musi być w stanie wykazać, że przetwarzanie danych jest „***bezwzględnie niezbędne***" oraz że wszelkie ograniczenia związane z prawami osoby, której dane dotyczą, „***podlegają odpowiednim zabezpieczeniom***". Ponadto (inaczej niż w sytuacji przewidzianej w decyzji ramowej Rady z 2008 r.) osoby fizyczne mogą obecnie powoływać się na dyrektywę w celu dochodzenia swoich praw, przy czym Trybunał Sprawiedliwości Unii Europejskiej może ostatecznie ustalić, czy jakiekolwiek przepisy krajowe przyjęte w tym kontekście spełniają kryterium „*bezwzględnej niezbędności*" i zawierają „*odpowiednie zabezpieczenia*"; a Komisja jest uprawniona do podejmowania działań w zakresie egzekwowania prawa, jeżeli uważa, że prawo państwa członkowskiego dopuszczające przetwarzanie danych szczególnie chronionych na potrzeby egzekwowania prawa/bezpieczeństwa publicznego nie spełnia tych kryteriów.

Również LEDPD, podobnie jak RODO, reguluje **zautomatyzowane podejmowanie decyzji**, **w tym profilowanie,** ale z pewnymi różnicami. Dyrektywa ta stanowi w szczególności, że takie przetwarzanie musi być „*dozwolone prawem Unii lub prawem państwa członkowskiego*" i musi

[180] LEDPD oczywiście nie zawiera przepisu opartego na art. 10 zdanie pierwsze RODO, stanowiącego, że przetwarzania danych osobowych dotyczących wyroków skazujących oraz czynów zabronionych wolno dokonywać *„wyłącznie pod nadzorem władz publicznych lub [...] dozwolone prawem Unii lub prawem państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw i wolności osób, których dane dotyczą*": zapewniają to zarówno LEDPD, jak i odpowiednie przepisy krajowe. Podobnie nie ma potrzeby powtarzania w LEDPD zapisu zawartego w ostatnim zdaniu art. 10 RODO, zgodnie *z którym „Wszelkie kompletne rejestry wyroków skazujących są prowadzonie wyłącznie pod nadzorem władz publicznych*".

[181] Z wyjątkiem tego, że wyjątek dotyczący przetwarzania danych w celu ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby na podstawie art. 9 ust. 2 lit. c) RODO ma zastosowanie wyłącznie wtedy, gdy *„osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody*" – co nie jest wymagane na podstawie LEDPD.

podlegać „*odpowiednim zabezpieczeniom*", które muszą obejmować „*co najmniej prawo do uzyskania interwencji ludzkiej ze strony administratora*". Jednak w przeciwieństwie do RODO, LEDPD nie stanowi, że w przypadku występowania takiej „interwencji ludzkiej " osoba, której dane dotyczą, powinna mieć możliwość „*wyrażenia własnego stanowiska i [...] zakwestionowania tej decyzji [zautomatyzowanej/opartej na profilowaniu]*".

W szczególności LEDPD stwierdza, że:

> **Profilowanie skutkujące dyskryminacją osób fizycznych na podstawie danych osobowych szczególnych kategorii, o których mowa w art. 10, jest zabronione** zgodnie z prawem Unii. (dodano podkreślenie)

W odniesieniu do kwestii „dopuszczenia na mocy prawa" ważne jest również uwzględnienie faktu, że podczas opracowywania wniosku ustawodawczego w tej sprawie **należy konsultować się z** właściwym **organem ochrony danych** państwa członkowskiego (art. 28 ust. 2).

Inspektorzy ochrony danych we właściwych organach muszą dokładnie rozważyć, w jaki sposób te istotne nowe wymogi LEDPD – interwencja ludzka i obowiązek niedyskryminacji – mogą być rzeczywiście i skutecznie stosowane w praktyce w różnych kontekstach.

Biorąc pod uwagę zakres jej zastosowania, LEDPD zezwala na dość znaczne **ograniczenia praw osoby, której dane dotyczą,** do uzyskania informacji na temat przetwarzania, dostępu do swoich danych oraz do sprostowania lub usunięcia danych, które nie spełniają odpowiednich norm jakości danych, lub są w inny sposób przetwarzane niezgodnie z zasadami określonymi w instrumencie – ale ograniczenia te muszą być ograniczone do tego, co jest „niezbędne" i „proporcjonalne" w społeczeństwie demokratycznym (zob. w szczególności art. 12 – 16 LEDPD i art. 15). LEDPD umożliwia również wykonywanie tych praw w sposób **pośredni**, za pośrednictwem właściwego organu nadzorczego (art. 17). Jeżeli dane osobowe „*znajdują się w orzeczeniu sądu, protokole lub aktach sprawy przetwarzanych w toku postępowania przygotowawczego lub sądowego w sprawie karnej*", prawa te mogą również być uregulowane we właściwych przepisach prawa krajowego (art. 18). Zazwyczaj **przepisy prawne dotyczące policji lub kodeksy postępowania karnego** regulują dostęp podejrzanego, oskarżonego, osoby, której postawiono zarzuty, osoby postawionej w stan oskarżenia lub skazanego do określonych części właściwych akt na niektórych etapach postępowania (zazwyczaj umożliwienie ograniczonego dostępu na wczesnych etapach i szerokiego dostępu w późniejszym terminie, w szczególności gdy dana osoba jest formalnie postawiona w stan oskarżenia) i w związku z tym takie ustalenia mogą zostać zachowane.

Wymogi praktyczne i formalne

Również w wielu innych kwestiach LEDPD wprowadza wymogi praktyczne i formalne podobne do wymogów RODO.

Przede wszystkim, podobnie jak RODO, LEDPD zawiera nową **zasadę rozliczalności** (art. 4 ust. 4)[182] i wymaga, aby „*uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia"*, wszyscy administratorzy objęci tą dyrektywą:

> ... wdrażali odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszą dyrektywą i **aby móc to wykazać**.
>
> (art. 19 ust. 1, dodano podkreślenie)

W artykule tym dodano, że „*środki te są w razie potrzeby poddawane przeglądom i uaktualniane*"; oraz że „w *stosownych przypadkach*" muszą one obejmować (opracowanie, przyjęcie i) wdrożenie przez administratora „*odpowiednich polityk ochrony danych*" (art. 19 ust.

[182] Szczegółowo omówiono w części drugiej, sekcja 2.3 poniżej.

1 ostatnie zdanie i ust. 2).

Ponadto, podobnie jak w przypadku RODO, LEDPD wymaga rozbudowanego **prowadzenia wykazów i ewidencjonowania** (art. 24 i 25), które są ważnymi środkami zapewnienia możliwości weryfikacji legalności przetwarzania danych, co stanowi szczególne wyzwanie w obszarze stosowania LEDPD.

LEDPD określa te same wymogi co RODO w odniesieniu do „**współadministratorów**" (art. 21 ust. 1) oraz do korzystania z usług podmiotów przetwarzających (art. 22).

LEDPD wymaga przeprowadzenia **oceny skutków dla ochrony danych („DPIA",** art. 27**)** w podobnych okolicznościach, jakie przewidziano w RODO, tj.:

> Jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele **może skutkować powstaniem wysokiego ryzyka naruszenia praw i wolności osób fizycznych** (art. 27, dodano podkreślenie).

Należy skonsultować się również z właściwym **organem nadzorczym** (którym może być ogólny krajowy organ ochrony danych, ale również odrębny organ, o ile spełnione są warunki niezależności itp.: zobacz poniżej), jeżeli ocena skutków dla ochrony danych *„wykaże, że przetwarzanie powodowałoby wysokie ryzyko naruszenia w razie niepodjęcia przez administratora środków w celu zminimalizowania tego ryzyka*" lub gdy (niezależnie od takich środków) *„odnośny rodzaj przetwarzania – zwłaszcza z użyciem nowych technologii, mechanizmów lub procedur – stwarza poważne ryzyko naruszenia praw i wolności osób, których dane dotyczą"* (art. 28 ust. 1 lit. a) i b)).

Jako środek przyczyniający się do jej skutecznego stosowania, w szczególności w odniesieniu do zasady rozliczalności, LEPDP przewiduje wyznaczenie przez każdego administratora **inspektora ochrony danych (IOD)** (art. 32), wyjaśnia stanowisko IOD (art. 33) i wymienia zadania IOD (art. 34). Jest to również zgodne z RODO, które wymaga wyznaczenia IOD przez wszystkie podmioty sektora publicznego objęte tym rozporządzeniem[183]. Jednak LEDPD nie przewiduje wyraźnie, że inspektor ochrony danych musi być w stanie działać w sposób niezależny[184].

Inspektorzy ochrony danych w organach ds. egzekwowania prawa oraz wszelkich innych agencjach lub organach podlegających LEDPD będą miały do odegrania ważną rolę w odniesieniu do przestrzegania przez ich organizacje zasady rozliczalności oraz odpowiednich bieżących przeglądów środków podjętych w celu zastosowania się do tej zasady; opracowania „ustaleń" z jakimkolwiek współadministratorem oraz umów z podmiotami przetwarzającymi; konsultacji z organami ochrony danych; oraz przeprowadzenia ocen skutków dla ochrony danych na mocy LEDPD[185].

Międzynarodowe przekazywanie danych właściwym organom w państwach trzecich

Ze względu na wysoki stopień wrażliwości kontekstu oraz danych osobowych w tej dziedzinie, rozdział V LEDPD przewiduje szereg warunków przekazywania danych osobowych do państwa spoza UE („państwa trzeciego") lub organizacji międzynarodowej, podobnych do warunków przekazywania danych w RODO, ale z dodatkowymi przepisami dotyczącymi przekazywania do państwa trzeciego lub organizacji międzynarodowej przez państwo członkowskie UE danych osobowych otrzymanych od innego państwa członkowskiego oraz dalszego przekazywania danych przez państwo trzecie będące odbiorcą danych do innego państwa trzeciego lub do

[183] Zob. Część druga sekcja 2.4.2 poniżej.

[184] Por. art. 38 ust. 3 RODO, który stanowi, że: *„Administrator lub podmiot przetwarzający zapewniają, by inspektor ochrony danych nie otrzymywał instrukcji dotyczących wykonywania tych zadań. Nie jest on odwoływany ani karany przez administratora ani podmiot przetwarzający za wypełnianie swoich zadań. Inspektor ochrony danych bezpośrednio podlega najwyższemu kierownictwu administratora lub podmiotu przetwarzającego*."

[185] Por. szczegółowe omówienie zadań IOD na mocy RODO w części trzeciej niniejszego Podręcznika.

organizacji międzynarodowej – oraz z bardziej szczegółowymi wyjątkami ze szczególnych powodów, jak omówiono poniżej.

Należy jednak zauważyć, że w szczególności w odniesieniu do międzynarodowego przekazywania danych LEDPD pozwala na przedłużające się opóźnienia w pełnym stosowaniu zasad omówionych poniżej, ze szczególnych powodów, jak omówiono w punkcie *„Opóźniona transpozycja*" na końcu tej sekcji dotyczącej LEDPD.

Ogólne warunki wstępne takiego przekazywania:

W art. 35 LEDPD **określono trzy warunki wstępne** dotyczące przekazywania danych do państwa trzeciego (należy jednak zauważyć, *że dwa z nich mogą zostać uchylone w pewnych okolicznościach*, jak wskazano):

- przekazanie musi być „**niezbędne**" do celów, o których mowa w art. 1 ust. 1, tj. do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom;

- przekazanie musi następować do **organu w państwie trzecim lub organizacji międzynarodowej właściwej dla wyżej wymienionych celów** (przy czym Międzynarodowa Organizacja Policji Kryminalnej, Interpol, jest wyraźnie wymieniona w motywie (25))[186]. Podobnie jak „właściwe organy" w UE nie ograniczają się do organów ścigania działających na pierwszej linii, organy w państwach trzecich, którym mogą zostać przekazane dane, również nie muszą być organami ścigania działającymi w pierwszej linii, o ile są one właściwe (również) w odniesieniu do odpowiednich spraw karnych.

  Należy zauważyć, że *w niektórych sytuacjach można odstąpić od tego warunku wstępnego* pod pewnymi warunkami, jak omówiono poniżej w punkcie „*Przekazywanie do innych organów*".

- *„w przypadku przesyłania lub udostępniana danych od innego państwa członkowskiego, to inne państwo członkowskie wyraziło na przekazanie **uprzednią zgodę** zgodnie ze swoim prawem krajowym*" (z zastrzeżeniem wyjątku, o którym mowa poniżej).

  (art. 35 ust. 1 lit. a) – c))

  Ten ostatni przepis dotyczy przekazania z jednego państwa członkowskiego do państwa trzeciego lub organizacji międzynarodowej danych osobowych pierwotnie otrzymanych

[186] W tym względzie można zauważyć, że **Interpol** nie jest „organizacją międzynarodową", zgodnie ze zwyczajową definicją w międzynarodowym prawie publicznym, tj. organizacją opartą na umowie lub w inny sposób ustanowioną na mocy prawa międzynarodowego: zob. art. 2 projektu artykułów Komisji Prawa Międzynarodowego dotyczącego obowiązków organizacji międzynarodowych. Natomiast Interpol został utworzony przez organy policji uczestniczących państw. W tej sprawie zob. pytanie przedłożone Komisji przez Charlesa Tannocka w dniu 15 października 2013 r., dostępne na stronie internetowej: https://www.europarl.europa.eu/sides/getDoc.do?type=WQ&reference=E-2013-011707&language=EN — oraz odpowiedź udzielona przez Komisję, zob. na stronie internetowej: https://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2013-011707&language=EN. Jednak Interpol nadal jest często traktowany jako organizacja międzynarodowa, również w pewnym stopniu przez UE, która przyjęła wspólne stanowisko Rady w sprawie wymiany danych o paszportach z Interpolem i państwami członkowskimi Interpolu, z zastrzeżeniem gwarancji ochrony danych: Wspólne stanowisko Rady 2005/69/JHA z dnia 24 stycznia 2005 r. w sprawie wymiany niektórych danych z Interpolem, Dz.U. L 27 z 29 stycznia 2005 r. s. 61, dostępne pod adresem: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32005E0069 (w sprawie ochrony danych, zob. art. 3). Zob. również decyzja Rady 2007/533/JHA z dnia 12 czerwca 2007 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II), Dz.U. L 205 z 7 sierpnia 2007 r. s. 63, która zakazuje przekazywania lub udostępniania danych SIS II państwom trzecim i organizacjom międzynarodowym (art. 54), ale wprowadza wyjątek dotyczący wymiany z Interpolem danych na temat skradzionych, przywłaszczonych, utraconych lub unieważnionych paszportów (art. 55), zob. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32007D0533. Motyw (25) LEDPD sugeruje, że w ramach tego instrumentu można dokonywać wymianych większej ilości danych osobowych z Interpolem i za pośrednictwem Interpolu, o ile spełnione są ogólne warunki przekazywania danych organizacjom międzynarodowym (i państwom trzecim) określone w dyrektywie (jak omówiono w powyższym tekście).

z innego państwa członkowskiego, tj. dalsze przekazywanie takich danych wymaga „uprzedniej zgody" państwa członkowskiego, które pierwotnie przekazało dane.

Uwaga: *ta uprzednia zgoda nie jest wymagana, jeżeli*:

> przekazanie danych osobowych jest **niezbędne do zapobieżenia bezpośredniemu, poważnemu zagrożeniu dla bezpieczeństwa publicznego w państwie członkowskim lub państwie trzecim bądź dla ważnych interesów państwa członkowskiego,** a uprzedniej zgody nie da się uzyskać w odpowiednim terminie.

W takim przypadku „*organ odpowiadający za wydanie uprzedniej zgody [czytaj: organ, który powinien był zostać poproszony o wydanie uprzedniej zgodę, jeżeli nie było takiego bezpośredniego zagrożenia], zostaje **powiadomiony** bez zbędnej zwłoki*" (art. 35 ust. 2, dodano podkreślenie).

Po spełnieniu tych warunków wstępnych dane osobowe mogą zostać przekazane do państwa trzeciego lub organizacji międzynarodowej tylko wtedy, gdy spełniony **jest jeden z następujących trzech warunków**:

- Komisja wydała **decyzję stwierdzającą odpowiedni stopień ochrony** w odniesieniu do będącego odbiorcą państwa trzeciego lub organizacji międzynarodowej (zgodnie z dalszymi przepisami art. 36).

  Należy jednak zauważyć*, że Komisja Europejska nie podjęła jeszcze takich decyzji stwierdzających odpowiedni stopień ochrony na mocy dyrektywy, w* związku z czym nie można jeszcze powoływać się na tę klauzulę.

  <u>Lub</u>:

- Wprowadzono „**odpowiednie zabezpieczenia**", aby zapewnić, że dane osobowe, po ich przekazaniu, będą nadal przetwarzane zgodnie z „odpowiednimi" zabezpieczeniami ochrony danych.

  Wyjaśniono to dokładniej w art. 37, który stanowi, że odpowiednie zabezpieczenia muszą być wprowadzone **w prawnie wiążącym akcie** (który może być traktatem lub wiążącym prawnym porozumieniem administracyjnym) (art. 37 ust. 1 lit. a)) lub *„administrator **ocenił** [musiał ocenić] wszystkie okoliczności związane z przekazaniem danych osobowych i [stwierdził,] że istnieją odpowiedne zabezpieczenia ochrony danych* osobowych" (art. 37 ust. 1 lit. b)) – jednak w tym drugim przypadku **organ nadzorczy** musi zostać poinformowany o „kategoriach przekazań" dokonanych na podstawie tej klauzuli. Ponadto każde takie przekazanie musi być *„udokumentowane, a dokumentacja, w tym data i godzina przekazania, informację o właściwym organie odbierającym, uzasadnienie przekazania oraz przekazane dane osobowe, musi zostać udostępniona na żądanie organowi nadzorczemu "* – art. 37 ust. 3.

  Należy zauważyć, że wspomniane „**prawnie wiążące akty**" obejmują „*umowy międzynarodowe, które przewidują przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych i które zostały zawarte przez państwa członkowskie przed dniem 6 maja 2016 r.*", o których mowa w art. 61 LEDPD. Zgodnie z tym artykułem umowy te „*pozostają w mocy do czasu ich zmiany, zastąpienia lub uchylenia*", o ile „*są zgodne z prawem Unii mającym zastosowanie przed tą datą*". LEDPD nie wyznacza daty, do której umowy te, jeżeli nie są zgodne z zasadami zawartymi w LEDPD, powinny zostać zmienione, zastąpione lub uchylone, ani nawet nie określa, że państwa członkowskie muszą dokonać ich przeglądu w tym celu. Kwestia ta została szerzej omówiona poniżej w punkcie „*Opóźnione wdrożenie*".

  Należy również zauważyć, że alternatywne „**odpowiednie zabezpieczenia**" odnoszą się wyłącznie do ochrony danych: nie istnieje wymóg (taki jak ten nakładany w ramach dwóch pierwszych wyjątków omówionych w dalszej kolejności), że zostanie przeprowadzona ocena możliwego wpływu na inne „podstawowe prawa i wolności" osoby, której dane dotyczą, a jeśli tak, to czy mogą one „być nadrzędne wobec interesu publicznego przemawiającego za

przekazaniem";

Lub:

- (w przypadku braku decyzji stwierdzającej odpowiedni stopień ochrony na podstawie art. 36 i braku odpowiednich zabezpieczeń zgodnie z art. 37), jeżeli **zastosowanie ma wyjątek w szczególnej sytuacji**. Art. 38 dopuszcza takie wyjątki, jeżeli przekazanie jest „**niezbędne**" **w pięciu sytuacjach**, z których dwie wymagają „wyważenia" interesów. W innej kolejności niż w artykule, szczególne sytuacje i warunki są następujące:

  - Dane osobowe mogą być przekazywane do państwa trzeciego bez decyzji stwierdzającej odpowiedni stopień ochrony i bez odpowiednich zabezpieczeń, jeżeli jest to „**niezbędne**" do któregokolwiek z celów określonych w art. 1 ust. 1, tj. **do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w tym ochrony przed (prawnokarnymi) zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom** (art. 38 ust. 1 lit. d)), chyba że:

    właściwy organ przekazujący stwierdzi, że podstawowe prawa i wolności konkretnej osoby, której dane dotyczą, są nadrzędne wobec interesu publicznego przemawiającego za przekazaniem (art. 38 ust. 2).

  - Dane osobowe mogą być przekazywane do państwa trzeciego bez decyzji stwierdzającej odpowiedni stopień ochrony i bez odpowiednich zabezpieczeń, jeżeli jest to **„niezbędne"** dla **ustalenia, dochodzenia lub obrony roszczeń** odnoszących się do któregokolwiek z wyżej wymienionych celów (art. 38 ust. 1 lit. e)) – ponownie, chyba że:

    właściwy organ przekazujący stwierdzi, że podstawowe prawa i wolności konkretnej osoby, której dane dotyczą, są nadrzędne wobec interesu publicznego przemawiającego za przekazaniem (art. 38 ust. 2).

    Należy zauważyć, że powyższe dwie sytuacje odnoszą się do przypadków, w których występują poważne problemy w zakresie praw człowieka: z jednej strony przekazanie jest „niezbędne" dla ważnego interesu publicznego, ale z drugiej strony wpływa na podstawowe prawa i wolności osoby, której dane dotyczą – być może w możliwie najgorszy sposób, na przykład gdy informacje na temat podejrzanego, świadka lub ofiary są przekazywane organom w państwie, które poważnie narusza prawa człowieka; nie istnieją „odpowiednie zabezpieczenia", nawet w odniesieniu do (dalszego) przetwarzania danych osobowych osoby, której dane dotyczą. **Oczywiście w przypadku takiego przekazywania należy skonsultować się z inspektorem ochrony danych właściwego organu, który będzie znacznie obciążony w zakresie doradztwa w tym względzie.**

  - Dane osobowe mogą być przekazywane do państwa trzeciego bez decyzji stwierdzającej odpowiedni stopień ochrony i bez odpowiednich zabezpieczeń, jeżeli jest to **« niezbędne » dla zapobieżenia bezpośredniemu, poważnemu ryzyku naruszenia bezpieczeństwa publicznego państwa członkowskiego lub państwa trzeciego** (art. 38 ust. 1 lit. c)) — *w tym przypadku niezależnie od uwzględnienia podstawowych praw i wolności osoby, której dane dotyczą (chyba że można to interpretować jako „niezbędność"?)*.

  - Dane osobowe mogą być przekazywane do państwa trzeciego bez decyzji stwierdzającej odpowiedni stopień ochrony i bez odpowiednich zabezpieczeń, jeżeli jest to **« niezbędne » w celu ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby** (art. 38 ust. 1) lit. a)).

  - Dane osobowe mogą być przekazywane do państwa trzeciego bez decyzji

stwierdzającej odpowiedni stopień ochrony i bez odpowiednich zabezpieczeń, jeżeli jest to „**niezbędne**" **w celu zabezpieczenia uzasadnionych interesów osoby, której dane dotyczą, jeżeli prawo państwa członkowskiego przekazującego dane osobowe tak stanowi** (art. 38 ust. 1 lit. b)).

Dane przekazane na podstawie któregokolwiek z powyższych pięciu wyjątków muszą być ***„ściśle niezbędne"*** (motyw (72)) i muszą być **udokumentowane**, a:

> dokumentacja, w tym data i godzina przekazania, informacje o właściwym organie odbierającym, uzasadnienie przekazania oraz przekazane dane osobowe, **musi zostać udostępniona na żądanie organowi nadzorczemu**. (art. 38 ust. 3, dodano podkreślenie)

Celem tej dokumentacji i jej dostępności dla organu nadzorczego jest umożliwienie organowi nadzorczemu (z mocą wsteczną) „*kontroli zgodności przekazania z prawem*" (motyw (72)). Motyw (72) dodaje, że:

> [Wyjątki wymienione powyżej] należy **interpretować wąsko i nie powinny one umożliwiać częstego, masowego i zorganizowanego przekazywania** danych osobowych ani przekazywania danych na dużą skalę; powinny też być ograniczone do danych ściśle niezbędnych].

Ponownie każdy inspektor ochrony danych w każdej właściwej organizacji będzie miał istotne obowiązki związane z tą dokumentacją oraz we wszelkich kontaktach dotyczących istotnych kwestii z organem nadzorczym[187]**.**

Przekazywanie danych innym organom w państwach trzecich

Jak zauważono wcześniej, zasadniczo wszystkie wyżej wymienione rodzaje przekazywania mogą być dokonywane wyłącznie na rzecz organów w danym państwie trzecim, którym przyznano kompetencje w odniesieniu do celów wymienionych w art. 1 ust. 1 dyrektywy, tj. w odniesieniu *do „zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania [karnoprawnego?] takim zagrożeniom*" (art. 35 ust. 1 lit. b)) (mimo że odbiorcy nie muszą być właściwymi organami ścigania; mogą nimi być inne organy publiczne posiadające pewne zadania i uprawnienia związane z przestępczością lub bezpieczeństwem publicznym).

Jednakże art. 39 LEDPD zatytułowany *„Przekazywanie danych osobowych odbiorcom mającym siedzibę w państwach* trzecich" (chodzi o odbiorców innych niż organy, które w danym państwie trzecim są właściwe do spraw wymienionych w art. 1 ust. 1 dyrektywy) **dopuszcza wyjątki** od tej zasady.

W motywie (73) wyjaśniono przyczyny tych wyjątków (przerwy w ustępie i dodano podkreślenie):

> Właściwe organy państw członkowskich stosują obowiązujące dwustronne lub wielostronne umowy międzynarodowe zawarte z państwami trzecimi w dziedzinie współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej, by wymieniać istotne informacje do wykonywania prawnie ciążących na nich obowiązków. Odbywa się to zasadniczo dzięki współpracy właściwych organów państw trzecich prowadzonej na potrzeby niniejszej dyrektywy, lub przynajmniej we współpracy z tymi organami, czasami nawet przy braku odpowiedniej dwustronnej lub wielostronnej umowy międzynarodowej.
>
> **Niemniej w konkretnych indywidualnych przypadkach rutynowy tryb postępowania wymagający skontaktowania się z takim organem z państwa trzeciegom może okazać**

[187] Zob. Część trzecia niniejszego Podręcznika, *Zadania IOD,* Zadania 1 – 5 i 12.

się nieskuteczny lub niewłaściwy, w szczególności ze względu na to, że przekazanie mogłoby ulec opóźnieniu, lub dlatego, że organ [czytaj : właściwy organ ścigania] w państwie trzecim nie przestrzega praworządności lub międzynarodowych norm i standardów ochrony praw człowieka – w takiej sytuacji właściwe organy państw członkowskich mogą podjąć decyzję, że dane osobowe przekazane zostaną bezpośrednio odbiorcom [czytaj: innym podmiotom niebędącym organami ścigania] znajdującym się w takich państwach trzecich.

Może się tak zdarzyć wówczas, gdy zachodzi pilna potrzeba przekazania danych osobowych w celu ratowania życia osobie zagrożonej czynem zabronionym, lub gdy jest to konieczne do zapobieżenia spodziewanemu popełnieniu czynu zabronionego, w tym czynu terrorystycznego.

Nawet jeżeli takie przekazanie między organami a odbiorcami mającymi siedzibę w państwach trzecich miałoby się odbywać tylko w konkretnych indywidualnych przypadkach, niniejsza dyrektywa powinna wskazać zasady służące uregulowaniu takich przypadków.

Takich przepisów nie należy uznawać za wyjątki od obowiązujących dwustronnych lub wielostronnych umów międzynarodowych w dziedzinie współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej. Zasady te powinny obowiązywać obok pozostałych przepisów niniejszej dyrektywy, zwłaszcza przepisów o zgodności przetwarzania z prawem i przepisów rozdziału V.

Art. 39 ust. 1 można sparafrazować następująco[188]:

Prawo Unii lub prawo państwa członkowskiego mogą przewidywać, że organy ścigania – w indywidualnych i szczególnych przypadkach – przekazują dane osobowe bezpośrednio odbiorcom mającym siedzibę w państwach trzecich, które nie są właściwe w sprawach karnych i sprawach związanych z bezpieczeństwem publicznym, ale tylko wtedy, gdy spełnione są inne przepisy niniejszej dyrektywy i spełnione są wszystkie następujące warunki: ...

LEDPD nie wypowiada się na temat dokładnego charakteru właściwych „innych organów". Biorąc pod uwagę, że art. 39 ma zastosowanie do sytuacji mających szczególnie istotne znaczenie dla ochrony praw człowieka (zob. zdanie zaznaczone wytłuszczonym drukiem w cytacie z motywu (73) powyżej), zakłada się, że przewidywani są odbiorcy w państwie trzecim, w którym organ przekazujący we właściwym państwie członkowskim UE **posiada szczególne zaufanie**. W szczególności organ przekazujący musi mieć pewność, że odbiorca, który nie jest organem ścigania, nie przekaże informacji do organu ścigania w państwie trzecim, który „ *nie przestrzega praworządności lub międzynarodowych norm i standardów ochrony praw człowieka*". Odpowiednia ocena poszczególnych przypadków będzie zawsze wymagała indywidualnego podejścia, co powinno być co najmniej **dokładnie udokumentowane** (w tym powody, dla których dane mogą zostać przekazane zaufanemu organowi bez obawy, że trafiają one w ręce bardziej podejrzanym organów w danym państwie trzecim).

Jeżeli chodzi o przekazywanie nieobjęte umowami międzynarodowymi (jak to omówiono odrębnie poniżej), w art. 39 ust. 1 określono **pięć łącznych warunków** dotyczących określonych przypadków przekazywania. Dane mogą zostać przekazane właściwemu odbiorcy niebędącemu organem ścigania w państwie trzecim, jeżeli (dodano podkreślenia, wyjaśnienia w nawiasach kwadratowych i uwagi w ramach klauzul):

a. przekazanie jest **ściśle niezbędne** do wykonania zadania właściwego organu

[188] Art. 39 ust. 1 brzmi następująco: „ *Na zasadzie wyjątku od art. 35 ust. 1 lit. b) i z zastrzeżeniem umów międzynarodowych, o których mowa w ust. 2 niniejszego artykułu, prawo Unii lub prawo państwa członkowskiego mogą zapewniać, by właściwe organy, o których mowa w art. 3 pkt 7 lit. a), w indywidualnych, konkretnych przypadkach przekazywały dane osobowe bezpośrednio odbiorcom mającym siedzibę w państwach trzecich jedynie wówczas, gdy zachowane są pozostałe przepisy niniejszej dyrektywy i spełnione zostały wszystkie następujące warunki:...*"

przekazującego zgodnie z prawem Unii lub prawem państwa członkowskiego do celów, o których mowa w art. 1 ust. 1 **[tj. w odniesieniu do spraw karnych UE lub państw członkowskich lub spraw związanych z bezpieczeństwem publicznym**].

b. właściwy organ przekazujący stwierdza, że **podstawowe prawa i wolności danej osoby, której dane dotyczą, nie są nadrzędne wobec interesu publicznego przemawiającego za przedmiotowym przekazaniem.**

Należy zauważyć, że ustalenie to nie ogranicza się do interesów w zakresie ochrony danych osoby, której dane dotyczą, ale raczej ogólnie do tego, czy dane państwo trzecie i określone organy w tym kraju *« przestrzegają praworządności lub międzynarodowych norm i standardów ochrony praw człowieka »*. Ponadto ustalenie to powinno być dokonywane w **odniesieniu do poszczególnych przypadków**.

c. właściwy organ przekazujący uznaje, że **przekazanie organowi właściwemu do celów, o których mowa w art. 1 ust. 1** [sprawy karne i sprawy dotyczące bezpieczeństwa publicznego], w państwie trzecim byłoby **nieskuteczne lub niewłaściwe**, w szczególności dlatego, że *przekazanie nie może nastąpić w odpowiednim terminie* —

lub, co należy dodać, ponieważ byłoby to „niewłaściwe" z innych powodów: zob. uwaga przy kolejnej klauzuli.

d. **organ, który jest właściwy dla celów wskazanych w art. 1 ust. 1 w państwie trzecim**, **zostaje *poinformowany*** bez zbędnej zwłoki, chyba że byłoby to **nieskuteczne lub niewłaściwe**.

Należy zauważyć, że odniesienie do przekazywania do organu (ścigania), który normalnie byłby najwłaściwszy i najodpowiedniejszy, termin „**niewłaściwe**" może być rozumiany jako odnoszący się do sytuacji, w której ten organ „*nie przestrzega praworządności lub międzynarodowych norm i standardów ochrony praw człowieka*". Odniesienie do „**nieskuteczności**" tego organu może odnosić się do tego, że jest on *nieskuteczny, powolny, niekompetentny lub być może skorumpowany*.

e. **właściwy organ przekazujący informuje odbiorcę o konkretnym celu lub konkretnych celach, w których dane osobowe mają być wyłącznie przetwarzane przez odbiorcę, *pod warunkiem, że takie przetwarzanie jest niezbędne***.

Należy zauważyć, że oznacza to, że organ odbierający w państwie trzecim musi zapewnić (mocne i wiążące) **zapewnienia**, że będzie przestrzegał tych warunków i będzie rzeczywiście wykorzystywał dane dostarczone przez organ ścigania UE wyłącznie w konkretnym określonym celu i nie będzie ich wykorzystywał w żadnym innym celu; a nawet wówczas będzie wykorzystywał te dane wyłącznie w takim zakresie, w jakim jest to (ściśle) niezbędne do osiągnięcia określonego celu lub celów.

Oprócz spełnienia tych szczególnych warunków, jak zauważono, art. 39 ust. 1 podkreśla, *że „[wszystkie] pozostałe przepisy* niniejszej dyrektywy" również muszą być przestrzegane (zob. również ostatnie zdanie motywu (73), w którym podkreślono, że chodzi tu „zwłaszcza o przepisy o zgodności przetwarzania z prawem i przepisy rozdziału V", tj. pozostałe przepisy dotyczące przekazywania danych).

Wszystkie powyższe ustalenia pozostają jednak „**bez uszczerbku dla jakiejkolwiek umowy międzynarodowej**" (art. 39 ust. 1), przez którą należy rozumieć:

> jakąkolwiek dwustronną lub wielostronną umowę międzynarodową obowiązującą między państwami członkowskimi a państwami trzecimi dotyczącą współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej. (art. 39 ust. 2)

Powinno to być odczytywane łącznie z art. 61 LEDPD, który dotyczy *„stosunku do uprzednio zawartych umów międzynarodowych o współpracy wymiarów sprawiedliwości w sprawach*

karnych oraz o współpracy policyjnej", i który stanowi, że:

> Umowy międzynarodowe, które przewidują przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych i które zostały zawarte przez państwa członkowskie przed dniem 6 maja 2016 r. i które są zgodne z prawem Unii mającym zastosowanie przed tą datą, pozostają w mocy do czasu ich zmiany, zastąpienia lub uchylenia.

LEDPD nie określa daty, do której umowy te, o ile nie są zgodne z zasadami zawartymi w LEDPD, powinny zostać zmienione, zastąpione lub uchylone, ani nawet że państwa członkowskie muszą dokonać ich przeglądu w celu dostosowania ich do dyrektywy[189]. Jednakże art. 62 LEDPD stanowi, że:

> Do dnia **6 maja 2022 r.**, a następnie co cztery lata **Komisja** przedkłada Parlamentowi Europejskiemu i Radzie **sprawozdanie z oceny i przeglądu niniejszej dyrektywy**. Sprawozdania te są publikowane. (dodano podkreślenie)

Przeglądy te mają obejmować *„w szczególności stosowanie i funkcjonowanie rozdziału V w sprawie przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych* « (art. 62 ust. 2), „ze szczególnym uwzględnieniem" decyzji stwierdzających odpowiedni stopień ochrony na mocy art. 36 ust. 3 oraz **przekazywania danych „innym organom" na mocy art. 39**, jak to właśnie omówiono. Komisja może ponadto w tym kontekście *„wystąpić do państw członkowskich i organów nadzorczych o udzielenie informacji*" (art. 62 ust. 3), w tym, przypuszczalnie, na temat zawartych przez nie wyżej wymienionych umów międzynarodowych. Prawdopodobnie również Komisja może, na podstawie pierwszego przeglądu, **zaproponować wprowadzenie zmian** do tych umów lub przynajmniej przedstawić **sugestie** co do sposobu ich dostosowania do zasad zawartych w LEDPD, ale nie jest to przewidziane w dyrektywie (w przeciwieństwie do aktów Unii w tej dziedzinie)[190].

Według Komisji LEDPD będzie prowadzić do „**silniejszej współpracy międzynarodowej**"[191]:

> Współpraca między organami policji i wymiaru sprawiedliwości w sprawach karnych z państwami spoza UE również zostanie wzmocniona [LEDPD], ponieważ będą istniały jaśniejsze zasady międzynarodowego przekazywania danych w związku z czynami zabronionymi. Nowe przepisy zapewnią, że przekazywanie danych będzie się odbywało przy zachowaniu odpowiedniego stopnia ich ochrony.

Jednakże, jak zauważono poniżej w punkcie *„Opóźniona transpozycja*", zajmie to trochę czasu zanim nowe przepisy, o których mowa, będą miały w pełni zastosowanie.

Nadzór i egzekwowanie prawa

Rozdział VI LEDPD wymaga ustanowienia w państwach członkowskich **niezależnych organów nadzorczych** odpowiedzialnych za monitorowanie i egzekwowanie stosowania przepisów prawa krajowego przyjętych w celu wdrożenia („transpozycji") dyrektywy oraz za wykonywanie innych powiązanych zadań (zob. art. 41-46 LEDPD). Właściwym organem nadzorczym lub właściwymi organami nadzorczymi mogą, lecz nie muszą, być ogólny organ nadzorczy lub

[189] Nie są nam również znane jakiekolwiek przeglądy przeprowadzone przed wprowadzeniem LEDPD; nie wiadomo nam, czy umowy międzynarodowe obejmujące przekazywanie danych osobowych państwom trzecim lub organizacjom międzynarodowym, które zostały zawarte przez państwa członkowskie przed upływem tego terminu, są zgodne z obowiązującym wówczas prawem Unii.

[190] Art. 62 ust. 6 stanowi, **że do dnia 6 maja** 2019 r. Komisja powinna była dokonać przeglądu *takich „innych przyjętych przez Unię aktów regulujących przetwarzanie przez właściwe organy do celów określonych w art. 1 ust. 1, w tym aktów, o których mowa w art. 60, w celu oceny konieczności dostosowania ich do niniejszej dyrektywy, i w razie potrzeby przedstawia niezbędne propozycje zmiany takich aktów dla zapewnienia spójnego podejścia do ochrony danych osobowych wchodzących w zakres zastosowania niniejszej dyrektywy*".

[191] Komisja Europejska, Komisja Europejska, Factsheet – How will the data protection reform help fight international crime? (przypis 176 powyżej).

organy nadzorcze ustanowione na mocy RODO (art. 41 ust. 3): w niektórych krajach istnieją specjalne organy nadzorcze mające na celu nadzorowanie przetwarzania danych osobowych przez policję i organy ścigania, podczas gdy w innych zadanie to pełni również ogólny organ ochrony danych. Ponadto w niektórych krajach (zwłaszcza federalnych) istnieją różne organy krajowe (federalne) oraz lokalne lub regionalne.

Podobnie jak ogólne organy ochrony danych wyznaczone na mocy RODO, organy nadzorcze właściwe w sprawach objętych LEDPD muszą posiadać **szerokie uprawnienia**, w tym prawo do żądania (i uzyskania) „**dostępu do wszelkich** przetwarzanych **danych osobowych** i **wszelkich informacji** niezbędnych do wypełnienia jego zadań"; uprawnienie do wydawania ***ostrzeżeń*** administratorowi lub podmiotowi przetwarzającemu, do ***nakazania*** administratorowi lub podmiotowi przetwarzającemu ***dostosowania*** operacji do przepisów dyrektywy, *„w razie potrzeby w konkretny sposób i w konkretnym terminie, zwłaszcza poprzez nakazanie sprostowania lub usunięcia danych osobowych lub ograniczenia ich przetwarzania",* a także do ***wprowadzenia czasowych lub stałych ograniczeń przetwarzania, w tym zakazu*** przetwarzania; oraz uprawnienia do ***wszczęcia postępowania sądowego*** przeciwko administratorom lub podmiotom przetwarzającym, którzy rzekomo działali niezgodnie z dyrektywą, lub wniesienia takich spraw do właściwych organów (ścigania) (art. 47 ust. 1, 2 i 5 LEDPD). Organy nadzorcze pełnią również ważne **funkcje doradcze** i muszą mieć prawo:

> z własnej inicjatywy lub na wniosek [...] wydawać **opinie skierowane do [ich] parlamentu narodowego, rządu** lub, zgodnie z jego prawem krajowym, innych instytucji i organów oraz do społeczeństwa we wszelkich sprawach związanych z ochroną danych osobowych. (art. 47 ust. 3, dodano podkreślenie)

Muszą również publikować **roczne sprawozdanie** ze swojej działalności, *„w którym [organ nadzorczy] może wyszczególnić rodzaje zgłoszonych mu naruszeń i rodzaje nałożonych kar*" (art. 49).

Decyzje organów nadzorczych muszą jednak podlegać *„odpowiednim gwarancjom, w tym prawu do skutecznego środka prawnego przed sądem i rzetelnego procesu, określonym w prawie Unii i prawie państwa członkowskiego zgodnie z Kartą*" (art. 47 ust. 4).

W szczególności LEDPD stanowi, że:

> Państwa członkowskie zapewniają, by właściwe organy wprowadziły skuteczne mechanizmy zachęcania do poufnego zgłaszania naruszeń niniejszej dyrektywy. (art. 48)

Zapis ten jest zgodny z niedawno przyjętą dyrektywą w sprawie informowania o nieprawidłowościach[192].

Art. 50 przewiduje **wzajemną pomoc** między organami nadzorczymi państw członkowskich UE właściwymi w odniesieniu do przetwarzania danych osobowych, które podlega LEDPD.

Ponadto **Europejska Rada Ochrony Danych**, ustanowiona na mocy RODO, posiada również uprawnienia w odniesieniu do przetwarzania w ramach LEDPD (art. 51). Obejmują one opracowywanie ***wytycznych, zaleceń i najlepszych praktyk*** we wszelkich kwestiach zgłaszanych

> **opinii na potrzeby oceny, czy stopień ochrony w państwie trzecim, na terytorium lub w jednym lub więcej określonym sektorze państwa trzeciego lub w organizacji międzynarodowej jest odpowiedni**, w tym na potrzeby oceny, czy takie państwo trzecie, terytorium, określony sektor lub organizacja międzynarodowa nie przestały zapewniać

[192] Dyrektywa Parlamentu Europejskiego i Rady w sprawie ochrony osób zgłaszających przypadki naruszenia prawa Unii, 2019. W momencie przygotowywania niniejszego podręcznika tekst nie został jeszcze opublikowany w Dzienniku Urzędowym (a zatem nie ma jeszcze numeru), ale tekst w wersji przyjętej przez Parlament Europejski w dniu 16 kwietnia 2019 r. (który jest tekstem końcowym, z zastrzeżeniem wersji językowej i tłumaczenia) jest dostępny na stronie internetowej: https://www.europarl.europa.eu/doceo/document/TA-8-2019-0366_EN.html?redirect

odpowiedniego stopnia ochrony (art. 51 ust. 1 lit. g)).

Rada musi przekazywać swoje opinie, wytyczne, zalecenia i najlepsze praktyki Komisji (oraz komitetowi ustanowionemu na mocy art. 93 RODO) i podawać je do wiadomości publicznej (art. 51 ust. 3); Komisja musi z kolei informować Radę o podjętych działaniach (art. 51 ust. 4).

Środki ochrony prawnej, odpowiedzialność prawna i sankcje

W rozdziale VIII określono środki ochrony prawnej, zobowiązania i sankcje, które należy wprowadzić do przepisów krajowych transponujących LEDPD.

W skrócie, zgodnie z RODO, każda osoba, której dane dotyczą, ma **prawo wnieść skargę do** właściwego organu nadzorczego, jeżeli sądzi, że dotyczące jej przetwarzanie danych osobowych narusza przepisy przyjęte na podstawie niniejszej dyrektywy (art. 52), a także prawo do **skutecznego środka prawnego** przed sądem od prawnie wiążącej decyzji organu nadzorczego, która jej dotyczy (art. 53), oraz przeciwko każdemu administratorowi lub podmiotowi przetwarzającemu podlegającemu (prawu krajowemu transponującemu) LEDPD, *„jeżeli osoba ta uważa, iż jej prawa ustanowione w przepisach przyjętych na podstawie niniejszej dyrektywy zostały naruszone w skutek przetwarzania jej danych osobowych w sposób niezgodny z tymi przepisami*" (art. 54). Ponadto (również zgodnie z RODO):

> [...] osobie, której dane dotyczą, **prawo do umocowania organu, organizacji lub zrzeszenia** o charakterze niezarobkowym, które zostały należycie ustanowione zgodnie z prawem państwa członkowskiego, mają statutowo na celu interes publiczny i działają w dziedzinie ochrony praw i wolności osób, których dane dotyczą, w związku z ochroną ich danych osobowych, **do wniesienia w jej imieniu skargi oraz do wykonywania w jej imieniu praw, o których mowa w art. 52, 53 i 54**. (art. 55, dodano podkreślenie)

Osoby, których dane dotyczą, mają również **prawo do odszkodowania** za szkodę majątkową lub niemajątkową poniesioną w wyniku operacji przetwarzania niezgodnej z LEDPD (art. 56).

Ponadto państwa członkowskie muszą przewidzieć **„skuteczne, proporcjonalne i odstraszające" sankcje** za wszelkie naruszenia LEDPD (art. 57).

Opóźniona transpozycja

Jak już wspomniano we wcześniejszych podsekcjach, nie wszystkie operacje przetwarzania danych osobowych do celów egzekwowania prawa i bezpieczeństwa publicznego muszą być zgodne z LEDPD lub przepisami krajowymi transponującymi LEDPD: dyrektywa zawiera szereg przepisów umożliwiających dostosowanie niektórych instrumentów i operacji do dyrektywy w określonym terminie w przyszłości (lub nawet w nieokreślonym terminie w przyszłości). Przepisy umożliwiające opóźnienie wdrożenia odnoszą się do „aktów prawnych" UE; traktatów między państwami członkowskimi UE a państwami trzecimi lub organizacjami międzynarodowymi (w tym Interpolem); oraz systemów automatycznego przetwarzania danych w państwach członkowskich w dziedzinie prawa karnego i bezpieczeństwa publicznego.

Opóźnione wdrożenie przepisów w odniesieniu do unijnych aktów prawnych:

Art. 60 LEDPD stanowi w odniesieniu do około 123 instrumentów UE (różnego rodzaju „akty prawne") dotyczących wymiaru sprawiedliwości i spraw wewnętrznych (WSiSW[193]), że:

> Dyrektywa **nie wpływa** na szczegółowe przepisy o ochronie danych osobowych **w aktach prawnych Unii, które weszły w życie do dnia 6 maja 2016 r.** w dziedzinie współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej, które regulują przetwarzanie między państwami członkowskimi oraz dostęp wyznaczonych organów państw członkowskich do systemów informacyjnych ustanowionych na mocy traktatów

[193] Zob. Emilio De Capitani, o.c. (przypis 141, powyżej).

w ramach zakresu zastosowania niniejszej dyrektywy. (dodano podkreślenie)

Art. 62 ust. 6 LEDPD stanowi jednak, **że do dnia 6 maja** 2019 r. **Komisja musi** dokonać przeglądu:

> [wszelkich] innych przyjętych przez Unię aktów regulujących przetwarzanie przez właściwe organy do celów określonych w art. 1 ust. 1, w tym aktów, o których mowa w art. 60, **w celu oceny konieczności dostosowania ich do niniejszej dyrektywy, i w razie potrzeby przedstawia niezbędne propozycje zmiany takich aktów** dla zapewnienia spójnego podejścia do ochrony danych osobowych wchodzących w zakres zastosowania niniejszej dyrektywy (dodano podkreślenie).

Z powyższego wynika, że **te 123 „inne akty prawne" nie muszą być dostosowane do LEDPD do dnia 6 maja 2019 r.**: wszystko, czego się wymaga, to dokonanie ich ***przeglądu*** do tego czasu, aby w razie potrzeby ***zaproponować*** w nich zmiany. **Nie ustalono daty dokonania rzeczywistych niezbędnych zmian**, ani też przedłożenia odpowiednich, szczegółowych wniosków dla poszczególnych instrumentów[194].

W międzyczasie, jak określono w art. 60, przepisy dotyczące ochrony danych w tych około 123 aktach prawnych pozostają w mocy bez zmian i można się na nich oprzeć jako na podstawie przekazywania danych osobowych w dziedzinie prawa karnego i bezpieczeństwa publicznego, nawet jeśli nie spełniają one wymogów LEDPD, pod warunkiem, że spełnione są **trzy warunki wstępne** dotyczące takiego przekazywania danych określone w LEDPD, tj.: przekazanie jest (w opinii podmiotu przekazującego UE) „niezbędne" do celów prawa karnego lub do celów związanych z bezpieczeństwem publicznym; przekazanie odbywa się do organu w państwie trzecim posiadającego kompetencje w tych dziedzinach (chyba, że organ ten jest nieskuteczny lub jest zbyt powolny lub co gorsza: narusza prawa człowieka); oraz, jeżeli przekazane dane zostały pierwotnie uzyskane w państwie członkowskim, że to państwo członkowskie zezwoliło na przekazanie (lub w nagłych przypadkach zostało o nim przynajmniej poinformowane); oraz pod warunkiem, że ***albo*** odpowiedni instrument prawny zawiera „odpowiednie" zabezpieczenia ochrony danych ***albo*** (jeżeli instrument nie zawiera takich zabezpieczeń) *„właściwy organ przekazujący stwierdzi, że podstawowe prawa i wolności konkretnej osoby, której dane dotyczą*" nie *„są nadrzędne wobec interesu publicznego przemawiającego za przekazaniem*".

Co istotne, zgodnie z nową zasadą „**rozliczalności**", **oceny dokonane przez podmiot** — tj. czy dany instrument prawny zawiera „odpowiednie" zabezpieczenia ochrony danych, oraz czy i dlaczego interes publiczny przemawiający za przekazaniem przeważa nad potrzebą ochrony podstawowych praw i wolności osoby, której dane dotyczą – należy obecnie **rejestrować** i udostępnić na żądanie Europejskiemu Inspektorowi Ochrony Danych (i Trybunałowi).

Oczywiście każdy inspektor ochrony danych w ramach odpowiedniego właściwego podmiotu unijnego musi również odgrywać ważną rolę w tym zakresie: po pierwsze, poprzez ostrzeżenie organizacji o konieczności dokonania tych testów, a następnie poprzez wewnętrzną weryfikację, czy sprawdzenia te są stosowane, i czy są one właściwie stosowane, oraz poprzez zasięganie opinii Europejskiego Inspektora Ochrony Danych w przypadku sporu wewnętrznego lub pytań dotyczących tych kwestii.

Opóźnione wdrożenie w odniesieniu do traktatów między państwami członkowskimi UE a państwami trzecimi lub organizacjami międzynarodowymi:

Jak zauważono wcześniej, art. 61 stanowi, że:

> Umowy międzynarodowe, które przewidują przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych i które zostały zawarte przez państwa

[194] W czasie ostatniej zmiany pierwszego wydania tego Podręcznika na początku maja 2019 r. Komisja nie przedstawiła jeszcze takich propozycji.

> członkowskie przed dniem 6 maja 2016 r. i które są zgodne z prawem Unii mającym zastosowanie przed tą datą, pozostają w mocy do czasu ich zmiany, zastąpienia lub uchylenia.

W związku z tym operacje przekazywania na mocy któregokolwiek z traktatów państw członkowskich – państwa trzeciego/organizacji międzynarodowej - sprzed maja 2016 r. również mogą być na razie kontynuowane, pod warunkiem spełnienia trzech warunków wstępnych dla tego rodzaju operacji przekazywania określonych w LEDPD, tj.: przekazanie jest (w opinii organu przekazującego) „niezbędne" do celów prawa karnego lub do celów związanych z bezpieczeństwem publicznym; przekazanie odbywa się do organu w państwie trzecim posiadającego kompetencje w tych dziedzinach (chyba, że organ ten jest nieskuteczny lub jest zbyt powolny lub co gorsza: narusza prawa człowieka); oraz, jeżeli przekazane dane zostały pierwotnie uzyskane w państwie członkowskim, że to państwo członkowskie zezwoliło na przekazanie (lub w nagłych przypadkach zostało o nim przynajmniej poinformowane); oraz pod warunkiem, że ***albo*** traktat zawiera „odpowiednie" zabezpieczenia ochrony danych ***albo*** (jeżeli traktat nie zawiera takich zabezpieczeń) *„właściwy organ przekazujący stwierdzi, że podstawowe prawa i wolności konkretnej osoby, której dane dotyczą*" nie *„są nadrzędne wobec interesu publicznego przemawiającego za przekazaniem*".

Jednak ponownie, zgodnie z zasadą „**rozliczalności**" oceny organu – tj. czy traktat zawiera „odpowiednie" zabezpieczenia ochrony danych, oraz czy jest zgodny z prawem Unii sprzed maja 2016 r., bądź też czy i dlaczego interes publiczny przemawiający za przekazaniem przeważa nad potrzebą ochrony podstawowych praw i wolności osoby, której dane dotyczą – należy obecnie **rejestrować** i udostępnić na żądanie organowi nadzorczemu (i sądom).

Również w tym przypadku każdy inspektor ochrony danych w ramach odpowiedniego właściwego organu w danym państwie członkowskim będzie miał do odegrania ważną rolę.

Opóźnione wdrożenie w odniesieniu do specjalnych systemów zautomatyzowanego przetwarzania państw członkowskich w dziedzinie prawa karnego i bezpieczeństwa publicznego

Art. 63, który dotyczy w szczególności transpozycji do prawa krajowego LEDPD, stanowi w ust. 1, że[195]:

> Państwa członkowskie przyjmują i publikują do dnia 6 maja 2018 r. przepisy ustawowe, wykonawcze i administracyjne niezbędne do wykonania niniejszej dyrektywy. Tekst tych przepisów niezwłocznie przekazują Komisji. Państwa członkowskie stosują te przepisy od **dnia 6 maja 2018 r.** (dodano podkreślenie)

Zasadniczo z powyższego wynika, że „przepisy ustawowe, wykonawcze i administracyjne", o których mowa, musiały być w pełni dostosowane do LEDPD, do tej daty.

Artykuł ten przewiduje jednak w następnym ustępie następujący **wyjątek** pod pewnymi warunkami:

> W drodze wyjątku od ust. 1 państwo członkowskie może postanowić, że ***wyjątkowo, jeżeli wymaga to niewspółmiernie dużego wysiłku***, zautomatyzowane systemy przetwarzania utworzone przed dniem 6 maja 2016 r. zostają dostosowane do art. 25 ust. 1 do dnia **6 maja 2023 r**. (dodano podkreślenie)

Ustęp trzeci dopuszcza na razie dłuższe opóźnienia, z zastrzeżeniem dalszych warunków:

> W drodze wyjątku od ust. 1 i 2 niniejszego artykułu, ***w wyjątkowych okolicznościach*** państwo członkowskie może dostosować do art. 25 ust. 1 dany zautomatyzowany system

[195] Ostatni czwarty ustęp stanowi, że: *„Państwa członkowskie przekazują Komisji tekst podstawowych przepisów prawa krajowego przyjętych w dziedzinie objętej niniejszą dyrektywą*." Bardziej szczegółowy zapis w pierwszym ustępie podkreśla, że pełne zastosowanie LEDPD w rzeczywistości wymaga więcej pracy przez kilka lat, i nie będzie to jednorazowa transpozycja.

> przetwarzania, o którym mowa w ust. 2 niniejszego artykułu, **w konkretnym terminie** dłuższym niż termin, o którym mowa w ust. 2 niniejszego artykułu, ***jeżeli inaczej nastąpiłyby poważne problemy w funkcjonowaniu tego systemu***. Dane państwo członkowskie **informuje Komisję** o przyczynach tych poważnych problemów i uzasadnia konkretny termin, w którym ma dostosować dany zautomatyzowany system przetwarzania do art. 25 ust. 1. Ten konkretny termin w żadnym wypadku nie upływa później niż dnia **6 maja 2026** r**.** (dodano podkreślenie)

Wszystkie powyższe ustalenia oznaczają, że pełne zastosowanie wszystkich wymogów LEDPD, w tym w szczególności wymogów dotyczących przekazywania danych do państw trzecich i organizacji międzynarodowych, będzie jeszcze wymagało czasu.

W międzyczasie warto jednak przypomnieć, że na mocy dyrektywy (w przeciwieństwie do sytuacji wynikającej z poprzedniej decyzji ramowej Rady) zapewnienie zgodności z przepisami Unii i państw członkowskich oraz działaniami dotyczącymi spraw karnych i bezpieczeństwa publicznego jest obecnie możliwe. W ostatecznym rozrachunku obejmuje to zweryfikowanie, czy takie zasady i działania są zgodne z LEDPD, w tym zweryfikowanie, czy wyniki powyższych sprawdzeń (czy traktat zawiera „odpowiednie" zabezpieczenia ochrony danych oraz czy jest zgodny z prawem Unii sprzed maja 2016 r.; oraz czy w konkretnym przypadku interes publiczny przemawiający za przekazaniem przeważa nad potrzebą ochrony podstawowych praw i wolności osoby/osób, której/których dane dotyczą) są satysfakcjonujące; oraz w odniesieniu do wszelkich opóźnień w dostosowaniu wyżej wymienionych działań do dyrektywy, czy spełnione są szczególne warunki dotyczące takich opóźnień, określone w wyżej cytowanych ustępach.

1.4.4 Nowe instrumenty ochrony danych w obszarze wspólnej polityki zagranicznej i bezpieczeństwa (WPZiB)

Jak wyjaśnia Komisja[196]:

> Traktat z Lizbony z 2009 r. przyczynił się w dużym stopniu do wzmocnienia działań Unii w dziedzinie działań zewnętrznych. Po pierwsze, utworzył stanowisko **Wysokiego Przedstawiciela Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa**....
>
> Po drugie, w Traktacie ustanowiono **Europejską Służbę Działań Zewnętrznych (ESDZ)**. Od 2011 r. jest to zasadniczo nowa służba dyplomatyczna UE, która wspiera Wysokiego Przedstawiciela w prowadzeniu polityki zagranicznej UE. W szczególności ESDZ prowadzi sieć **141 delegatur UE** na całym świecie.
>
> ESDZ pracuje nad zapewnieniem spójności i koordynacji działań zewnętrznych Unii, przygotowywaniem wniosków politycznych i ich wdrażaniem po ich zatwierdzeniu przez Radę Europejską....
>
> Oprócz ESDZ powołano nową służbę Komisji – **Służbę ds. Instrumentów Polityki Zagranicznej (FPI)** w celu przejęcia odpowiedzialności za wydatki operacyjne.
>
> Obecnie, pod nadzorem Wysokiego Przedstawiciela i w ścisłej współpracy z delegaturami ESDZ i UE, FPI jest odpowiedzialna za... wykonanie budżetu wspólnej polityki zagranicznej i bezpieczeństwa (WPZiB) [oraz różne inne instrumenty i działania]....[197]
>
> Budżet na szeroki zakres działań zarządzanych przez FPI wynosi w 2014 r. 733 mln EUR.

Praca wykonywana przez Wysokiego Przedstawiciela, ESDZ i FPI będzie często wiązała się z przetwarzaniem danych osobowych, np. w związku z nakładaniem sankcji na osoby fizyczne lub zamrożeniem ich aktywów[198].

---

[196] Zob.: https://ec.europa.eu/fpi/about-fpi_en

[197] Wykaz linków do poszczególnych instrumentów lub działań znajduje się na stronie internetowej, o której mowa w poprzednim przypisie.

[198] Por. opinie i uwagi Europejskiego Inspektora Ochrony Danych w tej sprawie, wymienione poniżej:

Przetwarzanie takie nie podlega jednak tym samym przepisom traktatu UE, jak przetwarzanie danych przez podmioty objęte RODO, LEDPD czy nawet inne instytucje UE. Wszystkie spośród tych innych podmiotów są objęte ogólną gwarancją ochrony danych osobowych zawartą w art. 16 TFUE:

Art. 16

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.

Nie ma to jednak zastosowania do przetwarzania danych osobowych przez organy WPZiB, o których mowa powyżej, ponieważ ostatnie zdanie w art. 16 TFUE stanowi, że:

> Zasady przyjęte na podstawie niniejszego artykułu pozostają **bez uszczerbku dla zasad szczególnych** przewidzianych w **artykule** 39 Traktatu o Unii Europejskiej.

Ten ostatni artykuł w TUE stanowi, co następuje:

Art. 39

> Zgodnie z art. 16 Traktatu o funkcjonowaniu Unii Europejskiej i w drodze odstępstwa od jego ust. **2 Rada przyjmuje decyzję ustanawiającą zasady dotyczące ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez państwa członkowskie podczas prowadzenia przez nie działań wchodzących w zakres stosowania niniejszego** rozdziału [tj. w odniesieniu do WPZiB] oraz przepisy dotyczące swobodnego przepływu takich danych. Przestrzeganie tych zasad podlega kontroli niezależnych organów.

Nie jest to jednak miejsce, by dalej omawiać te kwestie[199]. Wystarczy zauważyć, że w dziedzinie WPZiB rozporządzenie dotyczące przetwarzania danych osobowych przez instytucje UE (itd.), rozporządzenie 2018/1725, omówione w następnej sekcji, ma zastosowanie, – ale jedynie w ograniczonym zakresie; a także, że aby uzyskać informacje na temat szczegółowych przepisów o ochronie danych odnoszących się do każdego działania w zakresie przetwarzania danych w kontekście WPZiB, w tym na temat tego, który organ ochrony danych jest właściwy w jakich kwestiach, oraz czy należy wyznaczyć inspektora ochrony danych, należy zapoznać się z konkretną decyzją Rady w tej sprawie.

https://edps.europa.eu/data-protection/our-work/subjects/common-foreign-and-security-policy_en.

[199] Dalsze dyskusje na ten temat:

- Pismo EIOD z dnia 23 lipca 2007 r. skierowane do prezydencji międzyrządowej w sprawie ochrony danych w ramach traktatu reformującego (tak nazywano Traktat Lizboński przy opracowywaniu jego projektu).
- EDPS, Joint Opinion n the notifications for Prior Checking received from the Data Protection Officer of the Council of the European Union regarding the processing of personal data for restrictive measures with regard to the freezing of assets [EIOD, Wspólna opinia dotycząca powiadomień o kontroli wstępnej otrzymanych przez inspektora ochrony danych w Radzie Unii Europejskiej w odniesieniu do przetwarzania danych osobowych w związku ze środkami restrykcyjnymi w odniesieniu do zamrożenia aktywów, Bruksela, 7 maja 2014 r. (2012 — 0724, 2012 – 0725, 2012 – 0726), s. 10, dostępna na stronie internetowej: Https://edps.europa.eu/sites/edp/files/publication/14-05-07_processing_personal_data_council_en.pdf.

1.4.5 Ochrona danych dla instytucji UE: nowe rozporządzenie

Jak zauważono w sekcji 1.3.6 powyżej, pierwszy unijny instrument dotyczący ochrony danych w związku z przetwarzaniem danych osobowych przez same instytucje UE, rozporządzenie 45/2001, został uchylony rozporządzeniem (UE) nr 2018/1725, które weszło w życie w **dniu 11 grudnia 2018 r.**[200] (jednak z **pewnymi** wyjątkami **i opóźnieniami w stosowaniu**, jak zauważono w poniższych punktach).

Dwa systemy

Odkładając kwestię wspomnianych wyjątków i opóźnień, rozporządzenie 2018/1725 w rzeczywistości tworzy **dwa odrębne systemy ochrony danych**: jeden dla wszystkich ***instytucji i organów UE niezaangażowanych we współpracę policyjną i sądową***, a drugi dla ***instytucji i organów UE zaangażowanych w taką współpracę*** (zob. art. 2 ust. 1 i 2)

- **System ochrony danych mający zastosowanie do instytucji i organów UE niezaangażowanych we współpracę policyjną i sądową:**

System ten, określony w rozdziałach I do VIII nowego rozporządzenia, jest w **dużej mierze taki sam jak system ustanowiony w ogólnym rozporządzeniu o ochronie danych (RODO)** w odniesieniu do przetwarzania, którego dotyczy ten ostatni instrument. W związku z tym rozporządzenie 2018/1725, podobnie jak RODO, obejmuje nową zasadę **« rozliczalności »** (art. 4 ust. 2; zob. również art. 26) i określa **obowiązki administratorów i podmiotów przetwarzających (Rozdział IV), faktycznie w taki sam sposób jak obowiązki administratorów i podmiotów przetwarzających podlegających RODO.**

W szczególności Rozdział IV zawiera przepisy dotyczące zasady „**ochrony danych w fazie projektowania i domyślnej ochrony danych**" (art. 27); rozwiązań, które należy wprowadzić w odniesieniu do „**współadministratorów**" (art. 28), **podmiotów przetwarzających** (art. 29) oraz **osób działających z upoważnienia administratora lub podmiotu przetwarzającego** (art. 30); obowiązku prowadzenia szczegółowego **rejestru czynności przetwarzania** („rozliczalność") (art. 31); **bezpieczeństwa przetwarzania danych** (art. 33), **zgłaszania naruszeń ochrony danych Europejskiemu Inspektorowi Ochrony Danych (EIOD), (który** jest organem nadzorczym w odniesieniu do instytucji i organów UE) (art. 34) oraz **zawiadamiania osób, których dane dotyczą, o naruszeniu ochrony danych** (art. 35) – wszystko na takich samych zasadach jak RODO.

Rozporządzenie 2018/1725 (podobnie jak poprzednie rozporządzenie 45/2001, omówione w sekcji 1.3.6 powyżej) nakłada na każdą instytucję lub organ Unii obowiązek wyznaczenia **inspektora ochrony danych (IOD)** (art. 43), który jest również zgodny z wymogiem RODO w odniesieniu do administratorów sektora publicznego. Przepisy dotyczące **statusu IOD** (art. 44) i **zadań IOD** (art. 45) są również zgodne z RODO, z tym, że wprowadzono ***pewne dodatkowe zapisy*** dotyczące dostępu każdego do inspektora ochrony danych i ochrony przed doznaniem uszczerbkiem z tego powodu (art. 44 ust. 7) oraz dotyczące kadencji IOD (art. 44 ust. 8); oraz w odniesieniu do zadań IOD - nieco silniejszy zapis (nieznajdujący się w RODO), że IOD „*zapewnia w sposób niezależny stosowanie przepisów niniejszego rozporządzenia wewnątrz instytucji lub organu*" (art. 45 ust. 1 lit. b))[201].

---

[200] Rozporządzenie (UE) 2018/1725 Parlamentu Europejskiego i Rady 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 1247/2002/WE, Dz.U. L 295 z 21 listopada 2018 r., s. 39 – 98, dostępne pod adresem: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1725.

[201] Jest to silniejsze, ponieważ chociaż RODO stanowi, że „*administrator oraz podmiot przetwarzający zapewniają, by inspektor ochrony danych nie otrzymywał instrukcji dotyczących wykonywania tych zadań*" oraz że „*nie jest on odwoływany ani karany przez administratora ani podmiot przetwarzający za wypełnianie swoich zadań*" (art. 38 ust. 3 RODO), co skutecznie gwarantuje, że IOD może działać „w sposób niezależny", w RODO stwierdza się, że IOD musi „*monitorować przestrzeganie*

Rozporządzenie 2018/1725 wymaga również **dokonania oceny skutków dla ochrony danych** w takich samych okolicznościach, jakie przewidziano w RODO, tj. w odniesieniu do przetwarzania, które „z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych" (art. 39); oraz stanowi, że muszą mieć miejsce „**uprzednie konsultacje**" z EIOD w podobnych okolicznościach, jak przewidziano w odniesieniu do uprzednich konsultacji z właściwym organem nadzorczym w RODO, tj., jeżeli ocena skutków dla ochrony danych wskazuje, że ryzyka tego nie da się w sposób wystarczający zminimalizować (art. 40) (w ostatnim zdaniu art. 40 dodaje się, że „*administrator zasięga porady inspektora ochrony danych w sprawie konieczności przeprowadzenia uprzednich konsultacji*", ale jest to oczywiście wskazane również w odniesieniu do przetwarzania w ramach RODO).

Co do treści, rozporządzenie 2018/1725 opiera się również na tych samych ***definicjach*** (art. 3) i ***podstawowych zasadach*** (art. 4), jak RODO, i zawiera faktycznie takie same przepisy dotyczące kwestii takich jak ***zgoda i inne podstawy prawne przetwarzania danych wrażliwych i niewrażliwych*** (por. art. 5 – 13), ale z pewnymi dalszymi szczegółowymi informacjami na temat „***zgodnego przetwarzania***" (art. 6) oraz ***przekazywania danych osobowych odbiorcom w państwach członkowskich*** (art. 9)[202]; oraz ***praw osób, których dane dotyczą*** (art. 14 – 24), w tym w odniesieniu do podejmowania ***w pełni zautomatyzowanych decyzji i profilowania*** (art. 24).

Przewidziano w nim również zasadniczo takie same dopuszczalne ***ograniczenia praw osób, których dane dotyczą, oraz obowiązek zawiadamiania osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych*** (art. 25 ust. 1), ale rozporządzenie rozszerza je również na ***obowiązek zapewnienia poufności łączności elektronicznej*** (jak wskazano poniżej) i ustanawia bardziej szczegółowe przepisy dotyczące tego, co wszelkie „***akty prawne lub przepisy wewnętrzne***" przewidujące takie ograniczenia powinny wyraźnie sprecyzować (zob. art. 25 ust. 2). Ponadto należy konsultować się z Europejskim Inspektorem Ochrony Danych w sprawie projektów takich przepisów (art. 41 ust. 2), co stanowi istotną gwarancję, że będą one rzeczywiście ograniczone do tego, co jest „*niezbędne i proporcjonalne [...] w społeczeństwie demokratycznym*".

Rozporządzenie 2018/1725 zawiera specjalną sekcję (Rozdział IV sekcja 3) dotyczącą **poufności łączności elektronicznej**. Stanowi ona, że:

> Instytucje i organy Unii **zapewniają poufność łączności elektronicznej**, w szczególności poprzez zabezpieczenie swoich sieci łączności elektronicznej (art. 36, dodano podkreślenie) —

oraz że:

> chronią informacje przesyłane do, przechowywane w, związane z, przetwarzane przez i pobierane z końcowych urządzeń użytkowników łączących łączącego się z dostępnymi publicznie stronami internetowymi i aplikacjami mobilnymi tych instytucji i organów zgodnie z art. 5 ust. 3 dyrektywy 2002/58/WE [tj. dyrektywy o prywatności i łączności elektronicznej, omówionej w sekcji 1.3.3 powyżej] (art. 37, dodano podkreślenie).

Ostatni artykuł w tej sekcji dotyczy **spisów użytkowników**, jak określono w art. 3 ust. 24, tj.:

> dostępny publicznie spis użytkowników lub wewnętrzny spis użytkowników dostępny w instytucji lub organie Unii, lub wspólny dla instytucji i organów Unii, zarówno w formie drukowanej, jak i elektronicznej.

[RODO i innych odpowiednich przepisów]" oraz „*informować i doradzać*" administratorowi i jego pracownikom (oraz wszelkim podmiotom przetwarzającym) w sprawie ich obowiązków (odpowiednio art. 39 ust. 1 lit. b) i lit. a) RODO), RODO nie wymaga od IOD „*zapewnienia*" przez niego wewnętrznego przestrzegania, zaś odpowiedzialność prawna spoczywa na administratorze.

[202] Zob. podsekcja 1.4.6 poniżej.

.

Art. 38 stanowi w tym względzie, że dane osobowe zawarte w takich spisach muszą być *„ograniczone do tego, co jest bezwzględnie konieczne do konkretnych celów spisu*" (art. 38 ust. 1) oraz że instytucje i organy:

> podejmują wszelkie niezbędne działania, aby zapobiec wykorzystywaniu danych osobowych zawartych w tych spisach do celów marketingu bezpośredniego, niezależnie od tego, czy dane te są ogólnodostępne czy też nie.

Przepisy zawarte w niniejszej sekcji odzwierciedlają niektóre przepisy dyrektywy o prywatności i łączności elektronicznej, omówione w sekcji 1.3.3 powyżej.

Przepisy dotyczące **przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych**, zawarte w rozdziale V rozporządzenia nr 2018/1725, ponownie opierają się na takim samym schemacie jak RODO: takie przekazywanie może mieć miejsce wyłącznie:

- na podstawie decyzji Komisji **stwierdzającej odpowiedni stopień ochrony** na mocy RODO; lub
- jeżeli zapewnione są „**odpowiednie zabezpieczenia**" za pomocą:
  - prawnie wiążącego i egzekwowalnego instrumentu między organami lub podmiotami publicznymi;
  - standardowych klauzul ochrony danych przyjętych przez Komisję;
  - standardowych klauzul ochrony danych przyjętych przez EIOD i zatwierdzonych przez Komisję;
  - jeżeli podmiot przetwarzający nie jest instytucją ani organem Unii, wiążących reguł korporacyjnych, kodeksów postępowania lub mechanizmów certyfikacji na podstawie RODO; lub

  pod warunkiem uzyskania zezwolenia EIOD:

  - klauzul umownych między odpowiednimi podmiotami; lub
- przepisów dotyczących ochrony danych zawartych w uzgodnieniach administracyjnych (umowach) między organami lub podmiotami publicznymi. (Art. 48)

Rozporządzenie 2018/1725 zawiera również zapis, identyczny jak ten z zawarty w RODO:

> Wyrok sądu lub trybunału oraz decyzja organu administracji państwa trzeciego wymagająca od administratora lub podmiotu przetwarzającego przekazania lub ujawnienia danych osobowych może zostać uznana lub być egzekwowalna wyłącznie, gdy opiera się na umowie międzynarodowej. (Art. 49)

Wreszcie w tym kontekście art. 50 rozporządzenia 2018/1725 przewiduje przekazywanie na podstawie **„wyjątków w szczególnych sytuacjach**", na tych samych zasadach, które zostały określone w RODO, tj., gdy osoba, której dane dotyczą, „**wyraźnie wyraziła zgodę**" na proponowane przekazanie (art. 50 ust. 1 lit. a)) lub gdy przekazanie jest **„niezbędne**" w ***kontekście umowy*** (art. 50 ust. 1 lit. b) i c)), ze względu na ***ważne względy interesu publicznego uznane w prawie Unii*** (art. 50 ust. 1 lit. d) w związku z art. 50 ust. 3), do ustalenia, dochodzenia lub ochrony ***roszczeń prawnych*** (art. 50 ust. 1 lit. e)), lub do ***ochrony żywotnych interesów osoby, której dane dotyczą, lub innych osób***, jeżeli osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody (art. 50 ust. 1 lit. f); lub gdy przekazanie następuje z **publicznie dostępnego rejestru** (pod warunkiem, że spełnione są warunki dostępu) (art. 50 ust. 1 lit. g)).

Rozporządzenie 2018/1725, podobnie jak RODO w odniesieniu do organów publicznych, stanowi, że trzy pierwsze z tych specjalnych wyjątków (wyraźna zgoda osoby, której dane dotyczą; warunki umowne) *„nie mają zastosowania do działalności prowadzonej przez instytucje i organy Unii w ramach wykonywania przysługujących im uprawnień publicznych"* (art. 50 ust. 2).

Rozdział VI rozporządzenia 2018/1725 dotyczy **ustanowienia zasad, statusu, zadań i obowiązków EIOD**. Zasadniczo EIOD spełnia w odniesieniu do przetwarzania danych osobowych przez instytucje i organy Unii tę samą funkcję, jaką pełnią organy nadzorcze (organy ochrony danych) ustanowione na podstawie RODO w odniesieniu do przetwarzania danych osobowych przez właściwe krajowe organy publiczne w państwie członkowskim (lub w regionie państwa członkowskiego), w odniesieniu, do którego są właściwe.

Rozdział VII dotyczy **współpracy między Europejskim Inspektorem Ochrony Danych a krajowymi organami nadzoru oraz skoordynowanego nadzoru ze strony Europejskiego Inspektora Ochrony Danych i krajowych organów nadzorczych**. Ponadto rozporządzenie, podobnie jak RODO, **zachęca do współpracy z państwami trzecimi i organizacjami międzynarodowymi** w zakresie ochrony danych osobowych (art. 51)[203].

Wreszcie rozdział VIII dotyczy **środków ochrony prawnej, odpowiedzialności i sankcji,** które są podobne do tych, które są wymagane na mocy RODO. Wystarczy zauważyć, że każda osoba, której dane dotyczą, której dane są lub były przetwarzane przez instytucję lub organ UE, ma prawo wnieść skargę do EIOD (art. 63) (tak jak każda osoba, której dane dotyczą, może wnieść skargę na podstawie RODO do odpowiedniego krajowego organu ochrony danych) i (również zgodnie z RODO) ma prawo do odszkodowania za wszelkie szkody majątkowe lub niemajątkowe spowodowane naruszeniem rozporządzenia (art. 65). Ponadto, podobnie jak w RODO, osoby, których dane dotyczą, mogą być w takich przypadkach reprezentowane przez organizacje niemające charakteru zarobkowego działające w dziedzinie ochrony danych osobowych (art. 67) - do czego rozporządzenie dodaje kolejny przepis dotyczący skarg pracowników UE (art. 68). Z kolei każdy urzędnik UE, który nie dopełnił obowiązków określonych w rozporządzeniu, podlega karze dyscyplinarnej (art. 69).

Trybunał Sprawiedliwości UE jest właściwy do rozstrzygania każdego sporu dotyczącego rozporządzenia, w tym w odniesieniu do odszkodowania (art. 64). A **EIOD może nakładać administracyjne kary pieniężne** na instytucje i organy Unii, które nie przestrzegają rozporządzenia (art. 66) (chociaż wysokość kar pieniężnych jest znacznie niższa od wysokości przewidzianej w RODO)[204].

[203] Podobnie jak w RODO, odpowiedni przepis (art. 50 RODO) jest nieco nietrafnie umieszczony w rozdziale dotyczącym przekazywania danych, a nie w rozdziale dotyczącym zadań i uprawnień organów nadzorczych.

[204] Maksymalne kary pieniężne, które EIOD może nałożyć na instytucje lub organy UE za nieprzestrzeganie rozporządzenia (WE) nr 2018/1725, wynoszą odpowiednio 25 000 EUR za jedno naruszenie i do wysokości łącznej kwoty 25 000 EUR rocznie za niektóre naruszenia oraz 50 000 EUR za jedno naruszenie i do wysokości łącznej kwoty 500 000 EUR rocznie w przypadku niektórych innych naruszeń (zob. art. 66 ust. 2 i 3). Jest to porównywalne do kar administracyjnych do wysokości 10 000 000 EUR lub – w przypadku przedsiębiorstwa (przedsiębiorstwa prywatnego) – w wysokości do 2 % całkowitego rocznego światowego obrotu (przy czym zastosowanie ma kwota wyższa) w przypadku niektórych naruszeń oraz do 20 000 000 EUR, a w przypadku przedsiębiorstwa – do 4 % całkowitego rocznego światowego obrotu (przy czym zastosowanie ma kwota wyższa) w przypadku niektórych innych naruszeń, które to kwoty mogą zostać nałożone na mocy RODO (art. 83 ust. 4 i 5) – chociaż RODO pozwala również państwom członkowskim na zmniejszenie tych kwot lub nawet całkowite zwolnienie organów i podmiotów publicznych mających siedzibę na ich terytorium z administracyjnych kar pieniężnych (art. 83 ust. 7) (ale takie organy zwolnione z kar pieniężnych lub podlegające ograniczonym karom pieniężnym powinny nadal podlegać uprawnieniom odpowiednich organów ochrony danych na mocy art. 58 ust. 2 RODO).

Biorąc pod uwagę, że główny system ochrony danych zgodnie z rozporządzeniem 2018/1725 jest ściśle dostosowany do RODO, często bardzo szczegółowe i praktyczne wytyczne oraz opinie wydane przez Europejskiego Inspektora Ochrony Danych instytucjom i organom UE podlegającym temu systemowi, również będą mieć bezpośrednie znaczenie dla administratorów przetwarzających dane osobowe na mocy RODO, szczególnie w sektorze publicznym, dlatego powinien być uważnie badany przez każdego inspektora ochrony danych pracującego dla takiego administratora (razem, oczywiście, z wytycznymi i opiniami Europejskiej Rady Ochrony Danych, której członkiem jest EIOD: opinie EIOD i EROD wzajemnie się uzupełniają).

- **System ochrony danych mający zastosowanie do instytucji i organów UE zaangażowanych we współpracę policyjną i sądową:**

Ogółem:

Jak wspomniano powyżej, rozporządzenie 2018/1725 **ustanawia oddzielny system ochrony danych dla organów i jednostek organizacyjnych Unii wykonujących czynności w dziedzinie współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej (**tj. czynności wchodzące *„w zakres części trzeciej tytuł V rozdział 4 lub 5 TFUE”*). Ten odrębny system określono **w rozdziale IX rozporządzenia**, obejmującym art. 70–95 (przy czym art. 2 ust. 2 wyjaśnia, że **definicje** określone w art. 3 mają również zastosowanie do tego rozdziału)[205].

Specjalny system reguluje przetwarzanie przez odpowiednie instytucje lub organy „**operacyjnych danych osobowych**”. Są one zdefiniowane w art. 3 ust. 2 jako:

> dane osobowe przetwarzane przez organy lub jednostki organizacyjne Unii przy wykonywaniu czynności, które wchodzą w zakres stosowania części trzeciej tytuł V rozdział 4 lub rozdział 5 TFUE, z myślą o osiągnięciu celów i realizacji zadań określonych w aktach prawnych ustanawiających te organy lub jednostki organizacyjne.

Co do zasady, przetwarzanie takich **operacyjnych danych osobowych** podlega specjalnemu systemowi określonym w rozdziale IX, podczas gdy przetwarzanie wszystkich „nieoperacyjnych” danych osobowych - takich jak dane dotyczące zasobów ludzkich odnoszące się do personelu odpowiednich organów i jednostek organizacyjnych - podlega głównemu systemowi określonemu we wcześniejszych rozdziałach rozporządzenia 2018/1725, jak opisano w poprzednim podtytule.

W poprzednim podtytule zauważyliśmy, że zasady dotyczące głównego systemu są ściśle dostosowane do RODO. Podobnie przepisy rozdziału IX rozporządzenia 2018/1725 są często zgodne z dyrektywą 2016/680 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości omówioną w sekcji 1.4.3 (lub zarówno z dyrektywą 2016/680, jak i z RODO oraz przepisami dotyczącymi głównego systemu na podstawie rozporządzenia 2018/1725) - ale rozdział IX nie jest tak ściśle związany z dyrektywą 2016/680, jak główny system z RODO. Te kwestie mogą być dość zawiłe[206].

Biorąc pod uwagę, że niniejszy Podręcznik jest skierowany do inspektorów ochrony danych w organach publicznych państw członkowskich, szczegóły dotyczące zgodności lub rozbieżności między przepisami w rozdziale IX i przepisami we wcześniejszej części rozporządzenia 2018/1725 – w tym w głównych

[205] W kwestii, czy, a jeśli tak, to w jakim zakresie, rozdziały VII i VIII mają zastosowanie do przetwarzania na podstawie rozdziału IX, patrz poniżej: *„Prawa, nadzór i egzekwowanie*”.

[206] Podając tylko jeden przykład: ściśle związanym z nową zasadą „rozliczalności”, która ma zastosowanie do wszystkich nowoczesnych instrumentów ochrony danych w UE, jest obowiązek administratorów do prowadzenia **rejestrów** i **ewidencji czynności**. RODO i zasady mające zastosowanie do głównego systemu na mocy rozporządzenia 2018/1725 wymagają jednak prowadzenia szczegółowego rejestrowania wszystkich operacji przetwarzania (art. 30 RODO; art. 31 rozporządzenia 2018/1725), ale nie wymagają przechowywania ewidencji czynności. Z kolei Dyrektywa 2016/680 wymaga prowadzenia zarówno szczegółowych rejestrów, jak i szczegółowych wykazów i ewidencji czynności (art. 24 i 25). Jednakże rozdział IX rozporządzenia 2018/1725 wymaga jedynie przechowywania ewidencji czynności związanych z przetwarzaniem operacyjnych danych osobowych (art. 88), bez wspominania o rejestrach.

unijnych instrumentach ochrony danych: RODO i dyrektywie 2016/680 – mogą zostać pominięte. Warto jednak w następnych podtytułach odnotować dwie szczególne kwestie.

Prawa, nadzór i egzekwowanie:

W rozdziale IX **nie ma odniesienia** do prawa osoby, której dane dotyczą, do **odszkodowania za szkody spowodowane niewłaściwym przetwarzaniem** (co w tym przypadku oznaczałoby przetwarzanie niezgodne z przepisami tego rozdziału), do bycia **reprezentowanym** przez organ non-profit lub uprawnienia EIOD do nakładania **administracyjnych kar pieniężnych**.

Przepisy rozdziału IX wielokrotnie wspominają o obowiązku administratora z zastrzeżeniem rozdziału IX **do informowania osób**, których dane dotyczą, o ich **prawie do wniesienia skargi do EIOD** (zob. Art. 79 ust. 1 lit. d), Art. 80 lit. f) oraz Art. 81 ust. 2), a także o możliwości wystąpienia do sądowego środka odwoławczego (Art. 81 ust. 2). Administratorzy podlegający rozdziałowi IX mogą również ustalić, że **osoby, których dane dotyczą** mogą *„wykonywać swoje prawa także za pośrednictwem Europejskiego Inspektora Ochrony Danych”* (Art. 84 ust. 1, tj. tylko pośrednio; i w tym przypadku administrator również musi poinformować osobę, której dane dotyczą:

> **o możliwości wykonywania przysługujących jej praw za pośrednictwem Europejskiego Inspektora Ochrony Danych** na mocy ust. 1. (Art. 84(2))

Administrator musi również **udostępnić** na żądanie **EIOD ewidencję** operacji przetwarzania (Art. 88 ust. 3) i **zgłosić EIOD naruszenia ochrony danych osobowych** (art. 92 ust. 1 i 4).

Jednakże, z Art. 2 ust. 2 rozporządzenia 2018/1725 wyraźnie wynika, że zarówno rozdział VIII, który dotyczy rozpatrywania skarg przez EIOD i jurysdykcji Trybunału Sprawiedliwości UE oraz działań egzekucyjnych EIOD, również w przypadku naruszenia danych osobowych oraz rozdział VI, który określa zadania i uprawnienia EIOD w tym zakresie, nie mają zastosowania do przetwarzania danych operacyjnych, które podlegają wyłącznie rozdziałowi IX.

Wydaje się, że w praktyce EIOD przejmuje uprawnienia nadzorcze i doradcze, również w odniesieniu do przetwarzania operacyjnych danych osobowych przez instytucje i organy UE na mocy rozdziału IX rozporządzenia 2018/1725, i będzie skłonny przyjąć skargi osób, których dane dotyczą, w związku z takim przetwarzaniem. Czy zezwoli na reprezentowanie osób, których dane dotyczą, w takich przypadkach przez organizacje pozarządowe, czy będzie skłonny nakazać odszkodowanie, a nawet nałożyć kary administracyjne na odpowiednie instytucje i organy - i czy Trybunał Sprawiedliwości poprze takie wykonywanie uprawnień EIOD w związku z takim przetwarzaniem - dopiero się okaże.

Wyjątki i opóźnione wdrożenie rozporządzenia 2018/1725

Zasadniczo rozporządzenie 2018/1725 ma zastosowanie do całego przetwarzania danych osobowych przez wszystkie instytucje i organy Unii (art. 2 ust. 1) - choć, jak widzieliśmy, poprzez utworzenie dwóch odrębnych systemów prawnych. Rozporządzenie zawiera jednak pewne wyjątki od jego stosowania i przewiduje opóźnione wdrożenie jego przepisów w niektórych innych kontekstach, co omówiono poniżej.

– **Wyjątki**

Artykuł 2 ust. 4 stanowi, że:

> **Niniejsze rozporządzenie nie ma zastosowania do przetwarzania danych osobowych przez misje, o których mowa w art. 42 ust. 1, art. 43 i 44 TUE.** (podkreślenia dodane)

Misje i zadania objęte zwolnieniem to:

- misje poza Unią mające na celu utrzymanie pokoju, zapobieganie konfliktom i wzmacnianie międzynarodowego bezpieczeństwa, zgodnie z zasadami Karty Narodów Zjednoczonych (Art. 42 ust. 1) oraz
- wspólne działania rozbrojeniowe, misje humanitarne i ratunkowe, misje wojskowego doradztwa i wsparcia, misje zapobiegania konfliktom i utrzymywania pokoju, misje zbrojne służące zarządzaniu kryzysowemu, w tym misje przywracania pokoju i operacje stabilizacji sytuacji po zakończeniu konfliktów. Wszystkie te zadania (art. 43, w którym rozwinięto art. 44).

W drugim zdaniu art. 43 dodaje się, że wszystkie operacje i zadania wymienione w tym artykule *„mogą przyczyniać się do walki z terroryzmem, w tym poprzez wspieranie państw trzecich w zwalczaniu terroryzmu na ich terytoriach”.*

– **Opóźnione wdrożenie**

Oprócz wspomnianego wyżej wyłączenia stosowania rozporządzenia w odniesieniu do określonych operacji, dla których można określić szczegółowe zasady, rozporządzenie określa również procesy dostosowania operacji przetwarzania danych niektórych innych instytucji i organów UE zgodnie z rozporządzeniem 2018/1725, z terminami odpowiednich przeglądów (ale nie faktycznego dostosowania tych operacji do rozporządzenia). W szczególności Art. 2 ust. 3 stanowi, że:

> Niniejsze rozporządzenie nie ma zastosowania do przetwarzania operacyjnych danych osobowych przez **Europol** i **Prokuraturę Europejską** dopóki [przepisy przedlizbońskie obejmujące ich działalność][207] nie zostaną dostosowane zgodnie z art. 98 niniejszego rozporządzenia. (podkreślenia dodane)

Ponadto Art. 98 stanowi, że:

> 1. **Do dnia 30 kwietnia 2022 r**. Komisja dokonuje **przeglądu** przyjętych na podstawie Traktatów aktów prawnych, które regulują przetwarzanie operacyjnych danych osobowych przez organy lub jednostki organizacyjne Unii wykonujące czynności które wchodzą w zakres części trzeciej tytuł V rozdział 4 lub rozdział 5 TFUE, w celu:
>
> a) **dokonania oceny** ich zgodności z dyrektywą (UE) 2016/680 i rozdziałem IX niniejszego rozporządzenia;
>
> b) **stwierdzenia** wszelkich rozbieżności, które mogą utrudniać wymianę operacyjnych danych osobowych między organami i jednostkami organizacyjnymi Unii podczas prowadzenia działań w tych dziedzinach i właściwymi organami; oraz
>
> c) **stwierdzenia** wszelkich rozbieżności, które mogą spowodować fragmentaryzację przepisów dotyczących ochrony danych w Unii.
>
> 2. Na podstawie tego przeglądu, aby zapewnić jednolitą i spójną ochronę osób fizycznych w odniesieniu do przetwarzania danych, **Komisja może przedstawić odnośne wnioski ustawodawcze, w tym w szczególności w razie potrzeby modyfikacje rozdziału IX niniejszego rozporządzenia, z myślą o zastosowaniu tego rozdziału do Europolu i Prokuratury Europejskiej.** (podkreślenia dodane)

Innymi słowy, przepisy dotyczące pracy Europolu i Prokuratury Europejskiej oraz wszelkich innych instytucji i organów objętych Art. 98 muszą zostać poddane ***przeglądowi do dnia 30 kwietnia 2022 r.,*** a następnie Komisja może ***zaproponować*** nowe zasady w celu dostosowania przetwarzania danych osobowych przez te organy do Dyrektywy 2016/680 (omówionej w sekcji 1.4.3) oraz do specjalnych przepisów ustanowionych w rozdziale IX rozporządzenia (omówionym powyżej). **Nie wyznaczono** jednak **daty** faktycznego przyjęcia nowych przepisów, które będą wymagały działań legislacyjnych Rady Ministrów i ewentualnie nowego Parlamentu Europejskiego oraz uzyskania opinii Europejskiego Inspektora Ochrony Danych i Europejskiej Rady Ochrony Danych - co zajmie trochę czasu. Dopóki te rozporządzenia są zmienione dla tych celów - tj. przynajmniej przez kilka następnych lat - przetwarzanie danych osobowych przez Europol i EPPO (i wszelkie inne instytucje lub organy objęte Art. 98 rozporządzenia 2018/1725) będą podlegać własnym, bieżącym zasadom ochrony danych (sprzed 2018 r.).

1.4.6 Przekazywanie danych osobowych między różnymi systemami ochrony danych w UE

[207] Odpowiednio: 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.U. L 135 z 24 maja 2016 r. str. 53 oraz Rozporządzenie Rady (UE) 2017/1939 z dnia 12 października 2017 r. wdrażające wzmocnioną współpracę w zakresie ustanowienia Prokuratury Europejskiej, Dz.U. L 283 z 31 października 2017 r. str. 1.

i. Różne systemy ochrony danych

Z poprzednich sekcji wynika, że w rzeczywistości istnieje wiele **różnych, ogólnych lub bardziej szczegółowych systemów ochrony danych w ramach głównych instrumentów i ram ochrony danych w UE**, a niektóre poza nimi (a nawet **całkowicie poza prawem UE**), w tym określone poniżej. Który system ma zastosowanie do określonej działalności lub operacji przetwarzania będzie zależeć od oceny każdej takiej działalności lub operacji i jej konkretnego celu, w szczególności od tego, czy sprawa wchodzi w zakres kompetencji UE, czy nie, czy ma to miejsce w sektorze prywatnym czy publicznym, czy obejmuje instytucje UE lub krajowe działające w sprawach gospodarczych lub karnych, itp.

Ogólne rozporządzenie o ochronie danych:

- System RODO stosowany do przetwarzania przez podmioty prywatne.
- System RODO stosowany w odniesieniu do przetwarzania przez podmioty publiczne nieuczestniczące w sprawach karnych, bezpieczeństwa publicznego lub bezpieczeństwa narodowego lub gdy nie są zaangażowane w takie sprawy (przy czym „bezpieczeństwo publiczne" należy rozumieć jako bardzo ograniczoną kategorię).

Dyrektywa o prywatności i łączności elektronicznej / proponowane rozporządzenie o prywatności i łączności elektronicznej:

- Szczegółowe zasady miały zastosowanie do dostawców usług łączności elektronicznej (a w przyszłości do innych dostawców, takich jak gracze „Over-The-Top").
- Szczegółowe zasady mające zastosowanie do wszystkich hostów internetowych (w tym organów publicznych posiadających własne strony internetowe) w odniesieniu do poufności komunikacji, korzystania z plików „cookie", itp.

Dyrektywa w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy:

- W odniesieniu do podmiotów publicznych („właściwych organów"), gdy przetwarzają dane osobowe w celu *„zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w tym do celów ochrony przed zagrożeniami dla bezpieczeństwa publicznego*", jako ich główne zadanie lub okazjonalnie, oprócz innych zadań publicznych.

Obszary wyłączone z zastosowania LEDPD (na chwilę obecną):

- Przepisy zawarte w około 123 unijnych instrumentach prawnych dotyczących tzw. spraw wymiaru sprawiedliwości i spraw wewnętrznych (WSiSW), które weszły w życie przed 6 maja 2016 r. (które nadal obowiązują, nawet jeśli nie są jeszcze zgodne z LEDPD).
- Przepisy zawarte w *„umowach międzynarodowych, które przewidują przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych i które zostały zawarte przez państwa członkowskie przed dniem 6 maja 2016 r. są zgodne z prawem Unii mającym zastosowanie przed tą datą "* (które również mają nadal zastosowanie, nawet jeżeli nie są jeszcze zgodne z LEDPD).
- Przepisy dotyczące korzystania z *„zautomatyzowanych systemów przetwarzania utworzonych przed dniem 6 maja 2016 r."* w państwach członkowskich, jeżeli nie zostały jeszcze dostosowane do tej dyrektywy, ponieważ pociągałyby za sobą *„niewspółmiernie duży wysiłek*".

Przetwarzanie danych osobowych w obszarze WPZiB:

- Przetwarzanie przez Wysokiego Przedstawiciela Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa, Europejską Służbę Działań Zewnętrznych (ESDZ) i 141 delegatur UE na całym świecie oraz Służbę ds. Instrumentów Polityki Zagranicznej (FPI) i przetwarzanie

przez państwa członkowskie w związku z tymi kwestiami (w tym w związku z przyjęciem decyzji Rady w dziedzinie WPZiB), *które nie są jeszcze objęte żadnym konkretnym unijnym instrumentem ochrony danych*. [zobacz jednak tiret trzecie w ramach kolejnego punktu]

Przetwarzanie danych osobowych przez instytucje lub organy UE na mocy rozporządzenia 2018/1725:

- System ochrony danych mający zastosowanie do instytucji i organów UE, które nie uczestniczą we współpracy policyjnej i sądowej.
- System ochrony danych mający zastosowanie do instytucji i organów UE zaangażowanych we współpracę policyjną i sądową.
- Przetwarzanie danych przez Sekretariat Rady we wdrażaniu decyzji Rady w sprawie WPZiB – ograniczony obszar działalności dotyczący WPZiB, podlegający przepisom o ochronie danych, tj. rozporządzeniu 2018/1725.

Obszary wyłączone z zakresu stosowania rozporządzenia 2018/1725 (na chwilę obecną):

- Przetwarzanie danych osobowych przez misje UE mające na celu **utrzymanie pokoju**, zapobieganie konfliktom i wzmacnianie bezpieczeństwa międzynarodowego, lub odpowiedzialne za wspólne **działania rozbrojeniowe**, **misje humanitarne i ratunkowe,** misje wojskowego doradztwa i wsparcia, **misje zapobiegania konfliktom i utrzymywania pokoju, zadania sił zbrojnych w sytuacjach kryzysowych,** w tym przywracanie pokoju i **stabilizacja sytuacji pokonfliktowej** (w tym gdy zadania takie dotyczą walki z terroryzmem, w tym poprzez wspieranie państw trzecich w zwalczaniu terroryzmu na ich terytorium).
- Przetwarzanie danych osobowych przez Europol i Prokuraturę Europejską oraz inne *„organy lub jednostki organizacyjne Unii wykonujące czynności które wchodzą w zakres części trzeciej tytuł V rozdział 4 lub rozdział 5 TFUE [tj. odnoszące się do współpracy policyjnej i sądowej], które* będzie nadal prowadzone na podstawie unijnych instrumentów prawnych odnoszących się do Europolu lub EPPO bądź do współpracy policyjnej lub sądowej, przyjętych przed wejściem w życie rozporządzenia 2018/1725.

Bezpieczeństwo narodowe:

- Przetwarzanie danych osobowych przez państwa członkowskie w odniesieniu do bezpieczeństwa narodowego — **które nie wchodzi w zakres prawa UE** —Karty praw podstawowych (chociaż takie przetwarzanie oczywiście podlega Europejskiej konwencji praw człowieka i jurysdykcji Europejskiego Trybunału Praw Człowieka)[208].

Nie zawsze łatwo jest wyznaczyć jasne granice między tymi wieloma różnymi systemami, np. między działaniami policji przeciwko przestępczości, działaniami policji w celu zabezpieczenia porządku, działaniami policji i innych organów w celu zapewnienia „bezpieczeństwa wewnętrznego", „bezpieczeństwa publicznego" i „bezpieczeństwa narodowego", a także między tymi działaniami a działaniami UE w odniesieniu do „terroryzmu"[209], wyżej wymienionych zadań misji UE oraz „bezpieczeństwa międzynarodowego".

[208] Europejski Trybunał Praw Człowieka wydał w tej sprawie kilka ważnych wyroków. Zob. Europejski Trybunał Praw Człowieka, *Bezpieczeństwo narodowe i europejskie - orzecznictwo*, Rada Europy, 2013, dostępne pod adresem: https://www.echr.coe.int/Documents/Research_report_national_security_ENG.pdf. Instytucje UE nie mogą jednak stosować tych przepisów w odniesieniu do takich działań.

[209] Por. John Vervaele, *Terrorism and information sharing between intelligence and law enforcement in the US and the Netherlands : emergency criminal law ? w*:Utrecht Law Review, tom 1, wydanie 1 (wrzesień 2005 r.) dostępne na stronie internetowej: http://www.utrechtlawreview.org/.

Nie jest to miejsce, w którym dogłębnie zostaną przeanalizowane te różnice. Wystarczy zauważyć, że w przypadku gdy różne systemy mają zastosowanie do różnych rodzajów działalności (działania należące do więcej niż jednej z powyższych kategorii), być może nawet przez te same podmioty, ważne będzie, aby właściwe podmioty, jako administratorzy danych (i często również jako podmioty przetwarzające, np. wspierając inne takie podmioty) **doprecyzowały**, **jaki system prawny ma zastosowanie jakich do operacji przetwarzania danych osobowych oraz do jakich danych osobowych, analizując każdą konkretną operację przetwarzania danych.** Legalność przetwarzania oraz zakres i wyjątki od tak ważnych kwestii jak prawa osób, których dane dotyczą, zawsze zależą od takich wyjaśnień.

Organy publiczne zaangażowane w różne działania, które podlegają różnym systemom ochrony danych, powinny zawsze starannie rozróżniać ich różne działania, różne operacje przetwarzania oraz różne dane osobowe wykorzystywane do poszczególnych operacji w dokumentacji dotyczącej przetwarzania danych osobowych oraz w swoich ocenach takiego przetwarzania[210]. Kluczową rolę w tym zakresie będą musieli odgrywać inspektorzy ochrony danych w takich organach publicznych[211].

[210] Zob. art. 74 rozporządzenia 2018/1725 w sprawie *„rozróżnienia poszczególnych rodzajów operacyjnych danych osobowych i weryfikacji jakości operacyjnych danych* osobowych", które stanowi dobry przykład ogólnej dobrej praktyki w przypadkach, gdy administrator danych prowadzi działalność podlegającą innym systemom ochrony danych.
[211] Zob. Część trzecia niniejszego Podręcznika.

i. Przekazywanie danych osobowych

Pojawiają się szczególne problemy w przypadku, gdy proponuje się lub wymaga, aby dane osobowe uzyskane w jednym celu na podstawie przepisów jednego z wyżej wymienionych systemów prawnych były wykorzystywane przez tego samego administratora do innego celu, w celu przetwarzania w ramach innego systemu prawnego; lub są przekazywane lub w inny sposób udostępniane innemu organowi (innemu administratorowi) w takim innym celu, w celu przetwarzania w ramach innego systemu prawnego[212].

Na przykład wydział oświatowy w organie samorządu lokalnego może gromadzić dane osobowe uczniów w celach edukacyjnych na podstawie RODO, ale może zostać poproszony przez lokalną policję o dostęp do (niektórych) tych danych, aby pomóc w rozwiązaniu problemu przestępczości lokalnej (np. w celu sprawdzenia, które dzieci w danym dniu były nieobecne w szkole). Proponowane przetwarzanie danych w drugim celu byłoby zgodne z LEDPD (lub bardziej precyzyjne, z przepisami prawa krajowego transponującymi LEDPD, a także z odpowiednimi przepisami w zakresie postępowania policji lub postępowania karnego). Czasami właściwe ustawy lub przepisy prawne precyzują, kiedy takie udostępnienie może mieć miejsce (np. tylko w odniesieniu do niektórych przestępstw lub tylko wtedy, gdy istnieją uzasadnione podejrzenia wobec zidentyfikowanych dzieci lub tylko w przypadku, gdy sąd wydał nakaz). Kwestia ta jest jednak często rozstrzygana przez właściwy organ lokalny w świetle przepisów różnych mających zastosowanie instrumentów. **Inspektor ochrony danych w organie lokalnym będzie odgrywał ważną rolę w doradzaniu w tej sprawie (i w razie wątpliwości powinien skonsultować się z organem ochrony danych).**

Rozporządzenie 2018/1725 zawiera pewne wskazówki dotyczące przekazywania danych osobowych przez instytucję lub organ UE *„odbiorcom mających siedzibę w Unii, innym niż instytucje i organy Unii*" – zazwyczaj organom publicznych państw członkowskich. Instytucje i organy UE mają prawo przekazywać dane podmiotowi w państwie członkowskim, które wnioskuje o przekazanie danych, pod warunkiem, że:

> (a) odbiorca [tj. podmiot w państwie członkowskim wnioskujący o dane] stwierdzi, że dane są niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej odbiorcy [tj. w tym podmiocie]; lub
>
> (b) odbiorca stwierdzi, że przekazanie danych jest niezbędne w określonym celu w interesie publicznym, zaś administrator [tj. instytucja lub organ UE, do którego zwrócono się o przekazanie danych], w przypadku gdy istnieje jakikolwiek powód, by uznać, że uzasadniony interes osoby, której dane dotyczą, może zostać zagrożony, ustali po wyraźnym dokonaniu oceny różnych przeciwstawnych interesów, że przekazanie danych osobowych w tym określonym celu jest proporcjonalne
>
> (art. 9 ust. 1)

Instytucjom lub organom UE zezwala się na przekazywanie (przesyłanie) takich danych podmiotom w państwach członkowskich bez wezwania, tj. z własnej inicjatywy, jeżeli mogą:

[212] Należy zauważyć, że omawiane operacje przekazywania danych różnią się od operacji przekazywania danych osobowych dokonywanych przez jeden podmiot do innego podmiotu w tym samym państwie lub w innym państwie członkowskim w tym samym celu, na podstawie tego samego [unijnego] systemu ochrony danych, np. przez jeden organ ds. egzekwowania prawa w jednym państwie członkowskim do innego organu ds. egzekwowania prawa w tym państwie członkowskim lub do organu ds. egzekwowania prawa w innym państwie członkowskim; oraz od przekazywania danych osobowych do państw trzecich (które podlegają specjalnym przepisom dotyczącym takich operacji przekazywania, ale należy zauważyć, że również one różnią się w poszczególnych systemach).

wykazać, że przekazanie danych osobowych jest niezbędne i proporcjonalne do celów przekazania, stosując kryterie określone w ust. 1 lit. a) lub b).

(art. 9 ust. 2)

W tym względzie należy jednak wziąć pod uwagę kilka elementów. Przede wszystkim powyższe odnosi się do instytucji i organów UE, które nie zajmują się przetwarzaniem w ramach współpracy policyjnej i sądowej, tj. mają zastosowanie wyłącznie do przetwarzania – i przekazywania – w ramach „systemu głównego" ustanowionego rozporządzeniem 2018/1725 dla instytucji i organów UE; oraz jak zauważono w sekcji 1.4.5 powyżej, ten „główny" system ochrony danych w tym rozporządzeniu jest ściśle dostosowany do ogólnego rozporządzenia o ochronie danych. Brak jest analogicznego przepisu dotyczącego przekazywania danych osobowych organom w państwach członkowskich w rozdziale IX rozporządzenia 2018/1725, który obejmuje przetwarzanie danych „operacyjnych" przez instytucje i organy UE zaangażowane w działania policji i wymiaru sprawiedliwości.

Po drugie, cytowane powyżej przepisy art. 9 są „bez uszczerbku" dla podstawowych zasad ochrony danych, w tym zasady ograniczenia celu i zasady „zgodnego" przetwarzania (zob. art. 6 rozporządzenia, które dodaje istotne warunki do tego), stosowności danych, itp. oraz przepisów dotyczących zgodnego z prawem przetwarzania danych (zob. wprowadzenie do art. 9 ust. 1). Pozostają one również bez uszczerbku dla przepisów szczególnych dotyczących przetwarzania danych osobowych szczególnie chronionych (*tamże*).

Art. 9 rozporządzenia 2018/1725 pokazuje jednak, że **w przypadku, gdy dane osobowe przetwarzane w ramach jednego z wyżej wymienionych systemów mają być przekazywane innemu podmiotowi (lub nawet do wykorzystania przez ten sam podmiot) w celu ich przetwarzania w ramach innego systemu, należy odpowiedzieć na ważne pytania dotyczące określenia celu, stosowności i adekwatności danych oraz na temat zgodności z prawem, niezbędności i proporcjonalności zmiany celu**.

W tym względzie należy przede wszystkim przypomnieć, że „przekazywanie" danych, jak każda inna forma „ujawniania" danych osobowych (w tym „udostępnianie [danych osobowych]", np. online), stanowi formę przetwarzania (zob. art. 4 ust. 2 RODO, powtarzalnie *dosłownie* we wszystkich innych unijnych instrumentach ochrony danych). Po drugie, wszelkie „przekazywanie" danych osobowych między różnymi podmiotami ma zawsze dwa aspekty:

- w przypadku podmiotu przekazującego jest to forma **ujawniania** danych (zob. powyżej); ale
- w przypadku podmiotu otrzymującego jest to **gromadzenie** danych osobowych – co stanowi odrębną czynność objętą ogólną koncepcją „przetwarzania", różniącego się od „ujawniania", „przekazywania" lub „udostępniania" danych osobowych.

Jeżeli w odniesieniu do ich odpowiednich działań związanych z przekazywaniem danych oba podmioty podlegają innym systemom ochrony danych, każdy powinien ocenić zgodność swoich odpowiednich działań z mającymi do nich zastosowanie zasadami ochrony danych.

W związku z tym w powyższym przykładzie lokalny wydział oświatowy będzie podlegał RODO oraz wszelkim „dalszym specyfikacjom" dotyczącym tego, w jaki sposób należy stosować przepisy RODO określone w odpowiednich krajowych przepisach o ochronie danych (lub być może w odpowiedniej części dotyczącej ochrony danych ustawy w sprawie zadań i uprawnień lokalnych wydziałów oświatowych, która powinna być nadal zgodna z ogólnym rozporządzeniem o ochronie danych).

Z drugiej strony lokalna jednostka policji będzie podlegać krajowym przepisom prawnym przyjętym w celu wdrożenia LEDPD (jak również wszelkim stosownym przepisom w krajowych przepisach dotyczących policji lub postępowania karnego, które powinny być zgodne z LEDPD).

W takim przypadku lokalny wydział oświatowy musi sprawdzić (z pomocą IOD i w razie potrzeby porady odpowiedniego organu ochrony danych), czy przepisy dotyczące ochrony danych, którym podlega, pozwalają na ujawnienie danych osobowych agencji policji (lub nie, lub na jakich warunkach).

Z drugiej strony lokalna agencja policji, przed złożeniem wniosku o przekazanie danych do wydziału oświatowego, powinna sprawdzić (z pomocą IOD i w razie potrzeby z pomocą odpowiedniego organu ochrony danych), czy przepisy dotyczące ochrony danych, którym podlega, pozwalają jej na wnioskowanie o lub żądanie danych osobowych od lokalnego wydziału oświatowego (lub nie, lub na jakich warunkach).

Często przydatne będzie omówienie tych kwestii przez dwóch inspektorów ochrony danych (i skonsultowanie się, w stosownych przypadkach, z organem ochrony danych).

Często odpowiednie przepisy będą wzajemnie zgodne i faktycznie wzajemnie się ze sobą wzajemnie się do siebie odwoływać. Na przykład ustawa o policji może przewidywać, w jakich przypadkach i na jakich warunkach lokalna agencja policji może zwrócić się do „innych organów publicznych" o informacje (zazwyczaj o dzieciach); a przepisy mające zastosowanie do wydziału edukacyjnego mogą stanowić, że departament może – lub musi – dostarczyć informacje wymagane przez „inny organ publiczny" (lub w szczególności przez policję), pod warunkiem że wniosek jest zgodny z prawem. Będzie to nadal wymagało od agencji policji przestrzegania przepisów i spełnienia odpowiednich warunków, a od służby edukacyjnej przynajmniej żądania zapewnienia (i dowodu), że wniosek złożony przez policję jest zgodny z prawem i spełnia odpowiednie warunki. Nie ma jednak żadnego problemu w odniesieniu do przekazywania danych.

Jeżeli zarówno jednostka przekazująca, jak i agencja wnioskująca podlegają najnowszym unijnym przepisom o ochronie danych, opisanym powyżej – w szczególności RODO, LEDPD i rozporządzeniu 2018/1725 – zazwyczaj nie powinno być żadnych problemów w tym zakresie (chociaż indywidualne przypadki mogą nadal wymagać poważnej analizy i uwagi).

Kwestie te są mniej jednoznaczne, jeżeli jeden podmiot – w szczególności podmiot występujący z wnioskiem – nie podlega najnowszym zasadom, lecz wciąż tylko mniej wymagającym przepisom, mimo że nadal będzie się opierał na ogólnych zasadach ochrony danych, leżących u podstaw wszystkich unijnych przepisów o ochronie danych.

Jednakże kwestie te mogą być w praktyce bardzo skomplikowane, gdy podmiot występujący z wnioskiem nie podlega w ogóle właściwym przepisom o ochronie danych, jak to miało miejsce w przypadku spraw z zakresu WPZiB, kwestii związanych z operacjami utrzymywania pokoju w UE lub innych misji wojskowych lub z bezpieczeństwem narodowym. W tym kontekście „odpowiednie" przepisy są zasadami wyraźnie opartymi na ogólnych zasadach ochrony danych i ich uznawania; które odbiegają od zwykłych przepisów opartych na tych zasadach jedynie w ściśle określonym zakresie w odpowiednim (publicznie dostępnym, jasnym i precyzyjnym) instrumencie prawnym, który jest „możliwy do przewidzenia" w jego stosowaniu, i tylko w zakresie, w jakim jest to „absolutnie niezbędne" do danego celu, przy czym każde takie odstępstwo jest w sposób oczywisty „proporcjonalne" do szczególnego

kontekstu[213]; oraz które przewidują kontrolę przestrzegania przepisów szczególnych przez niezależny organ[214].

Nie jest to miejsce na szczegółowe omówienie tej kwestii. Może jednak zostać podjęte w poważnych kwestiach.

W związku z tym każde przekazanie danych osobowych przez krajowy organ publiczny (lub instytucję lub organ UE), które podlega najnowszym unijnym przepisom o ochronie danych (tj. RODO, LEDPD lub rozporządzeniu 2018/1725) każdemu obywatelowi lub podmiotowi UE, który nie podlega żadnym odpowiednim przepisom o ochronie danych, jest potencjalnie bardziej szkodliwe dla ochrony danych UE, jako każde przekazanie takich danych do państwa bez odpowiednich przepisów o ochronie danych – co jest co do zasady zakazane, chyba że zostaną przyjęte „odpowiednie zabezpieczenia" (por. rozdział V RODO).

Podmioty podlegające któremukolwiek z wyżej wymienionych unijnych instrumentów ochrony danych powinny zatem zachować ostrożność przed przekazaniem danych osobowych podmiotowi składającemu wniosek, który nie podlega żadnym odpowiednim przepisom o ochronie danych. Powinni oni dokładnie sprawdzać – jak zawsze – z pomocą DPO i w razie potrzeby konsultując się z właściwym organem ochrony danych – czy instrument, który ma do nich zastosowanie, pozwala na takie przeniesienie (w ogóle), czy też zakazuje lub nakłada na niego warunki; i powinny odmówić przekazania danych, chyba że jest to dozwolone w ramach instrumentu, który ma do nich zastosowanie, w wystarczająco jasny sposób.

Nie wystarczy, aby podmiot występujący z wnioskiem, który nie podlega odpowiednim przepisom o ochronie danych, zwrócił uwagę na to, że podmiot wnioskujący ma możliwość uzyskania (zbierania) danych, o które wnioskuje się zgodnie z przepisami mającymi zastosowanie do tej jednostki wnioskującej: może to uzasadniać gromadzenie danych w rozumieniu tych przepisów, ale nie legitymizuje ujawniania danych („przekazywania") przez podmiot, do którego kierowany jest wniosek, na mocy przepisów o ochronie danych, które mają zastosowanie do podmiotu otrzymującego wniosek (zwłaszcza, jeżeli przepisy te są określone w wyżej wymienionych unijnych aktach prawnych dotyczących ochrony danych lub zostały przyjęte na ich podstawie).

Czasami państwa nadal stosują przepisy, które zapewniają niektórym agencjom – w szczególności ich **agencjom wywiadowczym** — prawo do żądania informacji lub dostęp do informacji, w tym danych osobowych, w najszerszym ujęciu; a czasami ustawy są sformułowane w taki sposób, że mają pierwszeństwo przed wszelkimi ograniczeniami w zakresie ujawniania informacji osobowych przez inne podmioty, które podlegają przepisom o ochronie danych i które (ogólne przepisy prawne) muszą spełniać takie wymogi niezależnie od tego, jakie odpowiednie przepisy o ochronie danych mają do nich zastosowanie. Obejmuje to prawo w państwach członkowskich[215].

W odniesieniu do krajowych agencji bezpieczeństwa właściwe państwo członkowskie może twierdzić, że przepisy, na mocy których agencje te mogą żądać informacji (lub dostępu do baz danych) nie wchodzą w zakres prawa UE – oraz że w związku z tym przekazywanie danych tym agencjom na podstawie jego przepisów nie wchodzi w zakres prawa UE i wykracza poza uprawnienia organów ochrony danych lub Trybunału Sprawiedliwości UE.

Byłoby to jednak wynikiem błędnej interpretacji sytuacji prawnej. Nawet jeżeli gromadzenie informacji osobowych przez te agencje znajduje się poza zakresem prawa UE (lub

[213] Są to wymogi w zakresie praworządności wypracowane przez Europejski Trybunał Praw Człowieka i stosowane w równym stopniu przez Trybunał Sprawiedliwości UE i odzwierciedlone w Karcie praw podstawowych Unii Europejskiej, która musi być przestrzegana w każdym działaniu, które może mieć wpływ na podstawowe prawa i wolności jednostki.
[214] Jak wyraźnie przewidziano w art. 8 (3) Karty praw podstawowych.
[215] Zob. Douwe Korff *et al.*, Boundaries of Law (przypis 172, powyżej), część 4.

uprawnieniami organów ochrony danych lub TSUE), przekazywanie danych tym agencjom przez wszelkie podmioty, które podlegają unijnym instrumentom ochrony danych, wchodzi w zakres prawa UE.Administratorzy takich podmiotów oraz ich inspektorzy ochrony danych powinni być świadomi tego, że w przypadku zaistnienia takich spornych spraw, powinni konsultować się z organami ochrony danych.

1.4.7 „Zmodernizowana" Konwencja Rady Europy o ochronie danych z 2018 roku

Chociaż Konwencja Rady Europy z 1981 roku została (w szeroki zakresie) uzgodniona z Dyrektywą WE o ochronie danych z 1995 roku poprzez dodanie w przyjętym w 2001 roku (patrz: pkt 1.3.2) Protokole dodatkowym zasad dotyczących transgranicznego przepływu danych i niezależnych organów ochrony danych, mimo to - podobnie jak Dyrektywa - uległa w pewnym stopniu dezaktualizacji do końca pierwszej dekady XXI wieku. Prace nad „modernizacją" Konwencji rozpoczęto w 2011 roku, a „zmodernizowaną Konwencję" przyjęto i otwarto do podpisu 10 października 2018 roku[216]. W czasie pisania Podręcznika (grudzień 2018 r.) nie weszła ona jeszcze w życie: będzie to miało miejsce trzy miesiące później po tym, jak pięć państw członkowskich Rady Europy przystąpi do zmodernizowanej Konwencji (art. 26(2)), ale oczywiście nawet wtedy wyłącznie w odniesieniu do tych państw. Natomiast do pozostałych państw będących stronami Konwencji z 1981 roku (i w stosownym przypadku Protokołu dodatkowego) zastosowanie będzie miała stara Konwencja (i Protokół)[217].

Sama Rada Europy przedstawiła bardzo przydatny **przegląd nowych elementów zmodernizowanej Konwencji**, które przedstawiono poniżej[218]:

> Główne nowości[219] w zmodernizowanej Konwencji można przedstawić następująco:
>
> **Przedmiot i cel Konwencji (art. 1)**
>
> Zgodnie z art. 1 Konwencji jej cel jest wyraźnie określony i oznacza zapewnienie każdej osobie fizycznej w ramach systemu prawnego jednej ze Stron (bez względu na jej narodowość i miejsce zamieszkania) ochronę jej danych osobowych w trakcie przetwarzania, przyczyniającą się do poszanowania jej praw i podstawowych wolności oraz w szczególności prawa do prywatności.
>
> Konwencja podkreśla fakt, że przetwarzanie danych osobowych może w pozytywny sposób umożliwiać wykonanie innych podstawowych praw i wolności, co można ułatwić poprzez zapewnienie prawa do ochrony danych.
>
> **Definicje i zakres stosowania (art. 2 i 3)**
>
> Chociaż istotne zwroty, takie jak definicja danych osobowych oraz osoby, której dane dotyczą, nie zostały w ogóle zmienione[220], zaproponowano inne zmiany w definicjach - porzucono koncepcję „zbioru danych". „Administratora zbioru danych" zastąpiono „administratorem danych", w związku z którym dodatkowo zastosowano zwroty „przetwarzający" i „odbiorca".

---

[216] Zob. https://www.coe.int/en/web/data-protection/background-modernisation. „Zmodernizowana Konwencja" była już w znacznej mierze gotowa do 2014 roku, ale jej formalne otwarcie do podpisu opóźniono, częściowo, by umożliwić jej uspójnienie z RODO, a częściowo, by zająć się obawami zgłaszanymi przez jedno z głównych państw członkowskich Rady Europy. Protokół zmieniający Konwencję w sprawie ochrony osób fizycznych w zakresie automatycznego przetwarzania danych osobowych, CETS 223, dostępny jest na stronie: https://www.coe.int/en/web/conventions/search-on-treaties/-/conventions/treaty/223; Skonsolidowany tekst zmodernizowanej Konwencji dostępny jest na stronie internetowej: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf –

[217] Do połowy grudnia 2018 roku zmodernizowana Konwencja została podpisana przez 22 państw, z których jednak żadne jej w tym okresie jeszcze nie ratyfikowało. Patrz:
https://www.coe.int/en/web/conventions/search-on-treaties/-/conventions/treaty/223/signatures?p_auth=ZmXAeCCF

[218] Zaczerpnięto z: https://rm.coe.int/modernised-conv-overview-of-the-novelties/16808accf8. Wszystkie informacje na temat konkretnych zmian w tekście w formie tabeli porównawczej dostępne są na stronie: https://rm.coe.int/cahdata-convention-108-table-e-april2018/16808ac958 (26 stron)

[219] Niniejszy przegląd prezentuje nowości i nie powtarza postanowień już istniejących od czasu wprowadzenia Konwencji z 1981 roku i Protokołu dodatkowego z 2001 roku. Całą zmodernizowaną Konwencję opublikowano w ujednoliconej wersji na stronie [Rady Europy] (oryginalny przypis z uwzględnieniem edycji).

[220] Należy jednak zauważyć, że szerokie wyjaśnienia dodano w Memorandum wyjaśniającym do zmodernizowanej Konwencji (dodany przypis).

Zakres stosowania obejmuje zarówno zautomatyzowane, jak i niezautomatyzowane przetwarzanie danych osobowych (przetwarzanie ręczne, gdy dane stanowią element struktury umożliwiającej wyszukiwanie według osób, których dane dotyczą, zgodnie ze z góry ustalonymi kryteriami), które podlega systemowi prawnemu strony Konwencji. Zachowano zbiorowy charakter Konwencji, a zakres naturalnie w dalszym ciągu obejmuje przetwarzanie zarówno w sektorze prywatnym, jak i publicznym, gdyż jest to jedna z najistotniejszych mocnych stron Konwencji.

Z drugiej strony, Konwencja nie ma już zastosowania do przetwarzania danych przez osoby fizyczne w celu realizacji wyłącznie osobistych czynności domowych[221].

Ponadto Strony nie mają już możliwości składania deklaracji mających na celu zwolnienie pewnych rodzajów przetwarzania danych ze stosowania Konwencji (np. cele bezpieczeństwa narodowego i obronności).

Obowiązki stron (art. 4)

Każda strona musi przyjąć w swoim prawie krajowym środki niezbędne, by wprowadzić w życie postanowienia Konwencji.

Ponadto każda strona powinna udowodnić, że środki takie zostały faktycznie podjęte i są skuteczne, oraz zaakceptować fakt, że Komitet ds. Konwencji może sprawdzić, czy wymagania te są przestrzegane. [*Nowy*] proces oceny stron („mechanizm monitorowania") jest konieczny, by mieć pewność, że strony są faktycznie w stanie zagwarantować ustalony Konwencją poziom ochrony.

Należy zauważyć, że organizacje międzynarodowe mają teraz możliwość przystąpienia do Konwencji (art. 27), podobnie jak Unia Europejska (art. 26).

Zasadność przetwarzania danych i jakość danych (art. 5)

Artykuł 5 wyjaśnia stosowanie zasady proporcjonalności w celu podkreślenia, że należy ją stosować w całym procesie przetwarzania, w szczególności w odniesieniu do środków i metod stosowanych w przetwarzaniu. Ponadto wzmocniono ją zasadą minimalizacji danych.

Nowe postanowienie wprowadzono, by jasno określić zasadę prawną przetwarzania - zgoda (która, by była ważna, musi spełniać kilka kryteriów) osoby, której dane dotyczą, lub innego rodzaju uzasadniona podstawa przewidziana prawem (umowa, istotny interes osoby, której dane dotyczą, obowiązek prawny administratora, itp.).

Wrażliwe dane (art. 6)

Katalog wrażliwych danych został poszerzony o dane genetyczne i biometryczne (które wpływały na UE), a także dane przetwarzane dla celów informacji, jaką ujawniają, dotyczącej członkostwa w związkach zawodowych lub pochodzenia etnicznego (te dwie ostatnie kategorie dodano do istniejącego [*stosowanego z zasady*] zakazu przetwarzania danych osobowych ujawniających pochodzenie rasowe, poglądy polityczne lub religijne albo inne przekonania, stan zdrowia lub życie seksualne oraz danych osobowych dotyczących przestępstw, postępowania karnego i wyroków skazujących).

Bezpieczeństwo danych (art. 7)

Jeżeli chodzi o bezpieczeństwo danych, wprowadzono wymóg bezzwłocznego zgłaszania wszelkich naruszeń bezpieczeństwa. Wymóg ten ogranicza się do spraw, które mogą poważnie ingerować w prawa i podstawowe wolności osób, których dane dotyczą, które należy zgłosić przynajmniej organom nadzorczym.

Przejrzystość przetwarzania (art. 8)

Administratorzy mają obowiązek zagwarantować przejrzystość przetwarzania danych i w tym celu muszą zapewnić wymagany zestaw informacji, w szczególności dotyczących swojej tożsamości i zwyczajowego miejsca zamieszkania lub prowadzenia działalności, podstawy prawnej i celów przetwarzania, odbiorców danych oraz kategorii przetwarzanych danych osobowych. Powinni ponadto przekazać dodatkowe informacje konieczne do zapewnienia uczciwego i przejrzystego przetwarzania. Administrator jest zwolniony z obowiązku przekazania takich informacji, jeżeli

[221] Takie „wyłącznie osobiste przetwarzanie" zostało po raz pierwszy wykluczone z przepisów o ochronie danych w Dyrektywie z 1995 roku w celu zapewnienia poszanowania prawa do życia prywatnego i powtórzono je w RODO (dodany przypis).

przetwarzanie jest wyraźnie przewidziane prawem lub przekazanie takich informacji okaże się niemożliwe albo wymaga nieproporcjonalnych starań.

Prawa osoby, której dane dotyczą (art. 9)

Osobom, których dane dotyczą, przyznaje się nowe prawa, tak aby posiadały one większą kontrolę nad swoimi danymi w erze cyfrowej.

Zmodernizowana Konwencja poszerza katalog informacji, jakie należy przekazać osobom, których dane dotyczą, gdy korzystają z przysługującego im prawa dostępu. Ponadto osoby, których dane dotyczą, mają prawo uzyskać informacje na temat przyczyn przetwarzania danych, którego wyniki ich dotyczą. To nowe prawo jest szczególnie istotne w odniesieniu do profilowania osób fizycznych[222].

Należy to powiązać z kolejną nowością, tj. prawem do niebycia przedmiotem decyzji, która ma skutki prawne dla osoby, której dane dotyczą, lub wywiera na nią poważny wpływ, a która zapada wyłącznie w trybie zautomatyzowanego przetwarzania bez uwzględnienia zdania osoby, której dane dotyczą.

Osoby, której dane dotyczą, mają prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania danych osobowych, chyba że administrator wykaże ważne i uzasadnione podstawy przetwarzania, które mają charakter nadrzędny wobec ich interesów lub podstawowych praw i wolności.

Dodatkowe obowiązki (art. 10)

Zmodernizowana Konwencja nakłada szersze obowiązki na podmioty przetwarzające dane lub zlecające przetwarzanie danych w ich imieniu.

Rozliczalność staje się integralną częścią systemu ochronnego, a administratorzy są zobowiązani udowodnić przestrzeganie zasad ochrony danych.

Administratorzy powinni podjąć wszelkie odpowiednie kroki - także gdy przetwarzanie zlecono podmiotowi zewnętrznemu - by zagwarantować prawo do ochrony danych (domyślna ochrona prywatności, zbadanie prawdopodobnego oddziaływania planowanego przetwarzania danych na prawa i podstawowe wolności osób, których dane dotyczą („ocena skutków dla ochrony danych") oraz domyślna ochrona prywatności).

Wyjątki i ograniczenia (art. 11)

Prawa przewidziane w Konwencji nie mają bezwzględnego charakteru i mogą zostać ograniczone, gdy jest to przewidziane prawem i stanowi środek konieczny w demokratycznym społeczeństwie w oparciu o określone i ograniczone podstawy. Wśród ograniczonych podstaw uwzględniono „zasadnicze cele interesu publicznego", a także odwołanie do prawa do wolności wypowiedzi.

Lista postanowień Konwencji, które można ograniczyć, została nieznacznie poszerzona (patrz odwołania do art. 7.1 w sprawie bezpieczeństwa oraz 8.1 w sprawie przejrzystości w art. 11.1), a nowy paragraf tego artykułu wyraźnie wspomina o czynnościach przetwarzania dla celów bezpieczeństwa narodowego i obronności narodowej, w którym to przypadku istnieje możliwość ograniczenia uprawnień Komitetu do monitorowania oraz niektórych misji organów nadzorczych. Wyraźnie określono wymóg, że czynności przetwarzania dla celów bezpieczeństwa narodowego i obronności narodowej muszą być przedmiotem niezależnego i efektywnego przeglądu oraz nadzoru.

Należy jeszcze raz przypomnieć, że w przeciwieństwie do poprzednich postanowień Konwencji 108 strony zmodernizowanej Konwencji nie będą już w stanie wyłączyć z zakresu jej stosowania określonych rodzajów przetwarzania.

Przepływ danych osobowych przez granice (art. 14)[223]

Celem tego postanowienia jest ułatwienie - tam, gdzie to stosowne - swobodnego przepływu informacji bez względu na granice, zapewniając jednocześnie odpowiednią ochronę osób fizycznych w związku z przetwarzaniem danych osobowych.

[222] Zob. Rekomendacja (2010) 13 w sprawie ochrony osób fizycznych w zakresie automatycznego przetwarzania danych podczas tworzenia profili wraz z Memorandum wyjaśniającym (oryginalny przypis).
[223] W tym względzie zmodernizowana Konwencja oparta jest na Protokole dodatkowym i przepisach UE.

Ze względu na brak zharmonizowanych zasad ochrony, które byłyby stosowane przez państwa należące do regionalnej organizacji międzynarodowej i które regulowałyby kwestie przepływu danych (patrz: na przykład ramowe przepisy UE o ochronie danych osobowych), należy więc zapewnić swobodny przepływ danych pomiędzy stronami.

Jeżeli chodzi o przepływ danych przez granice do odbiorcy, który nie podlega systemowi prawnemu strony, należy zagwarantować odpowiedni poziom ochrony w państwie lub organizacji odbiorcy. Ponieważ nie można tego z góry założyć, gdyż odbiorca nie jest stroną, Konwencja ustala dwa główne sposoby zapewnienia faktycznie odpowiedniego poziomu ochrony danych - albo na mocy prawa albo na mocy doraźnych lub zatwierdzonych standardowych zabezpieczeń, które są prawnie wiążące i możliwe do egzekwowania (tj. klauzul umownych lub wiążących zasad korporacyjnych), a także zostały należycie wdrożone.

Organy nadzorcze (art. 15)

Bazując na art. 1 Protokołu dodatkowego, zmodernizowana Konwencja uzupełnia katalog uprawnień organów o postanowienie, że poza uprawnieniami do ingerowania, dochodzenia, uczestniczenia w postępowaniach prawnych i zwracania uwagi władz sądowych na naruszenia przepisów o ochronie danych, organy te mają także obowiązek podnosić świadomość, informować i edukować wszystkie uczestniczące w procesie strony (osoby, których dane dotyczą, administratorów, przetwarzających itp.). Pozwala także organom na podejmowanie decyzji i nakładanie sankcji. Ponadto przypomniano, że organy nadzorcze powinny być niezależne w wykonywaniu tego typu obowiązków i uprawnień.

Forma współpracy (art. 17)

Zmodernizowana Konwencja porusza także kwestię współpracy (i pomocy wzajemnej) pomiędzy organami nadzorczymi.

Organy nadzorcze muszą koordynować swoje dochodzenia, prowadzić wspólne działania oraz przekazywać sobie nawzajem informacje i dokumenty na temat swoich przepisów i praktyk administracyjnych dotyczących ochrony danych.

Informacje wymieniane pomiędzy organami nadzorczymi obejmować będą dane osobowe, tylko wtedy gdy dane takie są decydujące dla współpracy oraz gdy osoba, której dane dotyczą, wyrazi konkretną, dobrowolną i świadomą zgodę.

W końcu, Konwencja stwarza forum dla zwiększonej współpracy - organy nadzorcze stron muszą stworzyć sieć, by zorganizować swoją współpracę i wykonywać swoje przewidziane w Konwencji obowiązki.

Komitet ds. Konwencji (art. 22, 23 i 24)

Komitet ds. Konwencji odgrywa istotną rolę w interpretowaniu Konwencji, zachęcaniu do wymiany informacji pomiędzy stronami oraz opracowaniu standardów ochrony danych.

Zmodernizowana Konwencja wzmacnia rolę i uprawnienia Komitetu. Nie pełni on już jedynie roli „doradczej", ale także ma prawo oceniać i monitorować. Poza wydawaniem opinii na temat poziomu ochrony danych przez państwo *tak, jak wcześniej, czyni to teraz także w odniesieniu do* organizacji międzynarodowych przed przystąpieniem do Konwencji. Komitet ten jest także w stanie ocenić przestrzeganie prawa krajowego danej strony oraz ustalić skuteczność podjętych środków (istnienie organu nadzorczego, zakres odpowiedzialności, istnienie skutecznych środków prawnych).

Komitet może także ocenić, czy normy prawne mające zastosowanie do przekazu danych stanowią wystarczającą gwarancję odpowiedniego poziomu ochrony danych.

Nie jest to miejsce na szczegółowe analizowanie tego typu nowości. Wystarczy wspomnieć, że **wprowadzają one w nowej „zmodernizowanej" Konwencji system bliski systemowi ustanowionemu dla UE zgodnie z RODO.** Oznacza to, że gdy UE będzie oceniać „adekwatność" systemu ochrony danych w kraju trzecim (co omówiono w części drugiej, pkt 2.1), fakt, że dany kraj trzeci jest stroną zmodernizowanej Konwencji będzie stanowić najważniejszą braną pod uwagę sprawę.

W rzeczywistości, jeżeli chodzi o **zakres**, zmodernizowana Konwencja wykracza poza RODO w tym sensie, że - co zostało bardzo wyraźnie zaznaczone zarówno w tekście zmodernizowanej Konwencji, jak

i w powyższym przeglądzie - państwa będące stronami zmodernizowanej Konwencji **nie będą już mogły wykluczyć ze swoich obowiązków**, takich jak ***bezpieczeństwo narodowe i obronność,*** żadnego rodzaju przetwarzania, gdyż są to sprawy wykraczające poza zakres unijnych instrumentów o ochronie danych[224].

To, czy pod innymi względami zmodernizowana Konwencja - lub precyzyjniej przepisy krajowe państw będących stronami zmodernizowanej Konwencji, które wdrażają Konwencję - będzie zawsze zgodna z RODO - lub dokładniej z RODO w formie, w jakiej rozporządzenie to będzie interpretowane i stosowane w przyszłości przez nową Europejską Radę Ochrony Danych UE, organy ochrony danych państw członkowskich UE, Komisję Europejską oraz Trybunał Sprawiedliwości UE - oczywiście okaże się z czasem.

Na przykład wprowadzone w zmodernizowanej Konwencji nowe zasady dotyczące przepływu danych przez granice pozwalają na przekaz danych do krajów trzecich, które zapewniają „***odpowiedni***" poziom ochrony (art. 14), co na pierwszy rzut oka może wydawać się podobne do wymogu „***odpowiedniego***" poziomu ochrony w RODO (a także Dyrektywie o ochronie danych z 1995 roku), ale dopiero okaże się czy lub w jaki sposób nowy Komitet ds. Konwencji postąpi zgodnie z orzeczeniami Trybunału Sprawiedliwości UE utrzymującymi że zwrot „odpowiedni" należy interpretować jako oznaczający, że dany kraj trzeci musi zapewnić „***zasadniczo równoważną***" ochronę (jak orzekł Trybunał Sprawiedliwości UE, interpretując zwrot „odpowiedni")[225].

W pozostałych kwestiach, np. jeżeli chodzi o **zgodę udzielaną przez dzieci**, zmodernizowana Konwencja nie jest tak szczegółowa ani konkretna jak RODO.

Wykluczając tego typu sprawy oczywiste jest, że w swoich wzajemnych relacjach Rada Europy i Unia Europejska przewodzą w ustalaniu globalnych „złotych standardów" ochrony danych, mających zastosowanie zarówno w ramach państw, jak i w odniesieniu do przepływu danych przez granice.

W końcu należy zauważyć, że zmodernizowana Konwencja (w przeciwieństwie do poprzedniej wersji) jest otwarta dla organizacji międzynarodowych, co oznacza, że może zostać formalnie podpisana także przez Unię Europejską.

- o – O – o -

[224] Zob. pkt 1.3.1 powyżej „*Charakter i ograniczenia dyrektyw WE*", jeżeli chodzi o ograniczenie w stosunku do dyrektyw o ochronie danych z 1995 i 2002 roku, oraz Część drugą, pkt 2.1 poniżej, jeżeli chodzi o RODO. W związku z przetwarzaniem dla celów egzekwowania prawa (itp.) oraz przetwarzania przez same instytucje UE, UE oczywiście posiada stosowne zasady, które są w zasadniczej mierze zgodne ze standardami RODO (i tym samym zmodernizowanej Konwencji) (lub w przypadku instytucji UE będą takie, gdy zostaną uzgodnione z RODO).

[225] Trybunał Sprawiedliwości UE, wyrok w sprawie *Schrems* (przypis 73 powyżej), par. 73, wyrok TSUE z dnia 6 października 2015 r. C-362/14.

CZĘŚĆ 2

Ogólne rozporządzenie o ochronie danych

2.1 Wprowadzenie

Jak już wspomniano w pkt. 1.4.1 powyżej, Ogólne rozporządzenie o ochronie danych (RODO lub Rozporządzenie) zostało przyjęte częściowo dlatego że Dyrektywa o ochronie danych z 1995 roku nie zapewniła wystarczającego poziomu harmonizacji przepisów w państwach członkowskich, częściowo w odpowiedzi na masową ekspansję przetwarzania danych osobowych od momentu wprowadzenia Dyrektywy o ochronie danych z 1995 roku, a częściowo w odpowiedzi na orzecznictwo Trybunału Sprawiedliwości UE. Teraz okaże się, czy RODO wystarczy, by w pełni objąć zmiany w zakresie coraz bardziej inwazyjnych technologii, takich jak Big Data, internet rzeczy, oparty na algorytmach proces decyzyjny oraz wykorzystanie sztucznej inteligencji.

Rozporządzenie bazuje na Dyrektywie o ochronie danych z 1995 roku, jednak znacząco ją poszerza i jednocześnie zdecydowanie wzmacnia główny system ochrony danych w UE. Wprowadza *większą harmonizację, silniejsze prawa osób, których dane dotyczą, bliższą transgraniczną współpracę pomiędzy organami ochrony danych, silniejsze uprawnienia egzekucyjne i* znacznie więcej.

Dla ułatwienia Załącznik 1 do niniejszego Podręcznika zawiera *Spis rozdziałów, ustępów i artykułów RODO.* Załącznik 2 zawiera pełen tekst Rozporządzenia opublikowany w Oficjalnym Dzienniku UE, wraz motywami.

Punkt 3.2 objaśnia status i podejście RODO oraz bardziej szczegółowo omawia implikacje wynikające z faktu, że RODO zawiera klauzule pozwalające na dalsze uregulowanie pewnych kwestii na poziomie krajowym (podważając w ten sposób cel pełniejszej harmonizacji).

Punkt 3.3 zawiera przegląd RODO rozdział po rozdziale, sekcję po sekcji i artykuł po artykule.

Następnie przejdziemy do dwóch podstawowych kwestii dotyczących inspektorów ochrony danych - nowej zasady „rozliczalności" (obowiązek potwierdzenia zgodności) (pkt 3.4) oraz zasad mianowania, wymogów, warunków i obowiązków (itp.) inspektora ochrony danych (pkt 3.5) oraz wyjaśnimy istniejące pomiędzy nimi powiązania.

2.2 Status i podejście RODO - bezpośrednie z klauzulami precyzującymi

Rozporządzenie ...

RODO jest **rozporządzeniem**, tzn. prawem UE, które ma ***bezpośrednie zastosowanie*** w porządku prawnym państw członkowskich UE (oraz państw EOG niebędących członkami UE) bez konieczności transponowania na prawo krajowe, jak ma to miejsce w przypadku dyrektyw, takich jak Dyrektywa o ochronie danych z 1995 roku.

Ustawodawca unijny wybrał tą drogę celowo, ponieważ wdrożenie Dyrektywy z 1995 rok było nierówne - została ona różnie wdrożona w różnych państwach członkowskich, co doprowadziło do braku harmonizacji[226].

Dodatkowo w przynajmniej części krajów, takich jak Zjednoczone Królestwo, dyrektywę wdrożono w niewystarczającym stopniu[227].

W teorii rozporządzenie, mające bezpośrednie zastosowanie, powinno prowadzić do **pełnej harmonizacji** prawa w obszarze, który obejmuje. W przypadku RODO wzmacniają to znacznie silniejsze ustalenia dotyczące **wymiany informacji i współpracy** pomiędzy organami nadzorującymi (krajowymi

[226] Wniosek taki wyciągnięto już w zleconym przez Unię Europejską badaniu przeprowadzonym przez Douwe Korffa, Report on an EU study on the implementation of the [1995] data protection directive, 2002, zob. link: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1287667 – ale zajęcie się tym i zaproponowanie rozporządzenia zajęło UE kolejne 10 lat.

[227] Według Komisji UE w 2011 roku prawie jedna trzecia z 34 artykułów Dyrektywy nie została jeszcze właściwie wdrożona przez Zjednoczone Królestwo, patrz: http://amberhawk.typepad.com/amberhawk/2011/02/european-commission-explains-why-uks-data-protection-act-is-deficient.html. Chociaż Komisja zagroziła podjęciem działań egzekucyjnych, nie uczyniła tego, mimo że braków nigdy właściwie ani w pełni nie naprawiono.

organami nadzorczymi lub organami ochrony danych) oraz niżej opisanego szczególnego **mechanizmu „spójności".**

Jednoczesnie, jak przedstawiono w kolejnym podpunkcie, RODO w dalszym ciągu pozostawia wiele kwestii do dalszego uregulowania w prawie krajowym państw członkowskich UE, zgodnie z ich wewnętrznym systemem instytucjonalnym lub prawnym. Może to w niektórych obszarach podważać cel pełnej harmonizacji, ale - jak omówimy to w punktach zatytułowanych *„Wymogi dotyczące „klauzul precyzujących*" oraz *„Współpraca i spójność*" - istnieją także ograniczenia co do wolności państw członkowskich w tym zakresie oraz nowe środki nadzoru na poziomie UE, także związane z korzystaniem z takich „elastycznych" rozwiązań (przynajmniej w teorii).

... ale z „ klauzulami precyzującymi "[228]

Chociaż Rozporządzenie ma na celu większą harmonizację, w dalszym ciągu zawiera liczne „**elastyczne"** postanowienia, określane przez Komisję jako "klauzule precyzujące", odbiegające od prawa w państwach członkowskich, w szczególności w odniesieniu do sektora publicznego, ale także w odniesieniu do obowiązków nałożonych przez prawo krajowe na przedsiębiorstwa podlegające systemowi prawnemu odpowiedniego państwa członkowskiego (np. prawu pracy lub zasadom egzekwowania prawa) oraz na skład organu ochrony danych.

Rodzaje „klauzul precyzujących"

Włoski organ ochrony danych, *Garante della Privacy*, ustalił cztery różne (chociaż w pewnym stopniu zazębiające się) rodzaje klauzul, które pozostawiają miejsce do dalszej regulacji w prawie państw członkowskich[229]:

- **Dalsze specyfikacje**

Są to postanowienia, na mocy których państwa członkowskie mogą utrzymać lub wprowadzić *„konkretniejsze postanowienia w celu dostosowania stosowania*" odpowiednich przepisów Rozporządzenia (w tym celu stosowane są różne zwroty).

Przykłady:

Państwa członkowskie mogą określić, jakie operacje przetwarzania wymagają **wcześniejszej autoryzacji** lub uregulować kwestie dotyczące wykorzystania ***krajowych numerów identyfikacyjnych*** lub przetwarzania ***danych osobowych pracowników*.**

Państwa członkowskie mogą *„zachować lub wprowadzić **dalsze warunki, w tym ograniczenia** w odniesieniu do przetwarzania **danych genetycznych, danych biometrycznych lub danych dotyczących zdrowia***" poza warunkami i ograniczeniami przewidzianymi w RODO w art. 9(1) - (3) (artykuł dotyczący „szczególnych kategorii danych osobowych", zazwyczaj zwanych „wrażliwymi danymi") (art. 9(4)). Mogą więc na przykład przewidzieć, że w przypadku przetwarzania **danych genetycznych** zawsze wymagana jest ***wcześniejsza zgoda*.**

- **Możliwości i wybór**

Pod pewnymi względami RODO pozwala państwom członkowskim - poprzez ich prawo krajowe - **wybierać** z pewnych możliwości wyraźnie określonych w Rozporządzeniu albo poszerzyć obowiązek lub zakaz, który zgodnie z RODO ma zastosowanie jedynie w pewnych sytuacjach, o inne sytuacje.

Na przykład państwa członkowskie mogą zezwolić ***dzieciom*** w wieku powyżej 13, 14 lub 15 roku życia na ***wyrażenie zgody na pewne usługi informacyjne,*** a nie, jak przewiduje RODO, tyko osobom powyżej 16 roku życia, lub mogą wymagać **wyznaczenia inspektora ochrony danych**, gdy RODO tego nie wymaga.

228 Zobacz podrozdział „Związek między dyrektywą o prywatności i łączności elektronicznej a RODO" powyżej.

229 Antonio Caselli, pracownik *Garante*, prezentacja na pierwszej sesji szkoleniowej „T4DATA", czerwiec 2018, na temat *„RODO i zasad krajowych*". Istotę prezentacji opisano i w pewnym stopniu rozwinięto w Załączniku 4 do Podręcznika (w tomie drugim), gdzie podano też dodatkowe przykłady.

- **Ograniczenia i odstępstwa**

  Z zastrzeżeniem pewnych dość szeroko określonych **warunków** (omówionych poniżej w punktach zatytułowanych *„Wymagania dotyczące „klauzul precyzujących""* oraz *„Problemy wynikające „klauzul precyzujących""*, art. 23 RODO pozwala na **ogólnikowe ograniczenie** zasadniczo wszystkich praw osób, których dane dotyczą, w związku z szeroko definiowanymi **istotnymi celami interesu publicznego:** ***bezpieczeństwem narodowym, obroną, bezpieczeństwem publicznym, egzekwowaniem prawa i ochroną niezależności sądów,*** ale także ***ochroną interesów gospodarczych i finansowych państwa,*** egzekwowaniem ***etyki zawodowej***, wszelkiego rodzaju ***funkcjami kontrolnymi, inspekcyjnymi lub regulacyjnymi*** *związanymi, nawet sporadycznie, ze sprawowaniem władzy* w jakimkolwiek powszechnie chronionym interesie, ***ochroną osoby, której dane dotyczą, lub praw i wolności innych osób*** oraz ***egzekucją roszczeń cywilnoprawnych.***

  Art. 85, 86 i 89 RODO zawierają postanowienia, które z jednej strony pozwalają na **odstępstwa** (a pod pewnymi względami wymagają odstępstw) od pewnych zasad RODO w celu ochrony **wolności wypowiedzi,** zapewniają **wolność informacji** (dostępu do dokumentów i informacji znajdujących się w posiadaniu organów publicznych) i **archiwizacji** oraz ułatwiają prowadzenie (ogólnie korzystnych) **badań**, a z drugiej strony nakładają pewne **warunki** na tego typu odstąpienia (które dokładniej omówiono w punktach poniżej, zatytułowanych *„Wymagania dotyczące <klauzul precyzujących>"* oraz *„Problemy wynikające z „<klauzul precyzujących>")*.

  Uwaga: niektóre z tych szczególnych zasad mają chronić interesy „innych", natomiast pozostałe są postrzegane jako leżące w interesie ogólnym lub publicznym, a niektóre - jak wolność informacji - służą obydwu tym celom. Są to sprawy, których zasad do tej pory nie poddano harmonizacji, chociaż w niektórych państwach członkowskich UE nadzór zarówno nad ochroną danych, jak i wolnością informacji przekazano w ręce tych samych organów. Zważywszy, że kwestie te mają coraz bardziej transgraniczny charakter, np. transgraniczne wnioski o dostęp do danych publicznych, wolność wypowiedzi a ochrona danych i kwestie prywatności dotyczące publikacji w internecie oraz międzynarodowe badania medyczne, należy oczekiwać, że Europejska Rada Ochrony Danych wyda dalsze wytyczne w tym zakresie, w szczególności w odniesieniu do czynności transgranicznych. Komisja może także zaproponować podjęcie nowych inicjatyw w tym zakresie.

- **Obowiązki regulacyjne**

  Pod pewnymi względami innymi niż te wspomniane powyżej, w szczególności w związku z ustanowieniem niezależnych organów nadzorczych (organy ochrony danych) oraz programów certyfikacji, RODO **wymaga** od państw członkowskich przyjęcia szczegółowych zasad i przepisów wdrażających odpowiednie wymagania dla organów ochrony danych w ich krajowym porządku prawnym. Są to w znacznej mierze kwestie techniczne (chociaż wymagają także zgodności z istotnymi standardami, np. w zakresie niezależności oraz zapewnienia wystarczających zasobów).

Wymagania dotyczące „klauzul precyzujących"

Pod wieloma względami, z uwzględnieniem tych wspomnianych powyżej we fragmencie zatytułowanym *„dalsze specyfikacje"* oraz *„możliwości i wybór*", ale szczególnie tych wymienionych pod tytułem *„ograniczenia i odstępstwa*", RODO **wymaga** od państw członkowskich przyjęcia **zasad prawnych** dotyczących właściwych kwestii, ***które spełniają określone standardy demokratyczne/standardy dotyczące praw człowieka.***

Inne postanowienia (nieuwzględnione w wyżej wspomnianych fragmentach) także **sugerują potrzebę regulacji**, gdyż wymagają od państw członkowskich przyjęcia ***„odpowiednich zabezpieczeń***", ***„właściwych zabezpieczeń"*** lub ***„odpowiednich środków"*.** Ponieważ samo RODO często nie wyjaśnia, o jakie zabezpieczenia lub środki chodzi, państwa członkowskie będą musiały wyjaśnić to w swoich prawie krajowym, które również będzie musiało spełniać określone ***standardy*** demokratyczne/prawne.

Należy zauważyć, że **w tym zakresie nie nadano państwom członkowskim po prostu nieograniczonych uprawnień dyskrecjonalnych,** ponieważ z wymogów jasno wynika, że pewne środki lub zabezpieczenia muszą być „właściwe" lub „odpowiednie". Pod innymi względami, pewne ogólnie obowiązujące

standardy i warunki prawne zostały wyraźnie wymienione w RODO, ale faktycznie podobne standardy i warunki mają zastosowanie do wszystkich odpowiednich rozporządzeń.

Tak więc RODO wyraźnie przewiduje, że z zasady ogólnikowe odstępstwa dopuszczalne na mocy art. 23 (podsumowanego powyżej w punkcie zatytułowanym „*Ograniczenia i odstępstwa*") muszą zostać określone w **prawie** (***„akcie prawnym"***), który ***„nie narusza istoty podstawowych praw i wolności*** *oraz jest w demokratycznym społeczeństwie* ***środkiem niezbędnym i proporcjonalnym****, służącym"* odpowiedniemu interesowi. Wymagania takie stanowią bezpośrednie odzwierciedlenie wymogów, jakie muszą zostać spełnione przez ograniczenie któregokolwiek z głównych praw chronionych Europejską Konwencją Praw Człowieka (EKPC) i Kartą praw podstawowych UE (KPP). Cytując:

> Wszelkie ograniczenia w korzystaniu z praw i wolności uznanych w niniejszej Karcie muszą być przewidziane ustawą i **szanować istotę** tych praw i wolności. Z zastrzeżeniem zasady **proporcjonalności**, ograniczenia mogą być wprowadzone wyłącznie wtedy, gdy są **konieczne i rzeczywiście odpowiadają celom interesu ogólnego** uznawanym przez Unię lub **potrzebom ochrony praw i wolności innych osób.**
>
> (art. 52(1), pogrubienie dodane przez autorów Podręcznika)

Ponieważ każde ograniczenie lub zawężenie przez przepisy państwa członkowskiego prawa osoby, której dane dotyczą, na mocy „klauzul precyzujących" RODO musi być postrzegane jako ograniczenie gwarantowanego Kartą praw podstawowych UE prawa do ochrony danych (art. 8), wszystkie te przepisy muszą spełniać wyżej wskazane standardy.

A konkretnie, odpowiednie prawo musi spełniać istotne **wymagania dotyczące jakości**: zasady prawa muszą być „**zgodne z państwem prawa**" (co oznacza w szczególności, że nie mogą być ***dyskryminujące*** ani ***arbitralne*** oraz muszą być ***zaskarżalne*** oraz podlegać ***skutecznym środkom***), a także **dostępne** *(tj.* ***opublikowane****)* i wystarczająco **jasne** oraz **precyzyjne,** by były „***przewidywalne***" w swoim zastosowaniu[230].

Odwołanie do „poszanowania **istoty**" wspomnianych praw i wolności należy rozumieć jako **zakaz stosowania reguł prawnych, które głęboko naruszają prawo do ich unieważnienia.** Na przykład Trybunał Sprawiedliwości Unii Europejskiej uznał, że[231]:

> ustawodawstwo zezwalające organom publicznym generalnie na dostęp do treści komunikatów elektronicznych należy traktować jako zagrażające istocie podstawowego prawa do poszanowania życia prywatnego, gwarantowanego art. 7 Karty ...

Odstępstwa stosowane przez państwa członkowskie na mocy art. 23 RODO w szczególności, z uwzględnieniem odstępstw od zasad ochrony danych w celu zapewnienia bezpieczeństwa narodowego i obronności, mogą tym samym nigdy nie być równoznaczne z nadmiernymi odstępstwami od głównych zasad, których nigdy nie zagwarantowano oraz które nigdy nie będą mogły zostać zaakceptowane.

A konkretniej, wszelkie odstępstwa od art. 23 oraz w rzeczywistości wszelkie innego rodzaju wyłączenia od normalnych zasad w RODO na podstawie którejkolwiek z „klauzul precyzujących" muszą być „**konieczne i proporcjonalne w demokratycznym społeczeństwie**". Oznacza to, że każde odstąpienie od normalnych zasad lub ograniczenie nieuznawanego za bezwzględne prawa osoby, której dane dotyczą, na podstawie „klauzuli precyzującej" musi rzeczywiście realizować ***„uzasadniony cel" / „istotny cel interesu publicznego"****,* odpowiadać na ***„pilną potrzebę społeczną***" oraz być ***„w uzasadnionym zakresie proporcjonalne"*** w stosunku do takiej potrzeby. Decydując, co dokładnie jest w tym względzie potrzebne, państwa mogą uzyskać pewien ***„margines swobody***"[232], ale margines ten ogranicza wymóg, że środek (odstąpienie lub ograniczenie) musi być ***„w demokratycznym społeczeństwie"*** niezbędny.

---

[230] Zob. Harris, O'Boyle & Warbrick, Law of the European Convention on Human Rights, II wydanie, 2009, rozdział 8, pkt 3, *Limitations*. Prosty przegląd odpowiednich wymogów Europejskiej Konwencji Praw Człowieka – zob. Douwe Korff, The standard approach under articles 8 – 11 ECHR and article 2 ECHR (Podręcznik do nauczania), https://www.pravo.unizg.hr/_download/repository/KORFF_-_STANDARD_APPROACH_ARTS_8-11_ART2.pdf. Zob. w szczególności: tekst pod pytaniami 3 (Law) i 5 (Necessary and proportionate).

[231] Trybunał Sprawiedliwości UE, wyrok w sprawie *Schrems* (przypis 73 powyżej), par. 94.

[232] Doktryna „marginesu swobody", która jest mocno zakorzeniona w orzecznictwie Europejskiego Trybunału Praw Człowieka, jest znacznie mniej czytelnie wyrażona przez Trybunał Sprawiedliwości UE, który, jeżeli w ogóle, raczej wspomina o „uznaniu" lub „marginesie uznania" przypisywanego w pewnych sytuacjach państwom członkowskim. Jednak dla celów niniejszego

Ogólnie mówiąc, jeżeli istnieją **wyraźne wskazówki** w konkretnej sprawie, takie jak zostały przedstawione w ramach Dyrektywy o ochronie danych z 1995 roku przez Grupę Roboczą Art. 29 i Europejskiego Inspektora Ochrony Danych, a obecnie w RODO przez Europejską Radę Ochrony Danych (której członkiem jest EIOD), i/lub jeżeli istnieje **znaczna zbieżność poglądów** w sprawie pomiędzy państwami członkowskimi (lub ich organami ochrony danych), wtedy każda rozbieżność od takich wytycznych lub takiego konsensusu ze strony jednego państwa członkowskiego prawdopodobnie wskazuje, że rozbieżne środki (odstępstwa lub ograniczenia wykraczające poza to, co uznano za konieczne lub proporcjonalne w innych państwach członkowskich) nie są „konieczne" lub „proporcjonalne" „w demokratycznym społeczeństwie".

Jednak, jak zauważono w kolejnym punkcie, spraw takich nie można rozstrzygnąć poprzez zastosowanie „mechanizmów współpracy i spójności" (omówionych w dalszej części Podręcznika).

Problemy wynikające z „klauzul precyzujących"

Omówiliśmy „klauzule precyzujące" bardziej szczegółowo, ponieważ rodzą one problemy w skutecznym stosowaniu RODO. Wyróżniamy dwie formy takich problemów.

Po pierwsze, „klauzule precyzujące" będą ze względu na swój charakter prowadzić do stosowania **różnych (bardziej lub mniej szczegółowych) zasad, odzwierciedlających specyficzne cechy krajowe, w identycznych kwestiach w różnych państwach członkowskich.** Nie rodzi to dużego problemu w odniesieniu do przetwarzania, które ma miejsce w całości w jednym państwie członkowskim i dotyczy tylko osób, których dane dotyczą, w tym państwie członkowskim. Jednak, jak już zauważono, w XXI wieku coraz więcej działań państwowych niesie za sobą międzynarodowe implikacje i obejmuje transgraniczne operacje przetwarzania danych osobowych, także w sektorze publicznym, a nie tylko w odniesieniu do egzekwowania prawa lub granic. Dzieje się tak w szczególności w UE ze względu na „cztery wolności", które mają fundamentalne znaczenie dla europejskiego projektu - wolność przemieszczania się towarów, usług, ludzi i środków finansowych.

Gdy towary lub usługi są oferowane i nabywane poprzez granicę, w ramach UE lub nie, wraz z transakcją przekazywane są dane osobowe (mające istotne znaczenie dla danej transakcji). Gdy ludzie się przemieszczają, robią to także ich dane: ich dane dotyczące podatków, opieki społecznej i świadczeń emerytalnych, dane medyczne, dane dotyczące małżeństwa, narodzin, rozwodu, śmierci i zamieszkania. Realizacja płatności (pomiędzy jednostkami lub pomiędzy jednostkami i prywatnymi podmiotami albo pomiędzy jednostkami i agencjami państwowymi, takimi jak urząd podatkowy, meldunkowy lub emerytalny) pociąga za sobą przepływ danych finansowych i innych danych. Dzieje się to *a fortiori*, gdy przetwarzanie lub część przetwarzania odbywa się w internecie.

Gdy w takich okolicznościach istnieją różne zasady w różnych państwach członkowskich troszczących się o przetwarzanie takich danych, rodzi to potencjalne (i potencjalnie poważne) **kwestie prawne**, które będą musiały być rozwiązywane indywidualnie dla każdego przypadku (co często nie będzie łatwe). Ilustrują to niżej podane przykłady, które nawiązują do pewnych konkretnych odstępstw i ograniczeń, jakie mogą zostać wprowadzone na mocy wcześniej wspomnianych „klauzul precyzujących".

Przykłady:

- Jeżeli jedno państwo członkowskie nakłada na stosowanie krajowego numeru identyfikacyjnego ograniczenia, których nie stosuje się w innym państwie członkowskim, czy ograniczeń takich w dalszym ciągu musi przestrzegać odbiorca w tym drugim państwie członkowskim (z uwzględnieniem odbiorcy w sektorze publicznym), jeżeli numer taki jest do niego przekazywany?
- Jeżeli jedno państwo członkowskie nakłada „dodatkowe warunki" lub dodatkowe „ograniczenia" na przetwarzanie wszystkich lub pewnych rodzajów wrażliwych danych (np. na stosowanie danych biometrycznych lub genetycznych, których to ograniczeń nie stosuje się w

Podręcznika doktrynę tą można potraktować jako odzwierciedlenie orzecznictwa zarówno sądu w Strasburgu, jak i sądu w Luksemburgu, nawet jeżeli w różnym stopniu oraz w zależności od kontekstu. Zob. Francisco Javier Mena Parras, From Strasbourg to Luxembourg? Transposing the margin of appreciation concept into EU law, Bruksela, 2008, http://www.philodroit.be/IMG/pdf/fm_transposing_the_margin_of_appreciation_concept_into_eu_law_-_2015-7.pdf.

innym państwie członkowskim, czy takich warunków lub ograniczeń w dalszym ciągu musi przestrzegać odbiorca w tym drugim państwie członkowskim (z uwzględnieniem odbiorcy w sektorze publicznym), jeżeli dane takie są do niego przekazywane?

- Jeżeli jedno państwo członkowskie ustala wiek, w którym wymagana jest zgoda na użytkowanie usług informacyjnych dla dzieci, na powiedzmy 14 lat, a inne państwo członkowskie pozostawia wiek przewidziany w RODO, tj. 16 lat, czy dostawca usług informacyjnych w pierwszym państwie członkowskim może świadczyć swoje usługi dzieciom w wieku 14 lat w tym drugim państwie członkowskim w oparciu o zgodę osoby 14-letniej? Czy dostawca powinien wprowadzić rozróżnienie na podstawie adresu IP dziecka (nawet mimo że to, że nawet 14-latek możne łatwo poradzić sobie z „podrobieniem" VPN)?
- Jeżeli jedno państwo członkowskie wymaga uzyskania uprzedniej autoryzacji organu ochrony danych na przetwarzanie w związku z opieką społeczną i zdrowiem publicznym, a inne państwo członkowskie nie robi tego, czy organ publiczny w tym drugim państwie może przetwarzać dane osobowe dotyczące osób, których dane dotyczą, w pierwszym państwie członkowskim w tych celach bez takiej uprzedniej autoryzacji, co może mieć miejsce w odniesieniu do dzieci imigrantów, którzy zostawiają swojego małżonka i dzieci w swoim kraju ojczystym i pracują w innym państwie członkowskim, ale świadczenia na dziecko itp. są wypłacane małżonkom w kraju ojczystym? (Uwaga: w kontekście udzielania uprzedniej autoryzacji odpowiedni organ ochrony danych najprawdopodobniej nałoży pewne zabezpieczenia i ograniczenia lub będzie wymagać ich nałożenia. Czy agencja państwowa w innym państwie członkowskim musi ich także przestrzegać? Czy będzie ona o nich w ogóle wiedziała?)

Powyższe kwestie zdecydowanie pogarsza **nieobecność w RODO postanowienia o „odpowiednim prawie"** zgodnego z postanowieniem zawartym w Dyrektywie o ochronie danych z 1995 roku (nawet jeżeli postanowienie z art. 4, rodziło pytania w odniesieniu do różnych tłumaczeń i pod względem skuteczności[233]. Prawdopodobnie postanowienie takie zostało opuszczone w RODO, ponieważ założono, że jako rozporządzenie RODO będzie stosowane w pełni zharmonizowany sposób. Jednak, jak przedstawiono powyżej, w wielu obszarach podlegających „klauzulom precyzującym" (które muszą zostać rozstrzygnięte na poziomie krajowym w konkretnych przepisach) oczywiście sytuacja taka nie będzie miała miejsca.

Druga kwestia dotyczy **zgodności** z wyżej określonymi **wymogami państwa prawa.** Prawdopodobnie pojawią się wątpliwości co do tego, czy niektóre przepisy w niektórych państwach członkowskich, które ograniczają pewne prawa lub łagodzą pewne zasady, są wystarczająco dostępne, precyzyjne i przewidywalne w swoim stosowaniu, konieczne lub proporcjonalne do odpowiedniego (uzasadnione/istotnego) celu.

Kwestii tych nie można często rozstrzygnąć ani nawet rozpatrzyć w ramach niżej omówionych „mechanizmów współpracy i spójności", ponieważ mechanizmy te ograniczają się do współpracy w związku z krokami podjętymi lub zaproponowanymi przez organy ochrony danych - nie można ich stosować, by naprawić braki w prawie państw członkowskich. Może to rodzić poważne problemy, w szczególności w odniesieniu do przekazu danych osobowych z agencji państwowej w jednym państwie członkowskim UE do agencji państwowej w innych państwach członkowskich, jeżeli w drugim państwie dane będą przetwarzane na mocy prawa, które zapewne nie spełnia wymogów państwa prawa. Jednak doświadczenia w innych obszarach (takich jak sprawiedliwość i sprawy wewnętrzne, których nie omówiono w pierwszym wydaniu Podręcznika) pokazują, że tam, gdzie to konieczne, można podjąć działania dotyczące takich kwestii, w szczególności na podstawie sugestii lub propozycji Komisji lub Europejskiej Rady Ochrony Danych.

Implikacje dla inspektorów ochrony danych

Z powyższego powinno jasno wynikać, że inspektorzy ochrony danych powinni znać oraz **badać nie tylko zasady RODO, ale także odpowiednie krajowe zasady oparte na przewidzianych w RODO „klauzulach**

[233] Zob. Douwe Korff, *The question of applicable law"*, w: Compliance Guide 3 – Interim report, Privacy Laws & Business, listopad 1999 r.

precyzujących", a także w pewnym zakresie odpowiednie przepisy i zasady obowiązujące w innych państwach członkowskich i krajach trzecich, jeżeli ich organizacja ujawnia do takich innych państw dane osobowe.

Może to przybierać wiele form. W niektórych przypadkach państwa członkowskie mogą po prostu zatrzymać zasady, które obowiązywały przez wejściem w życie RODO, z uwzględnieniem szczególnych odstępstw, by chronić istotne interesy publiczne albo ułatwić badania, chociaż **nie zawsze spełniają one przewidziane w odpowiednich „klauzulach precyzujących" wymogi państwa prawa lub są „stosowne" albo „odpowiednie" w rozumieniu RODO** (co omówiono powyżej). W innych przypadkach ich państwo członkowskie może przyjąć określone przepisy lub zasady prawne, by „dodatkowo uregulować" sprawy pozostawione państwu członkowskiemu na mocy RODO albo by wyjaśnić, jakie możliwości zastosowano itp. W jeszcze innych przypadkach państwo członkowskie może objaśnić stosowanie na poziomie krajowym pewnych „klauzul precyzujących" w ogóle, jeżeli jeszcze tego nie uczyniono.

Inspektorzy ochrony danych nie mogą oczywiście sami korygować żadnych braków ani kwestii w tym zakresie. Jednak w ramach swoich własnych sieci inspektorów ochrony danych oraz w swoich interakcjach z krajowymi organami ochrony danych[234] mogą **oznaczyć takie kwestie i zachęcać do podjęcia odpowiednich działań.** Powinny także - najlepiej wspólnie z innymi inspektorami ochrony danych pracującymi w podobnych organizacjach - **zaalarmować wyższe szczeble swojej własnej organizacji** (w sektorze publicznym na przykład - odpowiedniego ministra w rządzie) o zauważonych nieprawidłowościach. W takich sytuacjach inspektorzy ochrony danych muszą opracować strategicznie skuteczne rozwiązania.

2.3 Przegląd RODO

Poniżej przedstawiono szeroki przegląd RODO rozdział po rozdziale i sekcja po sekcji.

* Mamy nadzieję, że dla celów przyszłego poszerzonego, drugiego wydania naszego Podręcznika będzie można opracować krótki komentarz na temat wszystkich postanowień RODO artykuł po artykule. Przegląd taki koncentrowałby się na konkretnym, praktycznym stosowaniu odpowiednich przepisów. W międzyczasie zaleca się, by inspektorzy ochrony danych zapoznali się z jednym z podstawowych komentarzy akademickich, które są publikowane w kilku językach, a także oczywiście jako oficjalnymi wskazówkami wydawanymi przez krajowe organy ochrony danych, Europejską Radę Ochrony Danych (EROD) oraz sądy krajowe i europejskie.

OGÓLNE ROZPORZĄDZENIE O OCHRONIE DANYCH Z 2018 ROKU:
Rozdział I: **Postanowienia ogólne (art. 1 - 4):** - Przedmiot i cele rozporządzenia; - Materialny zakres stosowania; - Terytorialny zakres stosowania; - Definicje.
Rozdział II: **Zasady (art. 5 – 11):** - Zasady dotyczące przetwarzania danych osobowych; - Zgodność przetwarzania z prawem [podstawy prawne]; - Warunki wyrażenia zgody; - Warunki wyrażenia zgody przez dziecko w przypadku usług społeczeństwa informacyjnego; - Przetwarzanie szczególnych kategorii danych osobowych [wrażliwych danych]; - Przetwarzanie danych osobowych dotyczących wyroków skazujących i naruszeń prawa; - Przetwarzanie niewymagające identyfikacji.
Rozdział III: **Prawa osoby, której dane dotyczą**

[234] Zob. „Extranet" **francuskiego** inspektora ochrony danych, który mógłby być przydatny w takim kontekście. Patrz: przypis 456 poniżej.

Sekcja 1 (art. 12):

Przejrzystość oraz tryb korzystania z praw

- Przejrzyste informowanie i przejrzysta komunikacja oraz tryb wykonywania praw przez osobę, której dane dotyczą.

Sekcja 2 (art. 13 - 15):

Informacje i dostęp do danych osobowych:

- Informacje podawane w przypadku zbierania danych od osoby, której dane dotyczą;
- Informacje podawane w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą;
- Prawo dostępu przysługujące osobie, której dane dotyczą.

Sekcja 3 (art. 16 - 20):

Sprostowanie i usuwanie danych:

- Prawo do sprostowania danych
- Prawo do usunięcia danych (prawo do ograniczenia przetwarzania, prawo do bycia zapomnianym)
- Prawo do ograniczenia przetwarzania [„blokowania”]
- Obowiązek powiadomienia o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania
- Prawo do przenoszenia danych

Sekcja 4 (art. 21 - 22):

Prawo do sprzeciwu oraz zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach:

- Prawo do sprzeciwu;
- Zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach, w tym profilowanie.

Sekcja 5 (art. 23):

Ograniczenia

ROZDZIAŁ IV:

Administrator i podmiot przetwarzający

Sekcja 1 (art. 24 - 31):

Obowiązki ogólne:

- Obowiązki administratora;
- Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych;
- Współadministratorzy;
- Przedstawiciele administratorów lub podmiotów przetwarzających niemających jednostki organizacyjnej w Unii;
- Podmiot przetwarzający;
- Przetwarzanie z upoważnienia administratora lub podmiotu przetwarzającego;
- Rejestrowanie czynności przetwarzania;
- Współpraca z organem nadzorczym.

Sekcja 2 (art. 32 - 34):

Bezpieczeństwo danych osobowych:

- Bezpieczeństwo przetwarzania;
- Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu;
- Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych.

Sekcja 3 (art. 35 - 36):

Ocena skutków dla ochrony danych i uprzednie konsultacje:

- Ocena skutków dla ochrony danych;
- Uprzednie konsultacje.

Sekcja 4 (art. 37 - 39):

Inspektor ochrony danych:

- Wyznaczenie inspektora ochrony danych;
- Status inspektora ochrony danych;
- Zadania inspektora ochrony danych.

Sekcja 5 (art. 40 - 43):

Kodeksy postępowania i certyfikacja:

- Kodeksy postępowania;
- Monitorowanie zatwierdzonych kodeksów postępowania;
- Certyfikacja;
- Podmiot certyfikujący.

ROZDZIAŁ V (art. 44 - 50):

Przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych:

- Ogólne zasady przekazywania;
- Przekazywanie na podstawie decyzji stwierdzającej odpowiedni stopień ochrony;
- Przekazywanie z zastrzeżeniem odpowiednich zabezpieczeń;
- Wiążące reguły korporacyjne;
- Przekazywanie lub ujawnianie niedozwolone na mocy prawa Unii;
- Wyjątki w szczególnych sytuacjach;
- Międzynarodowa współpraca na rzecz ochrony danych osobowych.

ROZDZIAŁ VI:

Niezależne organy nadzorcze:

Sekcja 1 (art. 51 - 54):

Niezależny status:

- Organ nadzorczy;
- Niezależność;
- Ogólne warunki dotyczące członków organu nadzorczego;
- Zasady ustanawiania organu nadzorczego.

Sekcja 2 (art. 55 - 59):

Właściwość, zadania i uprawnienia:

- Właściwość;
- Właściwość wiodącego organu nadzorczego;
- Zadania;
- Uprawnienia;
- Sprawozdanie z działalności.

ROZDZIAŁ VII:

Współpraca i spójność

Sekcja 1 (art. 60 - 62):

Współpraca:

- Współpraca miedzy wiodącym organem nadzorczym a innymi organami nadzorczymi, których sprawa dotyczy;
- Wzajemna pomoc;
- Wspólne operacje organów nadzorczych.

Sekcja 2 (art. 63 - 67):

Spójność:

- Mechanizm spójności;
- Opinia Europejskiej Rady Ochrony Danych;
- Rozstrzyganie sporów przez Europejską Radę Ochrony Danych;
- Tryb pilny;
- Wymiana informacji.

Sekcja 3 (art. 68 - 76):

Europejska rada ochrony danych:

- Europejska Rada Ochrony Danych;
- Niezależność;
- Zadania Europejskiej Rady Ochrony Danych;
- Sprawozdania;
- Procedura;
- Przewodniczący;
- Zadania przewodniczącego;
- Sekretariat;
- Poufność.

ROZDZIAŁ VIII (art. 77 - 84):

Środki ochrony prawnej, odpowiedzialność i sankcje:

- Prawo do wniesienia skargi do organu nadzorczego;
- Prawo do skutecznego środka ochrony prawnej przed sądem przeciwko organowi nadzorczemu;
- Prawo do skutecznego środka ochrony prawnej przed sądem przeciwko administratorowi lub podmiotowi przetwarzającemu;
- Reprezentowanie osób, których dane dotyczą;
- Zawieszenie postępowania;
- Prawo do odszkodowania i odpowiedzialność;
- Ogólne warunki nakładania administracyjnych kar pieniężnych;
- Sankcje.

ROZDZIAŁ IX (art. 85 - 91):

Przepisy dotyczące szczególnych sytuacji związanych z przetwarzaniem:

- Przetwarzanie a wolność wypowiedzi i informacji;
- Przetwarzanie a publiczny dostęp do dokumentów urzędowych;
- Przetwarzanie krajowego numeru identyfikacyjnego;
- Przetwarzanie w kontekście zatrudnienia;

- Zabezpieczenia i wyjątki mające zastosowanie do przetwarzania do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych; - Obowiązek zachowania tajemnicy; - Istniejące zasady ochrony danych obowiązujące kościoły i związki wyznaniowe.
ROZDZIAŁ X (art. 92 - 93): **Akty delegowane i akty wykonawcze:** - Wykonywanie przekazanych uprawnień; - Procedura komitetowa.
ROZDZIAŁ XI (art. 94 - 99): **Przepisy końcowe:** - Uchylenie dyrektywy 95/46/WE; - Stosunek do dyrektywy 2002/58/WE; - Stosunek do uprzednio zawartych umów; - Sprawozdania Komisji; - Przegląd innych aktów prawnych Unii dotyczących ochrony danych; - Wejście w życie i stosowanie.

2.4 Zasada rozliczalności[235]

2.4.1 Nowe zadanie wykazania zgodności

Chociaż może wydawać się, że to nic nowego (oraz można powiedzieć, że zostało to zainspirowane amerykańskim podejściem prawnym, które z kolei znalazło odzwierciedlenie w Wytycznych OECD z 1980 roku), faktycznie jedną z podstawowych funkcji nowego unijnego Ogólnego rozporządzenia o ochronie danych (RODO) - a może nawet jego główną funkcją - jest to, że kładzie ono poważny nacisk na fakt, że:

> **„Administrator jest odpowiedzialny za przestrzeganie przepisów oraz *musi być w stanie wykazać przestrzeganie* [zasad dotyczących przetwarzania danych] („rozliczalność")"** (art. 5(2)).

Włoski organ ochrony danych, *Garante della Privacy*, ujmuje to następująco[236]:

> Zagwarantowanie *rozliczalności* podmiotu oznacza przydzielenie takiemu podmiotowi działań i decyzji i **oczekiwanie, że będzie on za takie działania i decyzje odpowiadał.** W związku z powyższym rozliczalność to **stan bycia odpowiedzialnym** za przydzielone działania i decyzje.

Nowość polega na wprowadzeniu organu ds. przetwarzania, który jest odpowiedzialny za zapewnienie zgodności, co miało już oczywiście miejsce zgodnie z Dyrektywą o ochronie danych z 1995 roku (chociaż dyrektywa ta nie stosowała zwrotu „rozliczalność"). Nowość polega raczej na położeniu nacisku na konieczność „**wykazania**" tej zgodności przez administratora (a w niektórych przypadkach przez przetwarzającego) - Rozporządzenie stosuje ten zwrot co najmniej 33 razy.

Z kolei Dyrektywa z 1995 roku nigdzie wyraźnie nie wymagała od administratora lub przetwarzającego wykazania zgodności z czymkolwiek (chyba że oczywiście zostali do tego zobowiązani przez organ ochrony danych lub sąd). A konkretniej, różne systemy „zawiadamiania" i „rejestracji" ustanowione zgodnie z Dyrektywą w co najmniej kilku krajach nie przyczyniały się zbytnio do wykazania takiej zgodności[237], podczas gdy w innych krajach ich sukces polegał jedynie na tym, że były bardzo szczegółowe i prezentowane w taki sposób, by pokierować administratorów do stosowania wszystkich wymogów prawnych w stosunku do nowej operacji przetwarzania danych, przy czym odpowiedni organ ochrony danych miał alarmować administratora oraz sugerować modyfikacje lub udzielać porad wtedy, gdy było to konieczne lub wymagane. W kontekście gwałtownej ekspansji i ewolucji praktyk przetwarzania danych, a w krajach (takich jak państwa członkowskie UE), w których istnieje już znacząca

[235] Punkt ten oparty jest na oraz częściowo powtarza lub podsumowuje - Douwe Korff, The Practical Implications of the new EU General Data Protection Regulation for EU- and non-EU Companies, sierpień 2016 r. opracowanie zaprezentowane w trakcie CMS Cameron McKenna LLP, Londyn, w lutym 2017 r. http://ssrn.com/abstract=3165515.

[236] Luigi Carrozzi, prezentacja w trakcie pierwszej sesji szkoleniowej „T4DATA", czerwiec 2018 r. slajd „*Asset inventory and the Accountability Principle*" (podkreślenie oryginalne).

[237] Patrz motyw 89 RODO.

wiedza na temat stosowania zasad ochrony danych oraz doświadczenie w tym zakresie, także w kontekście promowania „odpowiedzialności społecznej" organizacji, konieczne było nowe podejście kładące nacisk na podstawową odpowiedzialność i rozliczalność podmiotów przetwarzających dane osobowe (administratora lub przetwarzającego). To oznacza właśnie zasada rozliczalności i obowiązek wykazania.

Jak wspomniano w pkt. 2.3, Rozporządzenie wymaga wyznaczenia Inspektorów ochrony danych dla wszystkich administratorów w sektorze publicznym oraz wielu w sektorze prywatnym, jako głównej instytucji odpowiedzialnej za wdrożenie zasady rozliczalności w praktyce.

Jak wyjaśnia przytoczona powyżej, przewidziana w art. 5(2), zasada rozliczalności, obowiązek wykazania przestrzegania dotyczy po pierwsze wszystkich podstawowych zasad, na których bazuje Rozporządzenie, a które określono w art. 5(1), tj. zasady zgodności z prawem, rzetelności i przejrzystości, wąskiego i wyraźnego określenia i ograniczenia celu, minimalizacji danych (z uwzględnieniem adekwatności, stosowności i niezbędności danych), prawidłowości (z uwzględnieniem aktualności), ograniczenia przechowywania (zatrzymywania), integralności i poufności oraz bezpieczeństwa. Oczywiście dotyczy to także (a fortiori) szczególnie bezwzględnego zastosowania tych zasad do przetwarzania szczególnych kategorii danych (tak zwanych wrażliwych danych - art. 9) lub danych, które z dużym prawdopodobieństwem mogą powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych (i które w związku z tym wymagają specjalnej oceny skutków dla ochrony danych - art. 35).

Poza tym Rozporządzenie wyraźnie lub w domniemany sposób nakłada obowiązek wykazania przestrzegania w kilku bardziej szczególnych kontekstach, w tym w odniesieniu do:

- uzyskania zgody (gdy jest wymagana) (patrz: art. 7(1));
- odmowy podjęcia działań w związku z żądaniem dostępu do danych lub sprostowania danych przez osobę, której dane dotyczą (patrz: art. 11(2) i 12(5));
- Niestosowania się do wyrażonego przez osobę, której dane dotyczą, sprzeciwu wobec przetwarzania (patrz: art. 21(1));
- zapewnienia „wystarczających gwarancji" dotyczących właściwości oraz podjęcia „odpowiednich środków technicznych i organizacyjnych" w celu zapewnienia bezpieczeństwa przetwarzania danych przez przetwarzających i podwykonawców przetwarzania (zob. art. 28 i 32);
- Zapewnienia „odpowiednich zabezpieczeń" dla przekazu danych osobowych do krajów trzecich niegwarantujących odpowiedniej ochrony danych (art. 46);
- itp.

Z obowiązkiem wykazania przestrzegania blisko związane są nowe ogólne i szczegółowe obowiązki nałożone przez RODO pod względem:

- **tworzenia rejestru operacji przetwarzania danych osobowych;**
- przeprowadzania **ogólnego przeglądu takich operacji;**
- **oceniania ryzyka** tego typu operacji dla praw i wolności osób fizycznych;
- przeprowadzania dogłębnej **oceny oddziaływania na ochronę danych** w odniesieniu do operacji, które uznano za mogące z dużym prawdopodobieństwem powodować ***„wysokie ryzyko";***
- wykorzystaniem ochrony **danych w fazie projektowania i domyślnej ochrony danych** w odniesieniu do wszystkich operacji przetwarzania danych osobowych;
- wymogów dotyczących **zgłaszania naruszenia danych.**

Przyjrzymy się bardziej szczegółowo tym wszystkim elementom w całości, ze szczególnym uwzględnieniem roli inspektorów ochrony danych, w trzeciej części Podręcznika. W tym miejscu wystarczy krótkie wspomnienie i nawiązanie do wyżej wspomnianej części.

Tak więc, po pierwsze Rozporządzenie nakłada istotny **ogólny wymóg prowadzenia szczegółowych rejestrów wszystkich czynności przetwarzania danych osobowych przez administratora**, określając konkretne dane każdej czynności (art. 30). Wpisy takie należy prowadzić w formie **rejestru czynności przetwarzania danych osobowych** i muszą one wykazywać, że oraz w jaki sposób powyższe ogólne i szczegółowe obowiązki są przestrzegane (zob. motyw 82). Patrz: dyskusja w zadaniu 1 w części trzeciej Podręcznika.

Po drugie, Rozporządzenie wymaga od administratorów, by przy pomocy swoich inspektorów ochrony danych dokonywali **przeglądu swoich czynności** oraz tam, gdzie to konieczne, uzgadniali je z postanowieniami Rozporządzenia, a także by odnotowali taki przegląd i wszystkie działania podjęte naprawcze w wyżej wspomnianym rejestrze. Patrz: dyskusja w Zadaniu 2 w części trzeciej Podręcznika.

Po trzecie, Rozporządzenie nakłada na administratorów ogólny obowiązek „uwzględnienia" **ryzyka** wynikającego z proponowanych przez siebie operacji przetwarzania **w powiązaniu z** obowiązkiem wdrożenia ***„odpowiednich środków technicznych i organizacyjnych*"**, by zwalczyć takie ryzyko oraz obowiązkiem *„wykazania, że przetwarzanie odbywa się zgodnie z tym Rozporządzeniem*", tj. że ryzyko zostało faktycznie ocenione oraz że środki podjęte w świetle takiej oceny były odpowiednie dla tego typu ryzyka (art. 24(1)), zob. także art. 32). Sprawy te należy również właściwie odnotować. Patrz: dyskusja w zadaniu 3 w części trzeciej Podręcznika.

Po czwarte, jeżeli ogólny wymóg oceny ryzyka (wspomniany powyżej) pokazuje, że istnieje prawdopodobieństwo **wysokiego ryzyka** dla praw i wolności osób fizycznych, administrator jest zobowiązany przed przetworzeniem przeprowadzić **ocenę skutków dla ochrony danych,** obejmującą wpływ planowanych czynności przetwarzania na ochronę danych osobowych, oraz taką oceną udokumentować. Dokument oceny musi zawierać: systematyczny opis planowanych operacji przetwarzania i celów przetwarzania; ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów; ocenę wynikającego z przetwarzania ryzyka naruszenia praw lub wolności osób, których dane dotyczą; a także opis środków planowanych w celu zaradzenia ryzyku, w tym *zabezpieczeń oraz środków i mechanizmów bezpieczeństwa mających zapewnić ochronę danych osobowych i wykazać przestrzeganie niniejszego Rozporządzenia, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy* (art. 35). Patrz: dyskusja w Zadaniu 4 w części trzeciej Podręcznika.

Po piąte, Rozporządzenie nakłada na administratorów ogólny obowiązek stosowania ochrony danych „**w fazie projektowania oraz domyślnej ochrony danych**" zarówno w trakcie przygotowania, jak i wykonywania wszystkich swoich operacji przetwarzania (art. 25), zaś administrator musi być w stanie wykazać, że zostało to uczynione. W tym względzie Rozporządzenie wspomina, że jako element wykazania przestrzegania można stosować certyfikację (pieczęcie w zakresie ochrony danych) (art. 25(3), omówiony poniżej). Patrz: dyskusja w Zadaniu 9 w części trzeciej Podręcznika.

Po szóste, administratorzy muszą **udokumentować wszystkie szczegóły** każdego naruszenia danych osobowych (naruszenia bezpieczeństwa danych osobowych) oraz podjęte środki naprawcze oraz **zgłosić** je odpowiedniemu (właściwemu) organowi nadzorczemu w ciągu 72 godzin (art. 33). Osoby, których dane dotyczą, na które naruszenie ma wpływ, należy poinformować, jednak wyłącznie wtedy gdy „naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia [ich] praw lub wolności", z uwzględnieniem mniejszej liczby szczegółów (art. 34). Patrz: dyskusja w Zadaniu 6 w części trzeciej Podręcznika.

Rozporządzenie przewiduje także kilka bardziej szczegółowych obowiązków dotyczących rejestracji. Jeżeli co najmniej dwóch administratorów wspólnie ustala cele i sposoby przetwarzania, są oni współadministratorami. W związku z tym „w przejrzysty sposób określają odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z niniejszego Rozporządzenia" w formie **„uzgodnienia",** a takie „uzgodnienie" „należycie odzwierciedla odpowiednie zakresy obowiązków współadministratorów oraz relacje pomiędzy nimi a podmiotami, których dane dotyczą". W praktyce, ponieważ administratorzy mogą zostać poproszeni przez organy nadzorcze o potwierdzenie przestrzegania tych obowiązków, uzgodnienie musi mieć **formę pisemną lub** należy je sporządzić w **porównywalnym wiarygodnym formacie elektronicznym** (art. 26).

I oczywiście różne postanowienia Rozporządzenia wymagające od administratorów, współadministratorów, podmiotów przetwarzających i podwykonawców przetwarzania określenia ustaleń zawartych pomiędzy nimi i/lub dotyczących przekazywania danych udokumentowania w **umowach lub podobnych prawnie wiążących instrumentach.**

2.4.2 Sposoby wykazywania zgodności

Ogólny obowiązek prowadzenia szczegółowych **rejestrów i wpisów** oraz bardziej szczegółowe obowiązki prowadzenia rejestru nałożone w odniesieniu do współadministratorów, naruszenia danych i oceny skutków dla ochrony danych stanowią główne, ogólne i przewidziane w niniejszym Rozporządzeniu sposoby wykazywania przestrzegania przepisów.

Rejestry takie powinny odzwierciedlać ogólną kulturę i mechanizm promowania ochrony danych, odzwierciedlony w takich **praktykach,** jak:

- sporządzanie i formalne przyjmowanie wewnętrznych polityk ochrony danych (oraz podejmowanie powiązanych działań, takich jak szkolenia);
- uwzględnianie zasady ochrony danych w fazie projektowania i zasady domyślnej ochrony danych we wszystkich wykonywanych przez administratora operacjach przetwarzania danych, produktach i usługach, na każdym kroku, od koncepcji po ich faktyczne funkcjonowanie;
- minimalizację wykorzystania i zatrzymywania danych osobowych i w szczególności wykorzystywania danych, które w dalszym ciągu pozwalają na identyfikację osoby, której dane dotyczą (stosowanie pseudonimizacji, anonimizacji możliwych do zidentyfikowania danych tam, gdzie to możliwe);
- zapewnienie najpełniejszej przejrzystości działań administratora dla osób, których dane dotyczą, oraz opinii publicznej w formie papierowej, internetowej oraz w jasnych i znacznie bardziej zróżnicowanych oświadczeniach o ochronie danych/prywatności na stronach internetowych (np. wyraźnie rozróżniających - bezpośrednio na stronie, na której dane osobowe są gromadzone, obowiązkowe i opcjonalne pola/cele i dane, a także umożliwiających użytkownikom strony znacznie większy uzasadniony wybór poprzez kliknięcie na pole), a także poprzez wdrażanie efektywnych i skutecznych sposobów rozpatrywania żądań osób, których dane dotyczą, o przekazanie ogólnych lub szczegółowych informacji; oraz
- zapewnienie, że administrator sam może w dalszym ciągu skutecznie monitorować działania, w szczególności w odniesieniu do bezpieczeństwa (poprzez protokoły dostępu i zmian itp.); oraz że jest w stanie poprawić bezpieczeństwo, gdy jest to konieczne (np. wydając „łaty").

  (Zob. motyw 78)

W części trzeciej przyjrzymy się tym sprawom dokładniej oraz przedstawimy konkretne przykłady i praktyczne wskazówki dotyczące wykonywania wyżej wspomnianych zadań.

Ponadto we wcześniejszym motywie (77) wymieniono różne **specjalne sposoby** wykazywania przestrzegania, tj.

- działanie zgodnie z zatwierdzonym kodeksem postępowania;
- działanie zgodnie z zatwierdzoną certyfikacją ochrony danych;
- działanie zgodnie z wytycznymi Europejskiej Rada Ochrony Danych;

  oraz oczywiście:

- działanie zgodnie z sugestiami inspektora ochrony danych.

Do tego można dodać, w szczególności w odniesieniu do przekazu transgranicznego oraz ujawniania danych osobowych:

- Wiążące reguły korporacyjne;
- umowy administracyjne („uzgodnienia") pomiędzy organami publicznymi oraz
- standardowe lub indywidualnie zatwierdzane umowy o przekazie danych.

W odniesieniu do naruszenia danych zgłoszenie (oraz podane w nim szczegóły) można także traktować jako specjalny sposób wykazania przestrzegania odpowiednich wymogów.

Należy jednak podkreślić, że w odniesieniu do wszystkich wymienionych sposobów, choć mogą one stanowić „elementy" w ogólnym procesie wykazywania przestrzegania prawa i „specjalne sposoby" do osiągnięcia tego celu, nie muszą one koniecznie stanowić prawnego dowodu przestrzegania prawa.

2.4.3 Wartość dowodowa różnych sposobów wykazywania zgodności

W większości przypadków przestrzeganie któregokolwiek z wyżej wymienionych sposób zapewnienia zgodności stanowi element wykazywania zgodności, tj. stwarza domniemanie zgodności, jednak jest to domniemanie o wzruszalnym charakterze. Jeżeli organ ochrony danych miałby dokładniej zbadać sprawę, mógłby ustalić, że - bez względu na stosowanie takich wskazówek, kodeksów, certyfikacji, umów, kontraktów lub zasad - w konkretnym przypadku Rozporządzenie nie było jednak przestrzegane (chociaż każdy podjęta w dobrej wierze próba przestrzegania miałaby oczywiście istotny wpływ na poziom kar pieniężnych, jeżeli kary takie faktycznie zostałyby nałożone – zob. art. 83).

2.5 Inspektor Ochrony Danych (IOD)

2.5.1 Doświadczenie

Koncepcja inspektorów ochrony danych wyznaczanych przez administratora w sektorze publicznym i prywatnym pochodzi z niemieckiego prawa o ochronie danych, które długo ich wymagało[238]. Nawet w krajach, które zgodnie z Dyrektywą o ochronie danych z 1995 roku, nie musiały wyznaczać inspektorów ochrony danych na mocy prawa (takich jak Austria, która pod innymi względami często idzie za przykładem Niemiec) lub w których pozostawiono im możliwość wyboru (jak we Francji), instytucja ta często była szeroko przyjmowana. W kilku krajach działają stowarzyszenia narodowe inspektorów ochrony danych oraz Konfederacja Europejskich Organizacji Ochrony Danych (Confederation of European Data Protection Organisations, CEDPO), która wydała „praktyczne wytyczne dla organizacji" w sprawie „wyboru najlepszego kandydata" jako inspektora ochrony danych[239]. Na poziomie globalnym działa Międzynarodowe Stowarzyszenie Specjalistów ds. Prywatności (International Association of Privacy Professionals, IAPP), z siedzibą w USA , które między innymi oferuje certyfikaty ochrony danych dla „specjalistów ds. prywatności informacji" (chociaż, podobnie jak inne systemy certyfikacji IOD, nie stanowią one certyfikacji zgodności opartej na RODO: zob. sekcja 2.5.3, poniżej, pod nagłówkiem „Formalne szkolenie i certyfikacja [IOD]").

(Patrz lista stowarzyszeń inspektorów ochrony danych na końcu tego podpunktu z linkami do ich stron internetowych).

Dyrektywa o ochronie danych z 1995 roku nie wymagała jeszcze wyznaczenia inspektorów ochrony danych przez podlegających jej postanowieniom administratorów. Uznawała raczej istnienie inspektorów ochrony danych w prawie i praktyce państwa członkowskiego, pozwalając państwom członkowskim na zwolnienie administratorów z obowiązków zgłaszania operacji przetwarzania odpowiedniemu krajowemu organowi ochrony danych, jeżeli prawo państwa członkowskiego wymagało od odpowiedniego administratora wyznaczenia inspektora ochrony danych odpowiedzialnego w szczególności za *„zapewnienie w niezależny sposób wewnętrznego stosowania przepisów prawa krajowego przyjętych na mocy niniejszej dyrektywy oraz za prowadzenie rejestru operacji przetwarzania danych wykonywanych przez administratora danych i zawierających [takie same informacje, jakie należałoby w innym przypadku zgłosić organowi ochrony danych*]" (art. 18(2)).

[238] Niemieckie zwroty to odpowiednio *behördliche*- i *betriebliche Datenschutzbeauftragter*. Krótkie podsumowanie ich roli i funkcji na mocy niemieckiego prawa – zob. np.: https://www.wbs-law.de/eng/practice-areas/internet-law/it-law/data-protection-officer/. Bardziej szczegółowe exposé w języku niemieckim, zob. np.: Däubler/Klebe/Wedde/Weichert, Kompaktkommentar zum BDSG (Krótkie podsumowanie niemieckiego prawa federalnego o ochronie danych), III wydanie (2010), komentarze na temat §4f BDSG, obejmujące 85 notatek na marginesie, str. 187 – 213.

[239] CEDPO, Choosing the best candidate as your Data Protection Officer (DPO) – Practical guidelines for organisations, 30 maja 2016 r. http://businessdocbox.com/Human_Resources/77901620-Choosing-the-best-candidate-as-your-data-protection-officer-dpo-practical-guidelines-for-organisations.html.

Jednak Rozporządzenie UE z 2001 roku określające zasady ochrony danych dla samych instytucji UE (Rozporządzenie (WE) 45/2001)[240] wymaga od każdej instytucji lub organu UE wyznaczenia co najmniej jednego inspektora ochrony danych (art. 24). Zasady dotyczące inspektorów ochrony danych w instytucjach UE, podkreślone w tym Rozporządzeniu, są bardzo podobne do tych w RODO.

Tak zwana Dyrektywa o ochronie danych przez organy ścigania (Dyrektywa 2016/680)[241], przyjęta jednocześnie z RODO, wymaga, by „właściwe organy" podlegające temu instrumentowi także wyznaczyły inspektora ochrony danych, a Wytyczne Grupy Roboczej Art. 29 dotyczące inspektorów ochrony danych (które, jak wspomniano poniżej zawierają główne wytyczne dla inspektorów ochrony danych wyznaczanych zgodnie z RODO) podkreślają, że „chociaż wytyczne te koncentrują się na inspektorach ochrony danych zgodnie z RODO, mają także zastosowanie do inspektorów ochrony danych zgodnie z Dyrektywą 2016/680, w odniesieniu do wszystkich podobnych postanowień"[242].

Wewnętrzni inspektorzy ochrony danych UE współpracują blisko z Europejskim Inspektorem Ochrony Danych (EDPS) oraz stworzyli Sieć Inspektorów Ochrony Danych Instytucji i Organów UE. Jako wsparcie EDPS stworzył stronę internetową „DPO Corner". Po wydaniu w 2005 roku przez EDPS dokumentu przedstawiającego jego stanowisko[243], w 2010 roku Sieć wydała zestaw profesjonalnych standardów dla inspektorów ochrony danych instytucji i organów UE działających na podstawie Rozporządzenia (WE) 45/2001 (Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001)[244]. W 2012 roku EDPS wydał sprawozdanie na temat statusu inspektorów ochrony danych w ramach procesu monitorowania przestrzegania przez instytucje postanowień Rozporządzenia (WE) 45/2001[245]. Sprawozdanie to potwierdza, że funkcja inspektora ochrony danych została dobrze ustanowiona w ramach instytucji i organów UE oraz że z zasady jest zgodna z art. 24 Rozporządzenia, a także zauważa pewne obszary wymagające dalszego monitorowania przez EDPS[246]. Dokumenty te zawierają dość szerokie wskazówki na temat spraw dotyczących mianowania, pozycji i zadań inspektorów ochrony danych.

Niedawno Grupa Robocza Art. 29 przedstawiła wytyczne dotyczące inspektorów ochrony danych w procesie przygotowania do rozpoczęcia stosowania RODO, co ma bezpośrednie powiązanie z niniejszym Podręcznikiem[247]. Europejska Rada Ochrony Danych, która przejęła zadania Grupy Roboczej Art. 29 po wejściu rozpoczęciu stosowania RODO, formalnie zatwierdziła te wytyczne (a także inne dokumenty w sprawach wynikających z RODO, jakie zostały przyjęte przez WP29 przed tym terminem)[248].

W efekcie kilka krajowych organów ochrony danych także wydało wskazówki dotyczące inspektorów ochrony danych, niektóre nawet przed wejściem w życie RODO, promując w nich konkretne usługi inspektorów[249].

---

[240] Pełny tytuł: Rozporządzenie (WE) 45/2001 Parlamentu Europejskiego i Rady z 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, O.J. L 8 z 12.1.2001 r. str. 1ff, https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32001R0045&from=PL

[241] Pełny tytuł: Dyrektywa (UE) 2016/680 Parlamentu Europejskiego i Rady z 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, OJ L 119, 4.5.2016, str. 89ff., http://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32016L0680&from=PL.

[242] Wytyczne Grupy Roboczej Artykułu 29 dotyczące inspektorów ochrony danych, pierwotnie przyjęte 13 grudnia 2016 r. następnie skorygowane i przyjęte 5 kwietnia 2017 r. (WP243 wer. 01), str. 4, przypis 2, http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048. Wytyczne te zwane są dalej „**Wytycznymi Grupy Roboczej Art. 29 dotyczącymi inspektorów ochrony danych".**

[243] EDPS, Position paper on the role of Data Protection Officers in ensuring effective compliance with Regulation (EC) 45/2001, https://edps.europa.eu/sites/edp/files/publication/05-11-28_dpo_paper_en.pdf.

[244] https://edps.europa.eu/sites/edp/files/publication/10-10-14_dpo_standards_en.pdf.

[245] EDPS, Monitoring compliance of EU institutions and bodies with Article 24 of Regulation (EC) 45/2001 – Report on the Status of Data Protection Officers, 17 grudnia 2012 r. https://edps.europa.eu/sites/edp/files/publication/2012-12-17_dpo_status_web_en.pdf.

[246] *Idem*, str. 3.

[247] Zob. przypis 242 powyżej.

[248] EDPB, Endorsement 1/2018, zatwierdzenie między innymi Wytycznych Grupy Roboczej Art. 29 dotyczących inspektorów ochrony danych (wymienione jako VII zatwierdzony dokument), 25 maja 2018 r. https://edpb.europa.eu/sites/edpb/files/files/news/endorsement_of_wp29_documents_en_0.pdf.

[249] Zob. *Guide de Correspondant Informatique et Libertés (CIL)* (*Guide Pratique Correspondant*), wydane przez francuski organ ochrony danych - CNIL, w 2011 r. https://www.cnil.fr/sites/default/files/typo/document/CNIL_Guide_correspondants.pdf. We

Ta część Podręcznika oparta jest na wytycznych Grupy Roboczej Art. 29 w szczególności, ale nawiązuje także do innych wyżej wspomnianych wytycznych, jako uzupełnienie myśli autora.

Jako główny punkt wprowadzenia do instytucji inspektorów ochrony danych, pod względem RODO, należy wspomnieć, że jest to zasadnicza nowa instytucja, którą należy postrzegać jako istotny środek mający nadać praktyczny skutek wyżej omówionej zasadzie „rozliczalności" (obowiązkowi wykazania przestrzegania) - gdy inspektor ochrony danych został wyznaczony i rzetelnie wykonuje swoje zadania (co omówiono w części 3 Podręcznika), powinno to prowadzić do lepszego, bardziej kompleksowego i poważnego przestrzegania RODO, niż uzyskano by to poprzez głównie nadzór zewnętrzny ze strony organów ochrony danych w związku z Dyrektywą o ochronie danych z 1995 roku. Obecnie, zgodnie z RODO, organy ochrony danych posiadają zarówno bezpośredni, znający się na rzeczy punkt kontaktowy w ramach organizacji wszystkich odpowiednich administratorów, jak i sojusznika w organizacji administratora. Nie dziwi więc, że teraz, gdy RODO ma zastosowanie, kilka organów ochrony danych uczyniło jednym ze swoich priorytetów sprawdzenie, czy organizacje, które muszą wyznaczyć inspektora ochrony danych (co zostanie omówione w pkt. 2.3.2) faktycznie to uczyniły[250].

Włoszech krajowy organ ochrony danych, *Garante dellal Privacy*, wydał zestaw Często zadawanych pytań (FAQs) dotyczących inspektorów ochrony danych, który jest dostępny na stronie: https://www.garanteprivacy.it/garante/doc.jsp?ID=8036793 (często zadawane pytania dla inspektorów ochrony danych w sektorze prywatnym); https://www.garanteprivacy.it/garante/doc.jsp?ID=7322110 (często zadawane pytania dla inspektorów ochrony danych w sektore publicznym). W **Polsce** krajowy organ ochrony danych - *Urząd Ochrony Danych Osobowych* (UODO) - udziela ważnych wskazówek i rekomendacji dotyczących stosowania RODO na swojej stronie internetowej w części dedykowanej specjalnie inspektorom ochrony danych: https://uodo.gov.pl/p/najwazniejsze-tematy/inspektor-ochrony-danych. Przed wejściem w życie RODO, polski organ utrzymywał stronę internetową ABI, która zwana była *Administratorzy Bezpieczeństwa Informacji.* Strona ta zawierała informacje przydatne także w przygotowaniu przyszłych inspektorów ochrony danych do wykonywania swojej funkcji. Patrz: https://abi.giodo.gov.pl/. Poprzez ten serwis przyszli inspektorzy ochrony danych mogli przekazywać swoje pytania i sugestie dotyczące stosowania i interpretacji przepisów prawnych o ochronie danych osobowych. W **Zjednoczonym Królestwie** krajowy organ ochrony danych, *Information Commissioner* (zazwyczaj zwany ICO, tj. Information Commissioner`s Office), przedstawił wytyczne na swojej stronie internetowej, które zasadniczo odzwierciedlają wytyczne Grupy Roboczej Art. 29 (i zawierają do nich odwołania), zob. https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/.

[250] Na przykład **szwedzki** organ ochrony danych ogłosił, że będzie przyglądać się, czy organizacje w sektorze bankowym, opieki zdrowotnej i ubezpieczeń wyznaczyły inspektorów ochrony danych. Zob. link do strony: https://www.datainspektionen.se/nyheter/datainspektionen-inleder-forsta-granskningarna-enligt-gdpr/. **Holenderski** organ ochrony danych podobnie podkreśla w swoim planie na lata 2018-2019, że *w szczególności w odniesieniu do organów publicznych* będzie sprawdzać *„przestrzeganie obowiązku prowadzenia rejestru czynności przetwarzania, obowiązku wyznaczenia inspektora ochrony danych oraz sposobu, w jaki organizacja go umiejscawia oraz umożliwia mu wykonywanie zadań zgodnie z RODO",* zob. link do strony internetowej: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/toezichtkader_autoriteit_persoonsgegevens_2018-2019.pdf (str. 7, w punkt „*Overheid*" (organ publiczny) (nasze tłumaczenie).

MIĘDZYNARODOWE I KRAJOWE STOWARZYSZENIA INSPEKTORÓW OCHRONY DANYCH:

Międzynarodowe stowarzyszenia:
Globalne:
International Association of Privacy Professionals (IAPP):
https://iapp.org/certify/cipp/

Europejskie:
Network of Data Protection Officers of the EU Institutions and Bodies:
https://edps.europa.eu/data-protection/eu-institutions-dpo_en

Confederation of European Data Protection Organisations, CEDPO
http://www.cedpo.eu/

Krajowe stowarzyszenia:
(Te oznaczone * są członkami CEDPO)

Francja:
Association Française des Correspondants à la Protection des Données à Caractère Personnel, AFCDP:*
https://www.afcdp.net/

Irlandia:
Association of Data Protection Officers, ADPO*:
https://www.dpo.ie/

Włochy:
Associazone Data Protection Officer, ASSO DPO*:
http://www.assodpo.it/en/home_en/

Holandia:
Nederlands Genootschap voor Functionarissen Gegevensbescherming, NGFG*:
https://www.ngfg.nl/

Polska:
Stowarzyszenie Administratorów Bezpieczeństwa Informacji, SABI*:
http://www.sabi.org.pl/

Hiszpania:
Asociación Profesional Española de Privacidad, APEP*:
http://www.apep.es/

Zjednoczone Królestwo:
National Association of Data Protection & Freedom of Information Officers, NADPO:
https://nadpo.co.uk/

Niemieccy i **austriaccy** członkowie CEDPO, odpowiednio *Gesellschaft für Datenschutz und Datensicherheit e.V.*, DGG* (utworzony w 1977) i *Arge Daten**, posiadają szerszy zakres członkostwa niż inspektorzy ochrony danych, ale są członkami CEDPO:
https://www.gdd.de/ueber-uns
http://www.argedaten.at/php/cms_monitor.php?q=PUB-TEXT-ARGEDATEN&s=15904tpb

2.5.2 Zadanie wyznaczenia inspektora ochrony danych dla organów publicznych[251]

[251] Niniejszy Podręcznik nie omawia zadania wyznaczania inspektora ochrony danych dla przedsiębiorstw „prywatnych" (komercyjnych), jeżeli nie realizują one omówionych w tekście „zadań publicznych" lub nie „wykonują uprawnień publicznych". Wystarczy zauważyć, że dla takich podmiotów Rozporządzenie z zasady wymaga wyznaczenia inspektora ochrony danych jedynie w następujących przypadkach:

- 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; lub
- główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 [tj. tak zwanych „wrażliwych danych"], oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10.
  (art. 37(1)(b) i (c) RODO).

Warunki te omówiono szczegółowo w Wytycznych Grupy Roboczej Art. 29 w sprawie inspektorów ochrony danych. Tutaj wystarczy zauważyć, że w praktyce większość przedsiębiorstw dowolnego rozmiaru uzna wyznaczenie inspektora ochrony

Inspektora ochrony danych muszą wyznaczyć wszystkie organy lub organy publiczne przetwarzające dane osobowe, podlegające RODO (art. 37(1)(a))[252]. Chociaż z zasady decyzja należy do państw członkowskich, Grupa Robocza Art. 29 właściwie stosuje szerokie spojrzenie na ten wymóg[253]:

„Podmiot lub organ publiczny"

RODO nie definiuje „podmiotu lub organu publicznego". Grupa Robocza Art. 29 uważa, że termin ten należy ustalić w prawie krajowym. W związku z tym podmioty i organy publiczne obejmują krajowe, regionalne i lokalne władze, przy czym zgodnie z odpowiednim prawem krajowym koncepcja ta z reguły uwzględnia także szereg innych podmiotów prawa publicznego[254]. W takich przypadkach wyznaczenie inspektora ochrony danych jest obowiązkowe.

Jednak obowiązek wyznaczenia inspektora ochrony danych w rzeczywistości wykracza poza tą czysto formalną kategorię.

Podmioty sektora prywatnego, które wykonują „zadania w interesie publicznym" lub „sprawują władzę publiczną"

Grupa Robocza Art. 29 podkreśla - w nawiązaniu do szczególnej podstawy prawnej przetwarzania przewidzianej w art. 6(1)(e) RODO, że (bez względu na ograniczenia dotyczące obowiązku wyznaczenia inspektora ochrony danych dla podmiotów sektora prywatnego) [255] inspektor ochrony danych powinien zostać także wyznaczony przez administratorów w sektorze prywatnym, którzy wykonują „zadania ... w interesie publicznym" lub którzy „sprawują władzę publiczną", nawet jeżeli nie są formalnie „organami publicznymi" w rozumieniu prawa krajowego, ponieważ w ramach takich czynności ich rola będzie podobna do roli organów publicznych[256]:

> Zadanie publiczne może być wykonywane, a władza publiczna może być sprawowana nie tylko przez podmioty lub organy publiczne, ale także przez inne osoby fizyczne lub prawne działające na mocy prawa publicznego lub prywatnego w takich sektorach jak - zgodnie z krajowymi przepisami każdego państwa członkowskiego - usługi transportu publicznego, dostawy wody i energii, infrastruktura drogowa, publiczne usługi radiowo-telewizyjne, budownictwo publiczne lub organy dyscyplinarne zawodów regulowanych.
>
> W takich przypadkach osoby, których dane dotyczą, mogą znaleźć się w bardzo podobnej sytuacji, do tej, w której ich dane są przetwarzane przez podmiot lub organ publiczny. W szczególności dane mogą być przetwarzane w podobnych celach, a jednostki często mają niewielki wybór lub wcale nie mają wyboru co do tego, czy ich dane będą przetwarzane, oraz w jaki sposób, i mogą przez to wymagać dodatkowej ochrony, jaką może zapewnić wyznaczenie inspektora ochrony danych.
>
> **Nawet mimo to, że nie ma obowiązku w takich sytuacjach, Grupa Robocza Art. 29 zaleca - jako dobrą praktykę - by organizacje prywatne wykonujące zadania publiczne lub sprawujące władzę publiczną wyznaczyły inspektora ochrony danych.** Taka działalność inspektora ochrony danych obejmuje wszystkie wykonywane czynności przetwarzania, w tym te niezwiązane z wykonywaniem zadania publicznego lub sprawowaniem oficjalnego obowiązku (np. zarządzanie bazą danych pracowników).

---

danych za przydatne w celu realizacji spoczywającego na nich obowiązku „rozliczalności"/„obowiązku wykazania przestrzegania" (patrz pkt 2.2 powyżej).

[252] Jedyny wyjątek dotyczy „sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości" (art. 37(1)(a) RODO). Jednak, jak podkreśla Grupa Robocza Art. 29 w swoich Wytycznych dotyczących inspektorów ochrony danych (przypis 209 powyżej), nie oznacza to, że nie muszą oni przestrzegać Rozporządzenia, wręcz przeciwnie - powinni go przestrzegać. Także przetwarzanie danych przez sądy w zakresie innym niż sprawowanie wymiaru sprawiedliwości wymaga wyznaczenia inspektora ochrony danych. Niniejszy Podręcznik nie zajmuje się inspektorami ochrony danych dla organów, które przetwarzają dane w całości poza zakresem unijnego prawa, takich jak krajowe agencje bezpieczeństwa.

[253] Wytyczne Grupy Roboczej Art. 29 dotyczące inspektorów ochrony danych, (przypis 242 powyżej), str. 6.

[254] Zob. np.: definicja „organu sektora publicznego" i „podmiotu prawa publicznego" w art. 2(1) i (2) Dyrektywy 2003/98/WE Parlamentu Europejskiego i Rady z 17 listopada 2003 r. w sprawie ponownego wykorzystywania informacji sektora publicznego, OJ L 345, 31.12.2003, str. 90ff. [oryginalny przypis]. Polski tekst dyrektywy dostępny jest na stronie: https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32003L0098&from=PL.

[255] Zob. przypis 251 powyżej.

[256] Wytyczne Grupy Roboczej Art. 29 dotyczące inspektorów ochrony danych, (przypis 242 powyżej) str. 6. Zastosowanie przez Grupę Roboczą Art. 29 zwrotów „zadanie publiczne" i „organ publiczny" jest kwestią jedynie lingwistyczną - w wytycznych zwroty te dotyczą wspomnianych w art. 6(1)(e) RODO „zadań realizowanych w interesie publicznym" oraz „sprawowania władzy publicznej".

Do przykładów wspomnianych przez Grupę Roboczą Art. 29 można dodać prowadzenie więzienia oraz innych państwowych instytucji lub służb (takich jak deportacja nielegalnych imigrantów) przez podmioty prywatne. We wszystkich tych przypadkach prywatne podmioty skutecznie działają jako ramię państwa i w każdym z nich przedsiębiorstwa te powinny wyznaczyć inspektora ochrony danych. Państwa członkowskie mogą ponadto wyjaśnić to w swoim prawie krajowym oraz nałożyć obowiązek wyznaczenia inspektora ochrony danych na konkretnych administratorów lub typy administratorów innych niż formalne podmioty i organy publiczne (patrz: art. 37(4).

PRZYKŁAD:

We **Włoszech** krajowy organ ochrony danych, *Garante*, jest zdania, że wszystkie podmioty, które wcześniej były objęte zakresem stosowania ust. 18 do 22 włoskiego kodeksu ochrony danych, muszą wyznaczyć inspektora ochrony danych. Ust. 18 do 22 Kodeksu określają ogólne zasady mające zastosowanie do przetwarzania danych przez podmioty publiczne, takie jak organy administracji państwowej, organy publiczne o charakterze non-profit na szczeblu krajowym, regionalnym i lokalnym, regiony, władze lokalne, uniwersytety, izby handlowe, ośrodki opieki zdrowotnej, niezależne organy nadzorcze, itp.

Garante utrzymuje również, że za każdym razem, gdy podmiot prywatny pełni funkcje publiczne, np. w oparciu o licencję lub koncesję, zdecydowanie zaleca się wyznaczenie inspektora ochrony danych, mimo że nie jest to obowiązkowe. Dodaje także, w nawiązaniu do Wytycznych Grupy Roboczej Art. 29 dotyczących inspektorów danych, że jeżeli inspektor ochrony danych zostaje wyznaczony dobrowolnie, jeżeli chodzi o kryteria dotyczące wyznaczania, stanowiska i zadań inspektora, mają zastosowanie takie same wymagania i warunki, jak w przypadku inspektora wyznaczonego obowiązkowo.

Inspektorzy ochrony danych dla podmiotów przetwarzających

Jak wskazuje Grupa Robocza Art. 29, artykuł w RODO, który nakłada obowiązek wyznaczenia w pewnych przypadkach inspektora ochrony danych (art. 37), co zostało opisane powyżej dla sektora publicznego, ma zastosowanie zarówno do administratorów, jak i podmiotów przetwarzających[257]. Dodaje również, że[258]:

> W zależności od tego, kto spełnia kryteria dotyczące obowiązkowego wyznaczenia, w niektórych przypadkach tylko administrator lub tylko podmiot przetwarzający, w innych przypadkach zarówno administrator, jak i podmiot przetwarzający są zobowiązani wyznaczyć inspektorów ochrony danych (którzy powinni następnie ze sobą współpracować).
>
> Należy podkreślić, że nawet jeżeli administrator spełnia kryteria obowiązkowego wyznaczenia, jego podmiot przetwarzający niekoniecznie musi być zobowiązany wyznaczyć inspektora ochrony danych. Może to stanowić jednak dobrą praktykę.

Dla sektora publicznego, gdzie wszystkie odpowiednie organy są w każdym przypadku zobowiązane wyznaczyć inspektora ochrony danych (co zostało omówione powyżej), nie wydaje się to być istotnym problemem. Jednak, biorąc pod uwagę ostatni komentarz Grupy Roboczej Art. 29, jeżeli organ publiczny miałby podzlecić pewne czynności przetwarzania podmiotowi prywatnemu (np. księgowość lub badania), zalecane byłoby przynajmniej wybranie podmiotu przetwarzającego, który sam także posiadałyby inspektora ochrony danych, albo zobowiązanie go do jego wyznaczenia.

W zakresie, w jakim współpracujące ze sobą organy publiczne mogą także czasami pełnić funkcję podmiotów przetwarzających dla siebie nawzajem, powinno to znaleźć odzwierciedlenie w pisemnym porozumieniu, o którym mowa w kolejnym punkcie i dodatkowo w części 3, pkt 3.1.

Inspektorzy ochrony danych dla dużych organów publicznych lub grup organów

Wraz z „cyfrową transformacją" dane osobowe są coraz częściej przetwarzane w wysoce złożonych środowiskach i architekturze technicznej, w których różne podmioty współpracują ze sobą i posiadają

[257] Wytyczne Grupy Roboczej Art. 29 dotyczące inspektorów ochrony danych (przypis 242 powyżej), pkt 2.2, *Inspektor ochrony danych podmiotu przetwarzającego*, na str. 9.

[258] *Idem*. Grupa Robocza Art. 29 podaje kilka przykładów zaczerpniętych z sektora prywatnego, które skupiają się na ograniczeniach obowiązku wyznaczania inspektora ochrony danych dla tego sektora. Nie są one więc szczególnie przydane w naszym Podręczniku.

wspólne lub powiązane zadania w odniesieniu do różnych czynności przetwarzania, w tym w odniesieniu do obywateli. Dzieje się tak także w sektorze publicznym, który w rzeczywistości posiada swoje własne zawiłości pod względem zakresu autonomii, jaką różne organy mogą posiadać w szerszych ramach konstytucyjnych lub administracyjno-prawnych. Jak dalej wspomniano w części 3, pkt 3.1, jednym z pierwszych zadań nowo mianowanego inspektora ochrony danych musi być ustalenie kontekstu przetwarzania danych osobowych, za którego nadzorowanie i/lub konsultowanie będzie odpowiadać. Część pracy polegać będzie na precyzyjnym wyjaśnieniu - w odniesieniu do złożonych kontekstów - statusu różnych podmiotów w ramach złożonej struktury oraz zawarciu i odnotowaniu odpowiednich porozumień.

W tym względzie należy zauważyć, że RODO wyraźnie przewiduje (podobnie jak Dyrektywa o ochronie danych z 1995 roku), że „jeżeli cele i sposoby ... przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego" (co zazwyczaj ma miejsce w przypadku organów publicznych), „w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania" (art. 4(7)). W takich przypadkach często ma sens wyznaczenie inspektora ochrony danych dla całego przetwarzania w urzędach podmiotu, który wyznaczono administratorem danych. W rzeczywistości może to wyjaśniać samo prawo ustalające administratora.

Jeżeli nie jest to przewidziane przepisami prawa, kwestię tę może rozstrzygnąć odpowiedni minister rządowy, wysoki urzędnik lub same podmioty publiczne. Powinno to prowadzić do jasnego porozumienia dotyczącego odpowiedniego zakresu odpowiedzialności i kompetencji różnych inspektorów ochrony danych w różnych podmiotach wchodzących w skład złożonej struktury. Obejmuje to także decyzję w sprawie tego, czy wyznaczyć należy jednego czy kilku inspektorów. Porozumienia takie powinny również obejmować powiązania i ustalenia pomiędzy różnymi inspektorami ochrony danych w podmiotach powiązanych operacyjnie.

Niektóre bardzo duże organy publiczne (lub ministrowie rządowi albo wyższego szczebla urzędnicy w takich organach) mogą podjąć decyzję o mianowaniu kilku inspektorów ochrony danych dla każdej z części, pod warunkiem że ich wybór odzwierciedla faktyczny podział uprawnień decyzyjnych pomiędzy poszczególnymi departamentami lub jednostkami dużych organów publicznych. Albo mogą wyznaczyć jednego inspektora dla całego organu, by współpracował z wyznaczonymi osobami w takich częściach całego dużego podmiotu. W tym drugim przypadku z komentarzy Grupy Roboczej Art. 29 wydanych w kontekście wyznaczania inspektorów ochrony danych na podstawie umowy o świadczenie usług (omówionej w kolejnym podpunkcie) wynika, że tak wyznaczone osoby w departamentach lub odrębnych częściach dużej organizacji powinny z jednej strony wypełniać wymagania dotyczące inspektorów ochrony danych, w szczególności nie wchodzić w konflikt interesów, a z drugiej strony powinny uzyskać podobną ochronę jak właściwy inspektor ochrony danych i nie powinny być karane za sprawowanie przypisanych mu funkcji[259].

Z kolei RODO wyraźnie pozwala **grupom (formalnie odrębnych) mniejszych organów publicznych** - takich jak organy lokalne (Fr: *communes*) podjąć decyzję o wspólnym mianowaniu inspektora ochrony danych (lub zleceniu jego wyznaczenia):

> Jeżeli administrator lub podmiot przetwarzający są organem lub podmiotem publicznym, dla kilku takich organów lub podmiotów można wyznaczyć – z uwzględnieniem ich struktury organizacyjnej i wielkości – jednego inspektora ochrony danych. (art. 37(3))

Taki centralny lub wspólny inspektor ochrony danych może być albo urzędnikiem jednego z organów, albo może zostać podjęta decyzja o wspólnym zatrudnieniu zewnętrznego inspektora ochrony danych na podstawie umowy o świadczenie usług (którą omówiono w kolejnym podpunkcie). Jeżeli mianowano jednego centralnego (wewnętrznego lub zewnętrznego) inspektora ochrony danych, każdy z pozostałych (małych) podmiotów powinien w dalszym ciągu wyznaczyć pracownika odpowiedzialnego za kontakty z centralnym (wspólnym) inspektorem i w takim przypadku zastosowanie ma taka sama

[259] Zob. Wytyczne Grupy Roboczej Art. 29 dotyczące inspektorów ochrony danych (przypis 242 powyżej), pkt 2.4, ostatni podpunkt, str. 12.

zasada jak w przypadku większych organów - wyznaczone osoby powinny spełniać wymagania dotyczące inspektora ochrony danych oraz uzyskać podobną ochronę jak właściwy inspektor.

Zewnętrzni inspektorzy ochrony danych

Jak już wspomniano w poprzednim podpunkcie, organy publiczne (i prywatne przedsiębiorstwa) nie muszą tworzyć wewnętrznego stanowiska dla inspektora ochrony danych, tym bardziej pełnoetatowego (chociaż wiele większych organów prawdopodobnie wybierze tą opcję, jeżeli jeszcze tego nie zrobiło). Raczej:

> „Inspektor ochrony danych może być członkiem personelu administratora lub podmiotu przetwarzającego lub wykonywać zadania na podstawie umowy o świadczenie usług" (art. 37(6)).

W Niemczech, skąd pochodzi pomysł ustanawiania inspektorów ochrony danych[260], kancelarie prawne lub inni niezależni eksperci oferują w ten sposób usługi inspektora ochrony danych. Ponadto wydaje się, że „zrzeszenia lub inne podmioty reprezentujące określone kategorie administratorów lub podmiotów przetwarzających" mogą także pełnić funkcje inspektora ochrony danych na rzecz swoich członków i w tym względzie działają w imieniu wszystkich członków (zob. art. 37(4)). Byłoby to przydatne w szczególności dla małych przedsiębiorstw. Szereg poważnych firm konsultingowych i kancelarii prawnych może także oferować wsparcie w zakresie usług inspektora ochrony danych na podstawie „umowy o świadczenie usług". Usługi takie będą także oferować niektóre małe firmy, w szczególności te specjalizujące się w teleinformatyce.

Zewnętrzni inspektorzy ochrony danych nie powinni być jednak zbyt oddaleni od organów, dla których świadczą swoje usługi, gdyż, jak wyjaśniono w następnej części Podręcznika, muszą oni posiadać pełne i dogłębne zrozumienie organów i ich operacji przetwarzania. Muszą być także w pełni i łatwo dostępni dla pracowników danych organów, a także osób, których dane dotyczą, i organów ochrony danych (organów nadzorczych). Ich dane kontaktowe powinny być wyraźnie podane na stronach internetowych i w ulotkach, itp. odpowiednich organów.

Francuski organ ochrony danych, CNIL, uważa, że najlepiej jest, gdy inspektor ochrony danych jest pracownikiem organizacji administratora, ale akceptuje też fakt, że w przypadku małych i średnich przedsiębiorstw nie zawsze rozwiązanie takie jest możliwe[261].

W sektorze publicznym często preferowanym rozwiązaniem jest posiadanie inspektora ochrony danych z konkretnego sektora, np., co zostało już omówione w poprzednim podpunkcie, centralnego inspektora dla dużego organu publicznego lub wspólnego dla grupy mniejszych podmiotów powiązanego z jednym z nich, raczej niż firmy z sektora prywatnego, która pełni funkcję zewnętrznego inspektora ochrony danych, ale to zależy jednak od kultury i praktyk stosowanych w danym kraju.

2.5.3 Kwalifikacje, cechy i pozycja inspektora ochrony danych

Wymagane kompetencje

Rozporządzenie przewiduje, że:

> Inspektor ochrony danych jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności **wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań**, o których mowa w art. 39 [który omówiono w pkt. 2.3.4].
>
> (art. 37(5), pogrubienie dodane przez autorów Podręcznika)

Jeżeli chodzi o pierwszy z punktów - fachową wiedzę - profesjonalne standardy opracowane przez inspektorów ochrony danych w instytucjach UE zwracają uwagę na potrzebę[262]:

> (a) Kompetencji w zakresie unijnego prawa o prywatności i ochronie danych, w szczególności art. 16 Traktatu o funkcjonowaniu Unii Europejskiej, art. 8 Karty praw podstawowych Unii Europejskiej, Rozporządzenia (WE) 45/2001 oraz innych stosownych instrumentów

[260] Zob. pkt 2.3.1 powyżej.
[261] CNIL, *Guide Pratique Correspondant* (przypis 249 powyżej), str. 6.
[262] Sieć Inspektorów Ochrony Danych Instytucji i Organów UE, Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001 (przypis 244 powyżej), str. 3 – 4.

prawnych dotyczących ochrony danych, a także kompetencji w obszarze informatycznym i bezpieczeństwa informatycznego, oraz

(b) Właściwego zrozumienia sposobu funkcjonowania instytucji [dla której inspektor został wyznaczony] oraz jej czynności z zakresu przetwarzania danych osobowych, a także możliwości interpretowania odpowiednich reguł ochrony danych w takim kontekście.

Szczególnie należy podkreślić wiedzę techniczną na temat systemów informatycznych. Jak ujmuje to **francuski** organ ochrony danych, CNIL[263]:

> W odniesieniu do informatyki konieczne jest właściwe zrozumienie terminologii, praktyk informatycznych oraz różnych form przetwarzania danych. Inspektor ochrony danych powinien znać na przykład systemy zarządzania danymi oraz systemy wykorzystywania danych, rodzaje oprogramowania, pliki i systemy przechowywania danych, a także wymogi poufności i polityki bezpieczeństwa (szyfrowanie danych, podpisy elektroniczne, dane biometryczne ...). Wiedza ta powinna umożliwić inspektorowi monitorowanie rozmieszczenia projektów informatycznych oraz udzielanie przydatnych porad odpowiedzialnemu za przetwarzanie administratorowi.

Motyw 97 RODO także podkreśla, że:

> Niezbędny poziom wiedzy fachowej należy ustalić w szczególności w świetle prowadzonych operacji przetwarzania danych oraz ochrony, której wymagają dane osobowe przetwarzane przez administratora lub podmiot przetwarzający.

Innymi słowy, charakter wymaganej „fachowej wiedzy" oraz „umiejętności" może różnić się w zależności od działalności administratora. Inspektor w organie skarbowym będzie potrzebować innych kompetencji niż inspektor pracujący dla podmiotu edukacyjnego lub opieki społecznej. Europejski Inspektor Ochrony Danych nazywa to potrzebą „**bliskości**" (inspektora ochrony danych do podmiotu, który obsługuje)[264]:

> Inspektor ochrony danych pełni centralną rolę w ramach instytucji/organu. Inspektorzy ochrony danych znają [tj. powinni znać] problemy podmiotu, w którym pracują *(idea bliskości*) oraz, biorąc pod uwagę ich status, mają do odegrania kluczową rolę w zakresie udzielania porad i pomocy w rozwiązywaniu problemów z ochroną danych [czytaj: dotyczących konkretnie danego organu].

Jak stwierdzono w Wytycznych Grupy Roboczej Art. 29 dotyczących inspektorów ochrony danych[265]:

> Inspektor ochrony danych powinien posiadać także wystarczające zrozumienie operacji przetwarzania [realizowanych w odpowiednim sektorze i odpowiedniej organizacji], a także systemów informacyjnych oraz potrzeb administratora w zakresie bezpieczeństwa i ochrony danych.
>
> W przypadku organu lub podmiotu publicznego inspektor ochrony danych powinien znać również [wewnętrzne] zasady i procedury administracyjne organizacji.

Można do tego dodać, że powinien znać także przepisy, zasady i procedury, na mocy których odpowiedni organ publiczny działa (np. prawo podatkowe, prawo dotyczące edukacji itp.), a także przepisy i procedury administracyjne w ogóle.

Z drugiej strony, jak zauważono poniżej w punktach „*Konflikty interesów*" i „*Pozycja w ramach organizacji*", wyznaczenie kogoś z obecnych pracowników organu publicznego może rodzić problemy, w szczególności, gdy wyznaczona osoba ma pracować na niepełny etat i w dalszym ciągu pełni inne funkcje w danym podmiocie.

Fachową znajomość przepisów i praktyk ochrony danych z zasady można potwierdzić poprzez szkolenie oraz kursy internetowe i stacjonarne itp., w jakich osoba taka uczestniczy, jak na przykład kursy oferowane w programie T4DATA, dla celów którego został napisany niniejszy Podręcznik. Oferowanych jest jednak powszechnie wiele innych kursów o różnym poziomie i różnej jakości.

Formalne szkolenie i certyfikacja

[263] CNIL, *Guide Pratique Correspondant* (przypis 249 powyżej), str. 8 (nasze tłumaczenie).
[264] EDPS, Position paper on the role of Data Protection Officers in ensuring effective compliance with Regulation (EC) 45/2001 (przypis 210 powyżej), str. 5, podkreślenie dodane przez autorów Podręcznika.
[265] Wytyczne Grupy Roboczej Art. 29 dotyczące inspektorów ochrony danych (przypis 249 powyżej), str. 11.

W momencie pisania Podręcznika (grudzień 2018 roku) podejmowano kroki w jednym z państw członkowskich UE, **Hiszpanii**, w kierunku stworzenia formalnego programu certyfikacji inspektorów ochrony danych, jednak program ten jeszcze nie funkcjonuje[266]. Ponadto wyżej wspomniany program certyfikacji inspektorów ochrony danych (oraz kilku innych funkcji) oparty jest na ISO 17024, tj. na programie certyfikacji osób fizycznych i specjalistów, gdyż nie spełniają oni wymogów ISO 17065, który jest programem wspomnianym w koncepcji certyfikacji przewidzianej w RODO (certyfikacja usług, produktów, ewentualnie systemów zarządzania). Tak więc, certyfikacje inspektorów ochrony danych, różne od certyfikacji z art. 42 RODO, są godne pochwały, ale nie są one zgodne z certyfikacjami przewidzianymi w RODO.

We **Francji** organ ochrony danych, CNIL, wydał 11 października 2018 r. dwa „*référentiels*" (specyfikacje - ang. „specifications") dotyczące certyfikacji inspektorów ochrony danych, które opublikowano w krajowym dzienniku ustaw. Jeden z nich dotyczy certyfikacji kompetencji inspektorów ochrony danych, a drugi określenia kompetencji inspektorów ochrony danych oraz organizacji akredytującej upoważnionej do ich certyfikacji[267].

W **Niemczech** oferowane są różne kursy i seminaria, z których część prowadzi do pewnych form certyfikacji[268], ale mimo że instytucja ta posiada w tym kraju długą historię, nie istnieje żaden ustawowo uregulowany i oficjalnie uznawany program. Kilka wcześniej wymienionych międzynarodowych i krajowych stowarzyszeń inspektorów ochrony danych także oferuje specjalistyczne szkolenia, jednak bez ustawowego umocowania[269].

Wiele kursów i seminariów ma na celu przekazanie uczestnikom wiedzy na temat RODO oraz wytycznych w zakresie zadań przypisanych na podstawie RODO inspektorom ochrony danych. Jednak RODO (podobnie jak niemieckie oraz inne przepisy krajowe) nie przewiduje żadnych bardziej szczegółowych kryteriów ani programów certyfikacyjnych. Możliwe że w przyszłości pozostałe państwa członkowskie, poza Hiszpanią, także ustanowią formalne i oficjalnie uznawane programy i/lub może je (najprawdopodobniej nieformalnie) zatwierdzić Europejska Rada Ochrony Danych[270]. Jednak do tego czasu parametry są raczej otwarte. Jak ujmuje to **włoski** organ ochrony danych, *Garante* [271]:

> Tak, jak w przypadku tak zwanych „zawodów nieregulowanych", opracowano własne programy dobrowolnej certyfikacji umiejętności i kompetencji zawodowych. Programami takimi zarządza kilka podmiotów certyfikujących. Tego rodzaju certyfikaty, które nie mieszczą się w zakresie art. 42 RODO, są czasami wydawane po udziale w szkoleniu i/lub odbyciu kursów weryfikujących.
>
> Chociaż stanowią one cenne narzędzie, które podobnie do innych atestów może potwierdzać posiadanie przez specjalistę przynajmniej podstawowej znajomości obowiązujących zasad, certyfikaty takie nie są jednoznaczne z kwalifikacjami umożliwiającymi wykonywanie zadań

---

[266] Hiszpański krajowy organ ochrony danych, *Agencia Española de Protección de Dato* (AEPD), ustanowił program certyfikacyjny dla inspektorów ochrony danych (*Esquema de Certificación de Delegados de Protección de Datos de la Agencia Española de Protección de Datos – Esquema AEPD-DPD*), w ramach którego hiszpańska krajowa agencja akredytacyjna (*la Entidad Nacional de Acreditación – ENAC*) może akredytować podmioty certyfikujące (*Entidades de Certificación*), które następnie mają prawo wydawać odpowiednie certyfikaty na podstawie kryteriów opracowanych przez organ ochrony danych (AEDP) oraz formalnego egzaminu, zob. https://www.aepd.es/reglamento/cumplimiento/common/esquema-aepd-dpd.pdf (wersja 1.3, 13 czerwca 2018 r.). Jednak żaden tego typu podmiot certyfikujący nie został jeszcze akredytowany, w związku z czym nie wydano też żadnego certyfikatu dla inspektora ochrony danych. Zob. krótka ogólna dyskusja na temat programów certyfikacyjnych w pkt. 2.1 powyżej.

[267] Zob. https://www.cnil.fr/fr/certification-des-competences-du-dpo-la-cnil-adopte-deux-referentiels.

[268] Zob. https://www.datenschutzexperten.de/grundlagenseminar-ausbildung-betrieblicher-datenschutzbeauftragter-nach-bdsg-mit-dekra.html.

[269] Opracowany przez inspektorów ochrony danych działających w instytucjach UE dokument poświęcony standardom zaleca stosowanie programów Międzynarodowego Stowarzyszenia Specjalistów ds. Prywatności (International Association of Privacy Professionals (IAPP)). IAPP oferuje regionalne certyfikaty, w tym jeden europejski, które w szczególności obejmują RODO. Zob. https://iapp.org/certify/cippe/. Sieć Inspektorów Ochrony Danych Instytucji i Organów UE, Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001 (przypis 244 powyżej), str. 5. Opracowany przez inspektorów ochrony danych w instytucjach UE dokument wspomina także o zarządzaniu bezpieczeństwem informatycznym oraz certyfikatach z kontroli, ale mają one bardziej ogólny charakter i nie są ukierunkowane na ochronę danych.

[270] Wytyczne Grupy Roboczej Art. 29 dotyczące inspektorów ochrony danych (przypis 242 powyżej) stwierdzają jedynie, że „Propagowanie odpowiednich i regularnych szkoleń dla inspektorów ochrony danych przez organy nadzorcze również może być przydatne." (str. 11).

[271] *Garante della Privacy*, FAQs on DPOs (przypis 249 powyżej), ust. 3.

> inspektora ochrony danych i nie mogą zastąpić spoczywającego na publicznych organach administracyjnych obowiązku oceny, czy inspektor spełnia wymagania mające zastosowanie do zadań i obowiązków przewidzianych w art. 39 RODO.

Konfederacja Europejskich Organizacji Ochrony Danych (Confederation of European Data Protection Organisations (CEDPO)) ujęła to następująco[272]:

> Kandydaci będą najprawdopodobniej prezentować mnóstwo certyfikatów i dyplomów, które zdobyli przez lata, by potwierdzić swoje kwalifikacje. Ale jak stwierdzić, które z nich są cenne, a które nie? Po pierwsze, należy sprawdzić kwalifikacje strony przeprowadzającej szkolenie i wydającej certyfikat. Jeżeli jest to dobrze znana akredytowana pan-unijna lub krajowa organizacja (w niektórych krajach certyfikaty wydają nawet organy ochrony danych), można być spokojnym. Należy także sprawdzić program szkolenia. Jednodniowe wydarzenie lub certyfikaty uzyskane głównie za opłatą oraz bardzo prosty egzamin nie zapewnią rzetelnego przeszkolenia inspektora ochrony danych.

Wszystkie różne wytyczne podkreślają także, że organizacja powinna zapewnić swojemu inspektorowi ochrony danych możliwość utrzymania i dalszej poprawy swoich kompetencji także po nominacji poprzez udział w stosownych kursach i seminariach. Wymaga tego także RODO (patrz: ostatnie słowa w art. 38(2)). Grupa Robocza Art. 29 ujmuje to następująco[273]:

> Inspektorzy ochrony danych powinni mieć możliwość bieżącej aktualizacji swojej wiedzy na temat zmian związanych z ochroną danych. Celem powinno być stałe podnoszenie poziomu kompetencji inspektorów ochrony danych, których należy zachęcać do udziału w szkoleniach o ochronie danych oraz w innych formach rozwoju zawodowego, takich jak udział w forach lub warsztatach poświęconych prywatności, itp.

Francuski organ ochrony danych, CNIL, zapewnia przydatny specjalny „**extranet**" dla zarejestrowanych inspektorów ochrony danych, dostępny tylko dla nich na podstawie nazwy użytkownika i hasła, w którym prezentowane są teksty prawne (ustawy, dekrety itp.) oraz szkolenia i informacje, z uwzględnieniem informacji na temat nowych sprawozdań lub wytycznych wydanych przez CNIL, a także innych prawnych i praktycznych zmian, oraz umożliwia im wymianę poglądów i prowadzenie dyskusji[274].

Doświadczenie

Wytyczne Grupy Roboczej Art. 29 dotyczące inspektorów ochrony danych nie zajmują się kwestią (długości) doświadczenia, jakie powinien posiadać inspektor ochrony danych. Jednak Sieć inspektorów ochrony danych w instytucjach UE zaleca, by inspektorzy posiadali następujące doświadczenie/następujący staż[275]:

> co najmniej 3 lata odpowiedniego doświadczenia [patrz poniżej], by pełnić funkcję inspektora ochrony danych w organie, w którym ochrona danych nie jest związana z główną działalnością [*idem*] (a czynności przetwarzania danych mają głównie charakter administracyjny) oraz
>
> co najmniej 7 lata odpowiedniego doświadczenia, by pełnić funkcję inspektora ochrony danych w instytucji unijnej lub w tych organach UE, w których ochrona danych jest związana z główną działalnością lub liczba operacji przetwarzania danych osobowych jest znacząca.

W przypisie dodano jeszcze, że:

> Odpowiednie doświadczenie obejmuje doświadczenie w zakresie wdrażania wymogów ochrony danych oraz doświadczenie w ramach mianującej inspektora instytucji/organizacji zapewniające wiedzę na temat jej funkcjonowania. W przypadku braku określonej liczby lat doświadczenia instytucja/organ mianujący inspektora powinien być przygotowany na zapewnienie inspektorowi dłuższego okresu na szkolenie lub realizację zadań z zakresu ochrony danych.

---

[272] CEDPO, Choosing the best candidate as your Data Protection Officer (DPO) – Practical guidelines for organisations (przypis 206 powyżej), str. 2.
[273] Wytyczne Grupy Roboczej Art. 29 dotyczące inspektorów ochrony danych (przypis 242 powyżej), str. 14.
[274] CNIL, *Guide Pratique Correspondant* (przypis 249 powyżej), str. 4.
[275] Sieć Inspektorów Ochrony Danych Instytucji i Organów UE, Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001 (przypis 244 powyżej), str. 4.

Jeżeli chodzi o to, czy przetwarzanie danych osobowych „jest związane z główną działalnością" danej organizacji, Wytyczne Grupy Roboczej Art. 29 dotyczące znaczenia podobnego zwrotu w RODO („główna działalność administratora lub przetwarzającego") przewidują, że[276]:

> „Główną działalność" można traktować jako kluczowe operacje konieczne do osiągnięcia celów administratora lub przetwarzającego.

Zwrotu „odpowiednie doświadczenie" nie należy rozumieć jako doświadczenie jako inspektor ochrony danych. Może to być doświadczenie w zakresie opracowywania i wdrażania polityk w odpowiedniej organizacji (lub podobnej organizacji) albo w odpowiednich obszarach, takich jak informatyka, rozwój produktów itp. Wystarczy zauważyć, że stanowiska tego nie należy powierzać względnie młodej niedoświadczonej osobie ani osobie niezaznajomionej z konkretną organizacją (konkretnym typem organizacji).

Cechy osobowe

Europejski Inspektor Ochrony Danych, inspektorzy ochrony danych w instytucjach unijnych oraz CEDPO prawidłowo zauważają, że inspektor ochrony danych musi posiadać specjalne cechy osobowe. Ponieważ piastuje delikatną funkcję, musi być w stanie w rzadkich przypadkach powiedzieć „nie" swoim szefom, ale częściej musi być w stanie pomóc znaleźć rozwiązanie problemów, które będzie zarówno akceptowalne dla organizacji, jak i w pełni zgodne z prawem (a przede wszystkim będzie poprawiać poziom prywatności). Jak stwierdzono w Wytycznych Grupy Roboczej Art. 29[277]:

> Cechy osobowe powinny obejmować na przykład rzetelne podejście oraz wysoki poziom etyki zawodowej, a inspektorowi powinno przede wszystkim zależeć na przestrzeganiu RODO. Inspektor odgrywa kluczową rolę w zakresie wspierania „kultury ochrony danych" w ramach podmiotu oraz pomaga w implementacji niezbędnych elementów RODO ...

Inspektorzy ochrony danych w instytucjach UE podkreślają potrzebę posiadania następujących umiejętności „osobistych" i „interpersonalnych"[278]:

> Osobiste umiejętności: prawość, inicjatywa, organizacja, wytrwałość, dyskrecja, umiejętność zaznaczenia swojego autorytetu w trudnych sytuacjach, zainteresowanie ochroną danych oraz motywacja do pełnienia funkcji inspektora ochrony danych.
>
> Umiejętności interpersonalne: komunikacja, negocjacje, rozstrzyganie konfliktów, umiejętność budowania relacji w pracy.

W innym miejscu wspomniano, że[279]:

> Właściwe wykonywanie zadań inspektora ochrony danych wymaga, aby inspektor stosował zdecydowane i wymagające podejście także w odniesieniu do administratorów, którzy mają wysoką pozycję w organizacji, co może być postrzegane - w najlepszym przypadku - jako biurokratyczne, a - w najgorszym przypadku - jako nieprzyjemne „stwarzanie problemów". Tak więc inspektor ochrony danych musi być w stanie wytrzymać naciski i trudności towarzyszące temu istotnemu stanowisku.

CEDPO dodaje, że[280]:

> Inspektor Ochrony Danych musi stawić czoła wielu wyzwaniom oraz różnym interesom. Dlatego też powinien posiadać dobre umiejętności komunikowania się powiązane z wyrafinowaną dyplomacją. Inspektor nie jest (i nie powinien być) „aktywistą na rzecz prywatności" - przy wsparciu pozostałych liderów organizacji, musi odgrywać rolę odpowiedzialnego pomocnika oraz wspierać organizację w uwzględnianiu kwestii prywatności w procesach decyzyjnych, musi nie tylko wykrywać zagrożenia i im zapobiegać, ale także kreować wartość. Ponadto RODO wymaga, by

[276] Wytyczne Grupy Roboczej Art. 29 dotyczące inspektorów ochrony danych (przypis 242 powyżej), str. 6.
[277] Wytyczne Grupy Roboczej Art. 29 dotyczące inspektorów ochrony danych (przypis 242 powyżej), str. 11.
[278] Sieć Inspektorów Ochrony Danych Instytucji i Organów UE, Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001 (przypis 244 powyżej), str. 4.
[279] *Idem*, str. 6. Sieć wydaje zalecenia mające złagodzić naciski w kontekście dyskusji na temat stanowiska, jakie ma zostać przyznane inspektorowi ochrony danych w odpowiedniej organizacji, co zostało omówione w punkcie „*Pozycja inspektora ochrony danych w ramach organizacji*".
[280] CEDPO, Choosing the best candidate as your Data Protection Officer (DPO) – Practical guidelines for organisations (przypis 239 powyżej), str. 3 (nieznacznie zmieniony).

inspektor podlegał przedstawicielom najwyższego szczebla zarządzania oraz by zapewniono jego niezależność. Wymaga to także „powagi" i umiejętności przywódczych.

Niezależność

Wspomnieliśmy już, że „Inspektor ochrony danych może być członkiem personelu administratora lub podmiotu przetwarzającego lub wykonywać zadania na podstawie umowy o świadczenie usług" (art. 37(6)). Jednak w żadnym przypadku nie jest to funkcja dla zwykłego pracownika lub wykonawcy. Rozporządzenie podkreśla w szczególności, że:

> Tacy inspektorzy ochrony danych – bez względu na to, czy są pracownikami administratora – powinni być w stanie wykonywać swoje obowiązki i zadania w sposób niezależny. (motyw 97)

Rozporządzenie przewiduje także, że:

> Administrator oraz podmiot przetwarzający zapewniają, by **inspektor ochrony danych nie otrzymywał instrukcji dotyczących wykonywania tych zadań.** Nie jest on **odwoływany ani karany przez administratora ani podmiot przetwarzający za wypełnianie swoich zadań.** Inspektor ochrony danych **bezpośrednio podlega najwyższemu kierownictwu** administratora lub podmiotu przetwarzającego.
>
> (art. 38(3))

Grupa Robocza Art. 29 wyjaśnia to następująco[281]:

> [Powyższe postanowienia] oznaczają, że, wypełniając swoje zadania wynikające z art. 39, inspektorzy ochrony danych nie mogą być instruowani, w jaki sposób rozwiązać daną sprawę, na przykład jaki wynik należy osiągnąć, w jaki sposób należy rozpatrzyć reklamację lub czy należy skonsultować się z organem nadzorczym. Ponadto nie wolno im zlecać przyjęcia określonego spojrzenia na sprawę związaną z przepisami ochrony danych, na przykład konkretną interpretacją prawa.
>
> Autonomia inspektorów nie oznacza jednak, że mają oni uprawnienia decyzyjne wykraczające poza zadania wynikające z art. 39.
>
> Administrator lub podmiot przetwarzający są w dalszym ciągu odpowiedzialni za przestrzeganie przepisów o ochronie danych i muszą to wykazać. W sytuacji podjęcia przez administratora lub podmiot przetwarzający decyzji niezgodnej z przepisami RODO i zaleceniami inspektora ochrony danych, inspektor powinien mieć możliwość jasnego przedstawienia swojej odrębnej opinii najwyższemu kierownictwu i osobom podejmującym decyzję.

Jak dalej zauważono w części trzeciej, porady inspektora ochrony danych oraz wszystkie działania podejmowane na ich podstawie należy zarejestrować, a zignorowanie takiej porady może zostać wykorzystane przeciwko administratorowi lub podmiotowi przetwarzającemu w kolejnym dochodzeniu prowadzonym przez właściwy organ ochrony danych. (Jak wcześniej zauważono, wręcz odwrotnie, fakt, że administrator lub przetwarzający działa zgodnie z poradą lub wskazówką inspektora ochrony danych może stanowić „element" procesu wykazywania przestrzegania postanowień RODO (motyw 77)[282].

Grupa Robocza Art. 29 wyjaśnia także zakres postanowienia, że inspektorzy ochrony danych nie powinni być zwalniani ani karani przez administratora lub podmiot przetwarzający za wykonywanie swoich zadań[283].

> Wymóg ten zwiększa niezależność inspektora ochrony danych i zapewnia możliwość wykonywania zadań w niezależny i odpowiednio chroniony sposób.
>
> Kary w świetle RODO niedozwolone są tylko w przypadkach, gdy są nałożone w związku z wypełnianiem przez inspektorów swoich zadań. Na przykład inspektor ochrony danych może uznać określone przetwarzanie za wysoce ryzykowne i zalecić administratorowi lub podmiotowi przetwarzającemu przeprowadzenie oceny skutków dla ochrony danych, ale administrator lub podmiot przetwarzający nie zgadza się z oceną inspektora. W takiej sytuacji inspektor ochrony danych nie może zostać odwołany ani karany za udzielenie określonego zalecenia.

[281] Wytyczne Grupy Roboczej Art. 29 dotyczące inspektorów ochrony danych (przypis 242 powyżej), pkt 3.3, str. 14 – 15.
[282] Zob. pkt 2.2.2 powyżej.
[283] Wytyczne Grupy Roboczej Art. 29 dotyczące inspektorów ochrony danych (przypis 242 powyżej), ust. 3.4, str. 15.

> Kary mogą przybrać szereg form i mogą być bezpośrednie albo pośrednie. Mogą polegać na braku albo opóźnieniu awansu, utrudnieniu rozwoju zawodowego, ograniczeniu dostępu do korzyści oferowanych pozostałym pracownikom. Nieistotny jest przy tym fakt nałożenia kary, gdyż sama możliwość jej wykonania i obawa z tym związana może być wystarczająca do utrudnienia inspektorowi ochrony danych wykonywania zadań.
>
> Zgodnie z normalnymi regułami, przepisami karnymi i prawa pracy, jak w przypadku każdego innego pracownika czy zleceniobiorcy, inspektor może zostać odwołany w uzasadnionych sytuacjach z przyczyn innych niż wykonywanie obowiązków inspektora ochrony danych (np. kradzież, nękanie fizyczne i psychiczne, molestowanie seksualne, ciężkie naruszenie obowiązków).
>
> W tym kontekście RODO nie wyjaśnia, jak i kiedy inspektor ochrony danych może zostać odwołany i zastąpiony inną osobą. Jednak im stabilniejszy kontrakt i szerszy zakres ochrony przed odwołaniem, tym większa szansa na wykonywanie zadań inspektora ochrony danych w sposób niezależny. Dlatego też GR Art. 29 zaleca stosowanie takiej polityki.

I na koniec, umowa o pracę oferowana inspektorowi ochrony danych powinna zawierać postanowienia powtarzające przepisy RODO o niezależności lub do takich przepisów nawiązujące. Trybunały i sądy orzekające w sprawach o zwolnienie powinny oczywiście brać w pełni pod uwagę postanowienia RODO. Tam, gdzie to konieczne, przydatne może okazać się wprowadzenie w tym zakresie zmian w prawie pracy. Państwa członkowskie mogą także wzmocnić niezależność inspektorów ochrony danych w innych przepisach krajowych - przykłady zabezpieczeń na wypadek zwolnienia pewnych pracowników można znaleźć w przepisach zapewniających szczególną ochronę na przykład pracowników związków zawodowych i/lub wymagających zgody rad pracowniczych na nominację na określone stanowiska oraz zwolnienie pracowników je piastujących.

Uwaga: inspektorzy ochrony danych w instytucjach unijnych omawiają kwestie niezależności i konfliktów interesów (następna kwestia omówiona w Podręczniku) głównie w kontekście zabezpieczeń umownych, długości zatrudnienia oraz innych zabezpieczeń, które omówiono poniżej w punkcie zatytułowanym *„Stanowisko inspektora ochrony danych w ramach organizacji”*. CEDPO zauważa jedynie, że organizacja, która mianuje inspektora ochrony danych powinna rozważyć, w jaki sposób zapewni jego niezależność[284].

Konflikty interesów

Jak zauważa Grupa Robocza Art. 29[285]:

> Artykuł 38(6) umożliwia inspektorom ochrony danych wykonywanie „innych zadań i obowiązków”. Dalej w artykule widnieje zapis, że „administrator lub podmiot przetwarzający zapewniają, by takie zadania i obowiązki nie powodowały konfliktu interesów”.
>
> Wymóg niepowodowania konfliktu interesów jest ściśle związany z wymogiem wykonywania zadań w sposób niezależny. I choć inspektorzy ochrony danych mogą posiadać inne zadania i obowiązki to jednak te nie mogą powodować konfliktu interesów. Oznacza to, że inspektor nie może zajmować w organizacji stanowiska pociągającego za sobą określanie sposobów i celów przetwarzania danych. Ze względu na indywidualny charakter każdej organizacji ten aspekt powinien być analizowany osobno dla każdego podmiotu.
>
> Co do zasady, za powodujące konflikt interesów uważane będą stanowiska kierownicze (dyrektor generalny, dyrektor ds. operacyjnych, dyrektor finansowy, dyrektor ds. medycznych, kierownik działu marketingu, kierownik działu HR, kierownik działu IT), ale również niższe stanowiska, jeśli biorą udział w określaniu celów i sposobów przetwarzania danych.
>
> Zależnie od rodzaju działalności, rozmiaru i struktury organizacji, dobrą praktyką dla administratorów i podmiotów przetwarzających może być:
>
> - Zidentyfikowanie stanowisk niekompatybilnych z funkcją inspektora ochrony danych;
> - Opracowanie wewnętrznych zasad uniemożliwiających łączenie stanowisk będących w konflikcie interesów;
> - Zapewnienie bardziej ogólnego wyjaśnienia dotyczącego konfliktu interesów;
> - Zadeklarowanie, że nie ma konfliktu interesów w funkcjonowaniu obecnego inspektora ochrony danych, celem zwiększenia świadomości na temat tego wymogu;

[284] CEDPO, Choosing the best candidate as your Data Protection Officer (DPO) – Practical guidelines for organisations (przypis 239 powyżej), str. 3.

[285] Wytyczne Grupy Roboczej Art. 29 dotyczące inspektorów ochrony danych (przypis 242 powyżej), pkt 3.5, str. 15 – 16. Trzeci paragraf („z zasady”) pojawia się jako przypis w dokumencie, a nie w głównej części tekstu, jak ma to miejsce tutaj.

- Wprowadzenie odpowiednich zabezpieczeń do wewnętrznych zasad organizacji celem zapewnienia, by ogłoszenia o rekrutacji na stanowisko inspektora ochrony danych czy też umowy o świadczenie usług były wystarczająco jasne i precyzyjne, aby niwelować ryzyko powstania konfliktu interesów. W tym kontekście należy również pamiętać, że konflikt interesów może przybierać różne formy, w zależności od tego, czy rekrutacja na stanowisko inspektora ochrony danych ma charakter wewnętrzny czy zewnętrzny.

Inspektorzy ochrony danych w instytucjach UE dodają, że[286]:

> Inspektor ochrony danych nie powinien mieć konfliktu interesów pomiędzy obowiązkami inspektora a innymi oficjalnymi obowiązkami, w szczególności w odniesieniu do stosowania postanowień Rozporządzenia (art. 24.3). Konflikt interesów ma miejsce, gdy inne zadania, o jakich wykonanie inspektor został poproszony, mogą mieć bezpośredni niekorzystny wpływ na ochronę danych osobowych w jego instytucji. W razie konieczności, inspektor powinien zgłosić taką sprawę organowi, który go wyznaczył.

Następnie należy ją rozpatrzyć bardziej szczegółowo w kontekście zabezpieczeń umownych, długości nominacji i innych zabezpieczeń, o których była mowa powyżej. CEDPO ponownie zauważa, że jeżeli inspektor nie pełni swojej funkcji na pełny etat, organizacja, która go wyznacza powinna rozważyć sposób radzenia sobie z konfliktami interesów"[287].

Pozycja inspektora ochrony danych w ramach organizacji

Hierarchiczna i umowna pozycja inspektora ochrony danych w ramach organizacji ma zasadnicze znaczenie w odniesieniu do zapewnienia jego efektywności, niezależności oraz unikania konfliktów interesów.

Z jednej strony, jak wcześniej zauważono, inspektor ochrony danych powinien być blisko organizacji, którą obsługuje (punkt zatytułowany *„Wymagane kompetencje"*). Ponadto CEDPO stwierdza, że[288]:

> Aby inspektor ochrony danych był skuteczny, powinien być na miejscu, nie tylko dostępny dla różnych zainteresowanych stron w ramach organizacji, ale aktywnie poszukujący możliwości interakcji z różnymi departamentami.

Może być to problematyczne w przypadku zewnętrznych inspektorów działających na podstawie umowy o świadczenie usług - z definicji nie będą oni częścią podmiotu, który wspierają. W sektorze prywatnym mogą działać także, a w niektórych krajach, takich jak Niemcy, niewątpliwie działają, zewnętrzni inspektorzy ochrony danych posiadający szerokie kompetencje w sektorze prywatnym lub podsektorze, w którym pracują. W sektorze publicznym może to być trudniejsze (por. pkt 2.3.2 w podpunktach zatytułowanych *„Inspektorzy ochrony danych dla dużych organów publicznych lub grup organów"* oraz *„Zewnętrzni inspektorzy ochrony danych*").

Jednak zawsze istnieje napięcie pomiędzy z jednej strony wymaganą „bliskością" inspektora do swojej organizacji, a z drugiej strony potrzebą unikania konfliktów interesów i zapewnienia w praktyce jego faktycznej niezależności.

Jak już wspomniano, zdaniem Grupy Roboczej Art. 29 oznacza to, że inspektor ochrony danych nie może uczestniczyć w ustalaniu celów i sposobów przetwarzania danych osobowych oraz nie może piastować stanowiska wyższego szczebla, takiego jak dyrektor wykonawczy lub dyrektor głównego departamentu[289].

---

[286] Sieć Inspektorów Ochrony Danych Instytucji i Organów UE (CEDPO), Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001 (przypis 244 powyżej), str. 15.

[287] CEDPO, Choosing the best candidate as your Data Protection Officer (DPO) – Practical guidelines for organisations (przypis 239 powyżej), str. 3.

[288] *Idem*, str. 2.

[289] Patrz powyżej, w punkcie zatytułowanym *„Konflikty interesów"*, ze szczególnym uwzględnieniem trzeciego paragrafu w cytacie pochodzącym z Wytycznych Grupy Roboczej Art. 29 dotyczących inspektorów ochrony danych. Z kolei **włoski** organ ochrony danych, *Garante,* w swoich najczęściej zadawanych pytaniach i odpowiedziach w sprawie inspektorów ochrony danych informuje, że:

> .. Art. 38(3) przewiduje, że inspektor ochrony danych „bezpośrednio podlega najwyższemu kierownictwu administratora lub podmiotu przetwarzającego". Ten wymóg bezpośredniej podległości może zagwarantować w szczególności, że najwyższe kierownictwo będzie informowane o wskazówkach i

Kwestią tą zajęli się bardziej szczegółowo inspektorzy ochrony danych w instytucjach UE. Chociaż ich poglądy mogą być oczywiście postrzegane w świetle specyficznego kontekstu, warto im się jednak przyjrzeć. Uwzględniając różne postanowienia w mającym do nich zastosowanie rozporządzeniu (Rozporządzenie (WE) 45/2001)[290], których celem jest zagwarantowanie ich niezależności, stwierdzają, co następuje[291]:

> W praktyce jednak wykonywanie obowiązków przez inspektora ochrony danych w pełni niezależny sposób może stanowić dla niego wyzwanie. Rzecz jasna, indywidualna sytuacja i osobowość inspektora będzie odgrywać tutaj rolę, ale można ogólnie założyć, że pewne elementy mogą osłabiać jego pozycję:
>
> - zatrudniony na niepełny etat inspektor musi stawiać czoła stałemu konfliktowi pomiędzy podziałem czasu i wysiłków na zadania inspektora ochrony danych i inne zadania. W odniesieniu do rozwoju kariery i przeglądu wyników kierownictwo może kłaść większy nacisk na czynności niezwiązane z funkcją inspektora ochrony danych. W ten sposób na inspektora wywierany jest nacisk, by skoncentrował swoje wysiłki na zadaniach innych niż obowiązki inspektora. Zatrudniony na niepełny etat inspektor ochrony danych jest także narażony na konflikty interesów.
> - Inspektor posiadający umowę na czas określony będzie prawdopodobnie mniej zmotywowany, by wykonywać aktywnie swoje obowiązki inspektora, niż w przypadku umowy stałej (oficjalny lub tymczasowy agent na postawie umowy na czas nieokreślony). Wynika to z tego, że może martwić się, w jaki sposób jego działania mogą niekorzystnie wpłynąć na odnowienie umowy. Inspektor ochrony danych, który jest bardzo młody i posiada ograniczone doświadczenie zawodowe, może mieć trudności, by postawić się administratorowi oraz może być bardziej skupiony na rozwoju swojej własnej kariery niż na aktywnej realizacji obowiązków inspektora.
> - Inspektor ochrony danych, który podlega służbowo oraz ocenie bezpośredniego przełożonego w hierarchii (dyrektorowi lub szefowi jednostki) może odczuwać nacisk, by współpracować i mieć dobre relacje z kierownictwem i innymi pracownikami, gdyż aktywne wykonywanie zadań inspektora może mieć niekorzystny wpływ na jego karierę ... By złagodzić ten nacisk, inspektor ochrony danych powinien podlegać służbowo i ocenie dyrektora administracyjnego instytucji lub organu. Jest to szczególnie istotne w przypadku niepełnoetatowych inspektorów, którzy z racji obowiązków inspektora powinni bezpośrednio podlegać służbowo i ocenie organu je nominującego oraz normalnemu zwierzchnikowi w hierarchii w związku z pozostałymi obowiązkami.
> - Inspektor ochrony danych, który musi prosić swojego bezpośredniego przełożonego o pracowników i zasoby (informatyczne, budżet na delegacje i szkolenia), może być napotkać trudności, jeżeli przełożony nie będzie w pełni zaangażowany w przestrzeganie przepisów o ochronie danych. Można tego uniknąć, jeżeli inspektor ochrony danych ponosi sam odpowiedzialność za budżet, oraz poprzez uzależnienie wniosków o dodatkowe zasoby od zgody organu go mianującego.
>
> Dobre praktyki mające pomóc w zapewnieniu niezależności inspektora ochrony danych:
>
> - Instytucja lub organ powinien ustanowić stanowisko inspektora ochrony danych w ramach organizacji jako stanowisko doradcy, szefa jednostki lub dyrektora i stanowisko takie

---

wytycznych przekazywanych przez inspektora ochrony danych pełniącego funkcję doradczą i/lub funkcję podnoszenia świadomości w organizacji administratora lub podmiotu przetwarzającego.
W związku z tym, jeżeli wyznaczono wewnętrznego inspektora ochrony danych, najlepiej byłoby z zasady, gdyby na stanowisko to został wybrany dyrektor departamentu lub przedstawiciel pracowników wyższego szczebla, jeżeli jest to wykonalne, biorąc pod uwagę strukturę organizacyjną oraz złożoność czynności przetwarzania. W ten sposób wyznaczony inspektor ochrony danych będzie w stanie wykonywać swoje obowiązki w pełni autonomicznie i niezależnie oraz będzie miał bezpośredni kontakt z najwyższymi szczeblami zarządzania. (*Garante*, FAQs on DPOs [przypis 249powyżej], ust. 2.)

Może najlepszym sposobem na uzgodnienie poglądów Grupy Roboczej Art. 29 oraz *Garante* w tym zakresie byłaby propozycja, aby inspektora ochrony danych mianowano *na szczeblu* dyrektora departamentu lub kierownika wyższego szczebla, nie ponoszącego jednak faktycznej odpowiedzialności za operacje przetwarzania danych.

[290] Zob. przypis 148 powyżej.

[291] Sieć Inspektorów Ochrony Danych Instytucji i Organów UE, Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001 (przypis 244 powyżej), str. 6 – 7.

powinno być zawsze oficjalnie uznawane jako stanowisko kierownicze w oficjalnym schemacie organizacyjnym.

- Instytucja lub organ powinien mianować inspektora ochrony danych na najdłuższy możliwy termin w świetle zawartej z nim umowy. Tak więc pięcioletnia nominacja powinna być normą, chyba że jest to w określonych okolicznościach niemożliwe;
- Inspektor ochrony danych powinien zawrzeć z instytucją lub organem umowę stałą/na czas nieokreślony oraz powinien posiadać wystarczające doświadczenie (...);
- Inspektor powinien poświęcić cały swój czas obowiązkom inspektora ochrony danych, w szczególności w dużych instytucjach i organach, a w mniejszych na wstępnym etapie tworzenia systemu ochrony danych. Należy zapewnić właściwe wsparcie w formie zasobów i infrastruktury. Nałożone na niepełnoetatowego inspektora obowiązki inne niż obowiązki inspektora ochrony danych nie powinny rodzić, ani sprawiać wrażenia, konfliktu interesów z obowiązkami inspektora;
- Inspektorzy ochrony danych w organizacjach, gdzie przetwarzanie danych stanowi główną działalność, z reguły będą wymagać różnych pracowników. Należy zapewnić odpowiednie kwalifikacje takich pracowników;
- W organizacji należy wprowadzić reguły nakładające na wszystkich pracowników obowiązek współpracy z inspektorem ochrony danych bez konieczności oczekiwania na nakaz lub pozwolenie ze strony ich przełożonego;
- Inspektor ochrony danych powinien podlegać szefowi instytucji lub organu, który powinien być odpowiedzialny za ocenę wyników pracy inspektora zgodnie z Rozporządzeniem. Osoba odpowiedzialna za ocenę wyników pracy inspektora ochrony danych powinna wziąć pod uwagę potrzebę przyjmowania przez niego zdecydowanego stanowiska, czego inne osoby w organizacji mogą nie doceniać. Inspektor ochrony danych nie powinien być narażony na uprzedzenia w związku z wykonywaniem swoich obowiązków. Organ mianujący inspektora powinien zapewnić, by przez cały okres piastowania swojego stanowiska miał możliwość przynajmniej „normalnego" rozwoju swojej kariery. W trakcie oceny wyników pracy inspektora osoba oceniająca powinna uważać, by nie ganić go za wydawanie niepopularnych stanowisk oraz nie traktować wymogów ochrony danych jako ciężaru administracyjnego. W przypadku niepełnoetatowych inspektorów wynikom oceny należy nadać wagi odpowiadające wynikom pracy w zakresie innych przyznanych im obowiązków ...;
- Inspektor ochrony danych powinien posiadać swój własny budżet, ustalony w zgodności z odpowiednimi zasadami i procedurami właściwej instytucji/właściwego organu, a jego wnioski o dodatkowe środki powinny podlegać zatwierdzeniu przez dyrektora administracyjnego. Inne ustalenia są do zaakceptowania, pod warunkiem że gwarantują inspektorowi zasoby, jakich potrzebuje, by realizować swoją misję w niezależny sposób.
- Inspektor ochrony danych powinien mieć uprawnienia do podpisywania korespondencji dotyczącej ochrony danych.

Organy ochrony danych mogą uznać za stosowne wydanie szczegółowych wytycznych w oparciu o powyższe postanowienia.

Zasoby i obiekty

RODO przewiduje, że:

> Administrator oraz podmiot przetwarzający wspierają inspektora ochrony danych w wypełnianiu przez niego zadań, o których mowa w art. 39 [o którym mowa w pkt. 2.3.4 poniżej], zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej.
>
> (art. 38(2))

W tym zakresie Grupa Robocza Art. 29 zaleca w szczególności[292]:

- wsparcie inspektora ochrony danych ze strony kadry kierowniczej (np. na poziomie zarządu);

[292] Wytyczne Grupy Roboczej Art. 29 dotyczące inspektorów ochrony danych (przypis 242 powyżej), pkt 3.2, str. 13 – 14.

- wymiar czasu umożliwiający inspektorowi ochrony danych wykonywanie zadań. Jest to szczególnie istotne w przypadku wewnętrznych inspektorów zatrudnionych w niepełnym wymiarze, albo w przypadku zewnętrznych inspektorów łączących obowiązki inspektora z innymi zadaniami. Wystąpienie sprzecznych priorytetów skutkować mogłoby zaniedbaniem obowiązków inspektora ochrony danych. Posiadanie wystarczającej ilości czasu na wypełnianie obowiązków inspektora jest bardzo ważne. Dobrą praktyką jest ustalenie procentowo czasu przeznaczonego na funkcję inspektora ochrony danych, jeżeli nie pracuje on na pełny etat. Dobrą praktyką byłoby wskazanie czasu, który należy poświęcić na obowiązki inspektora, oszacowane czasu potrzebnego na wypełnienie tych obowiązków, ustalenie priorytetów inspektora ochrony danych i stworzenie planu pracy inspektora (lub organizacji);
- Odpowiednie wsparcie finansowe, infrastrukturalne (pomieszczenia, sprzęt, wyposażenie) i kadrowe, gdy to właściwe;
- Oficjalne zakomunikowanie wszystkim pracownikom faktu wyznaczenia inspektora ochrony danych, tak aby wiedzieli o jego istnieniu oraz o pełnionych przez niego funkcjach;
- Umożliwienie dostępu do innych działów organizacji, np. HR, działu prawnego, IT, ochrony, itd., dzięki czemu inspektor ochrony danych mogą uzyskać niezbędne wsparcie, wkład lub informacje z tych innych działów;
- Ciągłe szkolenia. [Patrz punkt zatytułowany „*Formalne szkolenia i certyfikacja*"];
- W zależności od rozmiaru i struktury organizacji przydatne może być powołanie zespołu inspektora ochrony danych (inspektora i jego pracowników). W przypadku powołania takiego zespołu, jego struktura, podział i zakres obowiązków powinny zostać jasno ustalone. Również w przypadku wyznaczenia inspektora ochrony danych spoza organizacji, zespół pracowników podmiotu zewnętrznego powołany do wypełniania obowiązków związanych z ochroną danych osobowych może efektywnie wypełniać zadania inspektora, gdy wyznaczona zostanie osoba odpowiedzialna za kontakt z klientem.

> Co do zasady im bardziej skomplikowane procesy przetwarzania danych, tym więcej środków należy przeznaczyć dla inspektora ochrony danych. Ochrona danych musi być skuteczna i wymaga wystarczających zasobów, odpowiednich do zakresu przetwarzanych danych.

Jak już wspomniano, inspektorzy ochrony danych w instytucjach UE uważają, że „Inspektor ochrony danych, który musi prosić swojego bezpośredniego przełożonego o pracowników i zasoby (informatyczne, budżet na delegacje i szkolenia), może napotkać trudności, jeżeli przełożony nie będzie w pełni zaangażowany w przestrzeganie przepisów o ochronie danych". Dlatego też zalecają, by inspektor ochrony danych ponosił sam odpowiedzialność za budżet oraz by jego wnioski o dodatkowe zasoby wymagały zgody organu go mianującego (a nie bezpośredniego przełożonego)[293].

CEDPO zauważa, że:

> W złożonych organizacjach należy zastanowić się, czy inspektor ochrony danych będzie wspierany przez inne osoby z organizacji, które będą uzupełniać jego umiejętności na stałe (zespół inspektora ochrony danych) lub w razie potrzeby (zewnętrzny doradca).

W organach publicznych faktycznie zalecane byłoby stworzenie zespołu. W małych podmiotach publicznych w skład takiego zespołu mogą wchodzić po prostu obecni pracownicy regularnie spotykający się z inspektorem ochrony danych w celu omówienia istotnych spraw i opracowania polityki. W większych część pracowników może zostać formalnie przypisana do pełnienia funkcji wspierających inspektora ochrony danych na część etatu. W innych konieczne może okazać się mianowanie pełnoetatowych pracowników wspierających inspektora ochrony danych. Jak jasno wynika z wszystkich wytycznych, decyzje w tych sprawach należy podejmować, biorąc pod uwagę (i) złożoność lub wrażliwość operacji przetwarzania danych osobowych oraz (ii) rozmiar i zasoby danego podmiotu. Jednak w końcu zgodnie z RODO zasoby przydzielone inspektorowi ochrony danych (i zespołowi) muszą być odpowiednie do wykonywanych obowiązków.

Uprawnienia inspektora ochrony danych

Poza zasobami i wystarczająco silną i chronioną pozycją wyższego szczebla w organizacji inspektor ochrony danych, by wykonywać swoje obowiązki, potrzebuje także stosownych uprawnień. Art. 38(2) (zacytowany w poprzednim punkcie) wyjaśnia, że w tym celu podmiot mianujący inspektora musi zapewnić, by miał on „dostęp" do danych osobowych i operacji przetwarzania. Należy to rozumieć w

[293] Zob. punkt zatytułowany „*Pozycja inspektora ochrony danych w ramach organizacji*".

taki sam sposób, jak odpowiednie postanowienie rozporządzenia w sprawie inspektorów ochrony danych w instytucjach UE, art. 24(6) Rozporządzenia (WE) 45/2001[294]:

> Rozporządzenie wymaga, by administratorzy wspierali inspektora ochrony danych w wykonywaniu jego obowiązków oraz przekazywali informacje w odpowiedzi na pytania, a także stwierdza, że inspektor ochrony danych powinien mieć przez cały czas dostęp do danych będących przedmiotem przetwarzania, a także do wszystkich biur, instalacji przetwarzania danych i nośników danych.
>
> Chociaż inspektor ochrony danych nie posiada uprawnień egzekucyjnych w stosunku do administratorów, ma prawo monitorować przestrzeganie poprzez gromadzenie wszelkich odpowiednich danych, jakie instytucja/organ go mianujący i jego administratorzy są zobowiązani udostępnić.

Istotne są także inne komentarze inspektorów ochrony danych w instytucjach UE w odniesieniu do spoczywającego na inspektorze obowiązku zapewnienia przestrzegania zasad ochrony danych[295]:

> By wspierać inspektora ochrony danych w regularnym monitoringu, można opracować narzędzia informatyczne. Można poczynić także ustalenia administracyjne, takie jak zapewnienie, że inspektor otrzyma kopię wszelkiej korespondencji rodzącej kwestie ochrony danych oraz wymóg konsultowania z inspektorem tego typu dokumentów. Staranne, regularne monitorowanie przestrzegania oraz sprawozdawczość w zakresie wyników może wywierać na administratorów silny nacisk, by zapewnić zgodność ich operacji przetwarzania z przepisami. Regularne monitorowanie i regularna sprawozdawczość są więc najsilniejszymi narzędziami inspektora ochrony danych w procesie zapewniania przestrzegania przepisów. W tym celu dobrą praktyką jest badanie roczne/sprawozdanie roczne dla kierownictwa.

Szczególne problemy pojawiają się, gdy administrator lub podmiot przetwarzający odmawia zastosowania się do rady inspektora ochrony danych. Zdaniem Grupy Roboczej Art. 29[296]:

> W sytuacji podjęcia przez administratora lub podmiot przetwarzający decyzji niezgodnej z przepisami RODO i zaleceniami inspektora ochrony danych, inspektor powinien mieć możliwość jasnego przedstawienia swojej odrębnej opinii najwyższemu kierownictwu i osobom podejmującym decyzję. W tym zakresie art. 38(3) przewiduje, że inspektor ochrony danych „bezpośrednio podlega najwyższemu kierownictwu administratora lub podmiotu przetwarzającego". Taka bezpośrednia podległość zapewnia, że kierownictwu wyższego szczebla (np. zarządowi) znane są porady i rekomendacje inspektora ochrony danych wydawane w ramach spoczywającej na nim misji informowania i doradzania administratorowi lub podmiotowi przetwarzającemu. Innym przykładem bezpośredniej podległości jest sporządzenie raportu rocznego z działalności inspektora ochrony danych dla najwyższego kierownictwa.

Chociaż RODO nie nakłada na inspektora ochrony danych konkretnego obowiązku zgłaszania organom niezgodności z prawem, RODO przewiduje, że jest to jednym z zadań inspektora ochrony danych:

> pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, ... oraz **w stosownych przypadkach prowadzenie konsultacji** we wszelkich innych sprawach (art. 39(1)(e), pogrubienie dodane przez autorów Podręcznika)

W przypadku gdy inspektor ochrony danych uważa, że jego pracodawca działa z naruszeniem prawa, na pewno posiada prawo, a faktycznie - naszym zdaniem - obowiązek zgłoszenia tej kwestii krajowemu organowi ochrony danych w celu jej rozstrzygnięcia. Ilustruje to delikatny charakter stanowiska inspektora.

---

[294] Sieć Inspektorów Ochrony Danych Instytucji i Organów UE, Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001 (przypis 244 powyżej), str. 6 – 12. Należy zauważyć, że w przeciwieństwie do art 38(2) RODO, art. 24(6) Rozporządzenia (WE) 45/2001 nie wspomina wyraźnie dostępu do danych osobowych ani operacji przetwarzania danych. Mowa w nim jest ogólniej o zapewnieniu koniecznych zasobów. Wynika to prawdopodobnie z bardziej konkretnego i zdecydowanego postanowienia o konieczności przyznania dostępu do takich informacji (w ramach instytucji UE) Europejskiemu Inspektorowi Ochrony Danych.

[295] *Idem*.

[296] Wytyczne Grupy Roboczej Art. 29 dotyczące inspektorów ochrony danych (przypis 242 powyżej), str. 15. Takie samo podejście przyjęła Sieć Inspektorów Ochrony Danych Instytucji i Organów UE, patrz: Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001 (przypis 246 powyżej), str. 12 (zob. paragraf po cytacie w tekście powyżej).

Jednocześnie Grupa Robocza Art. 29 prawidłowo podkreśla, że[297]:

> Niezależność inspektora ochrony danych nie oznacza jednak, że posiada on uprawnienia decyzyjne wykraczające poza zadania wynikające z art. 39.
>
> Administrator lub podmiot przetwarzający są w dalszym ciągu odpowiedzialni za przestrzeganie przepisów o ochronie danych i muszą to wykazać.

Formalności

Wszystkie wyżej wspomniane wymagania itp. inspektora ochrony danych należy jasno odzwierciedlić w dokumencie prawnym, na mocy którego go mianowano. Włoski organ ochrony danych, *Garante della Privacy*, ujmuje to następująco w swoich Częstych pytaniach i odpowiedziach (FAQ) dotyczących inspektorów ochrony danych[298]:

> Art. 37(1) RODO przewiduje, że administrator danych lub podmiot przetwarzający wyznacza inspektora ochrony danych. W związku z tym istnienie instrumentu wyznaczającego inspektora ochrony danych stanowi integralną część ustaleń dotyczących wypełniania odpowiednich obowiązków.
>
> Jeżeli kandydat na inspektora jest pracownikiem, należy sporządzić doraźny instrument mianujący go na inspektora ochrony danych. Z kolei w przypadku wyboru zewnętrznego podmiotu, formalne wyznaczenie takiego podmiotu na inspektora ochrony danych stanowić będzie integralną część doraźnej umowy o świadczenie usług, jaką należy sporządzić zgodnie z art. 37 RODO (...).
>
> Bez względu na charakter i rodzaj instrumentu prawnego, musi z niego jednoznacznie wynikać, kto będzie inspektorem ochrony danych, z uwzględnieniem imienia i nazwiska inspektora, powierzonych mu zadań (które mogą wykraczać poza te przewidziane w art. 39 RODO) oraz obowiązków związanych ze wsparciem, jakie inspektor powinien udzielać administratorowi/podmiotowi przetwarzającemu zgodnie z odpowiednimi ramami prawnymi i regulacyjnymi.
>
> Jeżeli inspektorowi ochrony danych powierzane są dodatkowe zadania w stosunku do tych wstępnie wymienionych w nominującym go dokumencie, należy taki dokument lub umowę o świadczenie usług odpowiednio zmienić lub uzupełnić.
>
> Dokument nominujący i/lub umowa o świadczenie usług powinna zwięźle określać także przyczyny, dla których dana osoba fizyczna została wybrana inspektorem ochrony danych przez organ lub podmiot publiczny, by wykazać zgodność z wymogami wynikającymi z art. 37(5) RODO. W tym celu można nawiązać do wyników wewnętrznej lub zewnętrznej procedury wyboru. Specyfikacja kryteriów stosowanych przed wyznaczeniem konkretnego kandydata wskazuje nie tylko na przejrzystość i dobrą administrację, ale także stanowi element, który należy wziąć pod uwagę przy ocenie zgodności z zasadą „rozliczalności".
>
> Wyznaczywszy inspektora ochrony danych, administrator danych lub podmiot przetwarzający musi uwzględnić jego dane kontaktowe w informacji przekazywanej osobom, których dane dotyczą, a także opublikować je na odpowiedniej stronie internetowej. Przekazania takich danych zgodnie z art. 37(7) wymaga także Garante. Jeżeli chodzi o publikację na stronie internetowej, właściwe okazać może się umieszczenie danych inspektora ochrony danych w części strony dotyczącej „przejrzystości" lub „otwartości", a także ewentualnie na stronie dotyczącej polityki prywatności.
>
> Jak wyjaśniono w Wytycznych Grupy Roboczej Art. 29, imię i nazwisko inspektora ochrony danych nie musi być publikowane zgodnie z art. 37(7), jednak publikacja taka może stanowić w sektorze publicznym dobrą praktykę. Natomiast dane kontaktowe należy przekazać Garante, by ułatwić interakcję (...). Z drugiej strony dane kontaktowe inspektora ochrony danych należy przekazać osobom, których dane dotyczą, w przypadku naruszenia danych osobowych (patrz: art. 33(3)b).

2.5.4 Funkcje i zadania inspektora ochrony danych (przegląd)

[297] Wytyczne Grupy Roboczej Art. 29 dotyczące inspektorów ochrony danych, (przypis 242 powyżej), str. 15, w nawiązaniu do zasady „rozliczalności" w art. 5(2) RODO.

[298] (*Garante*, FAQs on DPOs (przypis 249 powyżej), ust. 1. *Garante* załącza do FAQ **wzór formularza nominacji [inspektora ochrony danych]**, a także **wzór formularza zgłoszenia danych inspektora ochrony danych do Garante.**

W stosunku do inspektorów ochrony danych w instytucjach UE, Europejski Inspektor Ochrony Danych (EDPS) wyróżnia **siedem funkcji**[299]:

- funkcja informowania i podnoszenia świadomości,
- funkcja doradcza,
- funkcja organizacyjna,
- funkcja współpracy,
- funkcja monitorowania przestrzegania prawa,
- funkcja obsługi zapytań i reklamacji oraz
- funkcja egzekwowania.

Inspektorzy ochrony danych mianowani na mocy RODO wykonują w znacznej mierze podobne funkcje. Są one skorelowane z zakresem bardziej szczegółowych obowiązków wskazanych w art. 39 RODO:

Artykuł 39

Zadania inspektora ochrony danych

1. Inspektor ochrony danych ma następujące zadania:

(a) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;

(b) monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk 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;

(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, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

2. Inspektor ochrony danych wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.

W praktyce inspektorzy ochrony danych w naturalny sposób będą także angażowani w określone zadania, które formalnie przypisano ich administratorowi danych, gdyż większość administratorów, wykonując takie zadania, będzie korzystać z pomocy swoich inspektorów ochrony danych (chyba że sami posiadają odpowiednie, dogłębne kompetencje poza biurem swoich inspektorów ochrony danych, np. w swoim departamencie prawnym lub departamencie zapewnienia zgodności z przepisami). W rzeczywistości, delikatnie mówiąc, w wielu przypadkach administratorzy danych w momencie natrafienia na nowe, wymagające zadania wynikające z RODO (w szczególności w ramach nowych obowiązków z zakresu rozliczalności/potwierdzenia zgodności) zlecą większość prac swoim inspektorom ochrony danych, nawet jeżeli, jak wyraźnie zostało to przewidziane w różnych aspektach w RODO, na mocy prawa to administrator, a nie inspektor ochrony danych zostanie pociągnięty do odpowiedzialności za wszelkie niepowodzenia w tym zakresie.

W szczególności art. 5(2) RODO wyjaśnia, że:

[299] EDPS, Position paper on the role of Data Protection Officers in ensuring effective compliance with Regulation (EC) 45/2001, (przypis 243 powyżej), str. 6-7.

> *Administrator* jest odpowiedzialny za przestrzeganie przepisów oraz musi być w stanie wykazać przestrzeganie [różnych zasad RODO].

Innymi słowy, odpowiedzialność ta nie spoczywa na barkach inspektora ochrony danych - co jasno wynika także z wcześniej cytowanego art. 39, który kładzie nacisk na zadania doradcze i pomocnicze inspektora.

Jednak inspektor ochrony danych odgrywa w dalszym ciągu zasadniczą rolę w tym zakresie, ponieważ poprzez swoje porady musi umożliwić najwyższemu kierownictwu oraz pracownikom niższych szczebli wypełnienie odpowiednich obowiązków. Z kolei najwyższe kierownictwo i przedstawiciele kadry zarządzającej niższego szczebla mają obowiązek konsultować z inspektorem ochrony danych wszelkie kwestie dotyczące przestrzegania postanowień RODO.

Europejski Inspektor Ochrony Danych (EDPS) przedstawił w tym celu przydatną macierz RACI („**R**esponsible, **A**ccountable, **C**onsulted, **I**nformed", czyli osoba odpowiedzialna, osoba nadzorująca, konsultant, osoba poinformowana) mającą zastosowanie w szczególności do prowadzenia rejestrów/rejestru operacji przetwarzania danych osobowych[300]:

	Osoba odpowiedzialna	Osoba nadzorująca	Konsultant	Osoba poinformowana
Najwyższe kierownictwo		**X**		
Właściciel w firmie	**X**			
Inspektor ochrony danych			**X**	
Departament informatyczny			**X**	
Podmioty przetwarzające, jeżeli dotyczy			**X**	

Dodano następujące objaśnienie terminów[301]:

> **„Odpowiedzialny"** oznacza obowiązek podjęcia działania i decyzji w celu osiągniecia wymaganych wyników. „**Nadzorujący**" oznacza odpowiedzialność za działania, decyzje i wyniki. **„Konsultant"** oznacza wnoszenie wkładu na prośbę zainteresowanej strony oraz przekazanie uwag. **„Poinformowany"** oznacza informowanie o podjętych decyzjach i procesie.

Europejski Inspektor Ochrony Danych stosuje zwrot „**właściciel w firmie**" na oznaczenie osoby odpowiedzialnej w praktyce i na co dzień za odpowiednie przetwarzanie - „właściciel" procesu. Jak wyjaśniono dalej poniżej, w punkcie zatytułowanym *„Podstawowe zadanie"*, częścią pierwszych obowiązków inspektora ochrony danych będzie odwzorowanie wewnętrznego podziału obowiązków.

Zgodnie z powyższym, w trakcie przeglądu obowiązków inspektora ochrony danych obowiązki te są często opisywane jako „pomagające administratorowi zapewnić" różne sprawy lub jako „doradzanie administratorowi" (lub odpowiedniemu „właścicielowi"/odpowiedzialnemu pracownikowi) w sprawie osiągnięcia określonych rezultatów, bardziej niż „zapewnienie" tych spraw lub dyktowanie, w jaki sposób należy się nimi zająć. W praktyce, w szczególności w małych organizacjach, może okazać się, że inspektor ochrony danych będzie sprawować większość tych funkcji we własnym zakresie, ale formalnie będą one mieściły się w zakresie odpowiedzialności administratora (i wewnętrznie odpowiedniego „właściciela"/odpowiedzialnego pracownika).

---

[300] EDPS, Accountability on the ground Part I: Records, Registers and when to do Data Protection Impact Assessments, luty 2018 r. str. 4, https://edps.europa.eu/sites/edp/files/publication/18-02-06_accountability_on_the_ground_part_1_en_0.pdf Do lewej kolumny można dodać „osoby, których dane dotyczą" oraz „organ ochrony danych" z X-ami w ostatniej kolumnie („osoba poinformowana"), ale odpowiednie obowiązki są w rzeczywistości bardziej złożone niż można byłoby to oznaczyć w ten sposób - osoby, których dane dotyczą, muszą zostać poinformowane o pewnych sprawach w wielu przypadkach (przez administratora z jego własnej inicjatywy lub na żądanie), ale nie zawsze o wszystkim, a organ ochrony danych musi w niektórych sytuacjach zostać nie tylko poinformowany, ale także należy się z nim skonsultować. W każdym przypadku macierz ma wyjaśnić sprawy w ramach organizacji administratora, a nie w podmiotach zewnętrznych.

[301] *Idem*, przypis 7 (pogrubienie dodane przez autorów Podręcznika).

Biorąc pod uwagę tego typu zastrzeżenie co do braku odpowiedzialności inspektora ochrony danych, z powyższego wnioskujemy, że istnieje piętnaście **zadań inspektora ochrony danych lub zadań, które w praktyce wymagają jego udziału** (plus *zadanie wstępne*), które można pogrupować w ramach siedmiu ustalonych przez Europejskiego Inspektora Ochrony Danych funkcji, co zostało wspomniane na początku ostatniej części niniejszego Podręcznika, tj. części trzeciej:

W tym miejscu wystarczy zauważyć, że takie funkcje i zadania są z kolei jasno i silnie związane z „**zasadą rozliczalności**" oraz powiązanymi **„zadaniami wykazania przestrzegania**" prawa, jakie nałożono na administratora i omówiono powyżej w pkt. 2.4 Podręcznika.

W kolejnej części Podręcznika (części trzeciej) przedstawimy wytyczne, w jaki sposób administrator i inspektor ochrony danych powinni te zadania wykonywać. Po pierwsze jednak, należy przypomnieć, że chociaż inspektor ochrony danych będzie mieć poważny wpływ i wkład w realizację tych zadań, nie ponosi osobistej formalnej odpowiedzialności za przestrzeganie RODO.

Oczywiście inspektor ochrony danych będzie musiał opracować strategię, by być w stanie zrealizować wszystkie zadania zgodnie z porządkiem ustalonym według lat lub półroczy, z zastrzeżeniem pewnej elastyczności w odniesieniu do wystąpienia ewentualnych niespodziewanych kwestii (takich jak nagły problem z ochroną danych lub naruszenie danych osobowych mające wpływ na organizację albo decyzja organu ochrony danych o przeprowadzeniu kontroli w organizacji).

- o – O – o -

CZĘŚĆ TRZECIA

Praktyczne wytyczne dotyczące zadań inspektora ochrony danych lub zadań wymagających w praktyce jego zaangażowania

(„Zadania inspektora ochrony danych")

W tej części Podręcznika prezentujemy praktyczne wytyczne dotyczące **zadań inspektora ochrony danych lub zadań wymagających w praktyce jego zaangażowania,** które zostały już wymienione w pkt. 2.5.4 powyżej oraz przypomniane poniżej. W skrócie będziemy stosować zwrot „Zadania inspektora ochrony danych". Jak zauważono w tym punkcie, te piętnaście zadań wynika z szerokiej listy zadań podanych w art. 39 RODO i pogrupowanych w ustalone przez Europejskiego Inspektora Ochrony Danych **siedem funkcji inspektora ochrony danych.** W różnych punktach omawiających dane zadanie przedstawiamy **przykłady** je ilustrujące w powiązaniu z faktyczną praktyką.

Zadania inspektora ochrony danych:

Zadanie wstępne:

Ustalenie zakresu środowiska administratora

Funkcje organizacyjne:

Zadanie 1: Tworzenie rejestru operacji przetwarzania danych osobowych

Zadanie 2: Przegląd operacji przetwarzania danych osobowych

Zadanie 3: Ocena ryzyka wynikającego z operacji przetwarzania danych osobowych

Zadanie 4 Radzenie sobie z operacjami, które mogą powodować „wysokie ryzyko": przeprowadzanie oceny skutków dla ochrony danych

Funkcje monitorowania przestrzegania prawa:

Zadanie 5: Powtarzanie zadań 1 - 3 (i 4) na bieżąco

Zadanie 6: Postępowanie z naruszeniem ochrony danych osobowych

Zadanie 7: Zadanie dochodzeniowe (z uwzględnieniem rozpatrywania skarg wewnętrznych)

Funkcje doradcze:

Zadanie 8: Zadanie doradcze - informacje ogólne

Zadanie 9: Wspieranie i promowanie „Ochrony danych w fazie projektowania oraz jako opcji domyślnej"

Zadanie 10: Doradzanie w sprawie zgodności oraz monitorowanie zgodności z politykami ochrony danych, postanowieniami umów pomiędzy współadministratorem a podmiotem przetwarzającym, dwoma administratorami a podmiotem przetwarzającym i administratorem a podmiotem przetwarzającym, Wiążącymi regułami korporacyjnymi i klauzulami o przekazywaniu danych

Zadanie 11: Udział w tworzeniu kodeksów postępowania i w procesie certyfikacji

Współpraca i konsultacje z organem ochrony danych:

Zadanie 12: Współpraca z organem ochrony danych

Obsługa wniosków osób, których dane dotyczą:

Zadanie 13: Obsługa wniosków osób, których dane dotyczą

Informowanie i podnoszenie świadomości:

Zadanie 14: Zadania informowania i podnoszenia świadomości

Zadanie 15: Planowanie i ocena działań Inspektora Ochrony Danych

Zadanie wstępne:

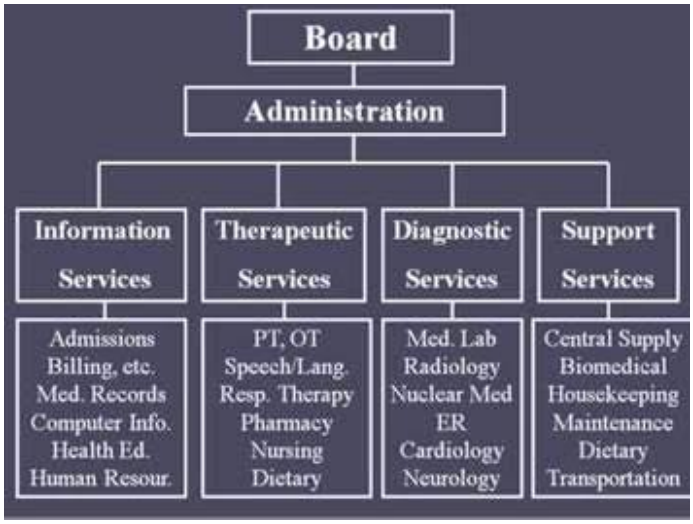
Wstępne zadanie inspektora ochrony danych - ustalenie zakresu środowiska administratora oraz szeroko pojęte odwzorowanie realizowanych przez organizację czynności przetwarzania

Inspektor ochrony danych może wykonywać swoje zadania w odniesieniu do swojego pracodawcy tylko wtedy, gdy w pełni zna (i) **wewnętrzny** podział zadań i obowiązków dotyczących przetwarzania (lub obejmujących przetwarzanie) danych osobowych, (ii) **zewnętrzne** powiazania i ustalenia danej organizacji z innymi organizacjami oraz (iii) ramy **prawne** tego procesu.

Przed podjęciem innych głównych zadań, z wyjątkiem przeprowadzenia wstępnego spisu (rejestru) operacji przetwarzania danych osobowych, wymienionych w kolejnym nagłówku (Zadanie 1), które mogą być wykonywane równolegle, inspektor ochrony danych musi odwzorować te wewnętrzne i zewnętrzne powiązania oraz linie podziału odpowiedzialności w odniesieniu do każdej i wszystkich operacji przetwarzania danych osobowych, a także umieścić je w szerszym kontekście roli i celów swojej organizacji oraz dokładnie zapoznać się z odpowiednimi zasadami.

Aby wyjaśnić struktury i role **wewnętrzne**, inspektor ochrony danych musi po pierwsze uzyskać i przeanalizować **schemat organizacyjny** swojej organizacji, który kierownictwo powinno mu przekazać.

PRZYKŁAD: Struktura organizacyjna szpitala



Źródło: *Principles of Health Science*, https://www.youtube.com/watch?v=FpQEwbAV3Qw

Legenda:

Zarząd

Administracja

Służby Informacyjne – Przyjęcia, Fakturowanie itp., Rejestry Medyczne, Informacja Komputerowa, Edukacja Zdrowotna, Zasoby Ludzkie

Służby Terapeutyczne – PT, OT, Terapia językowa, Terapia oddechowa, Farmacja, Pielęgniarstwo, Dietetyka

Służby Diagnostyczne – Laboratorium Medyczne, Radiologia, Medycyna Nuklearna, Rentgen, Kardiologia, Neurologia

Służby Wsparcia – Centralne Zaopatrzenie, Usługi biomedyczne, Sprzątanie, Utrzymanie, Dietetyka, Transport

Schematy organizacyjne zazwyczaj jednak prezentują jedynie odpowiednie jednostki i departamenty w ogólnym ujęciu - „zasoby ludzkie", „finanse i rachunkowość", „kwestie prawne", „zarządzanie klientami" itp. (a wiele organów publicznych przyjmuje terminologię podmiotów prywatnych, np. nazywając podopiecznych opieki społecznej „klientami" urzędu opieki społecznej). Stanowią one przydatny punkt wyjścia, ale niewiele ponad to. W dogłębnych rozmowach z kierownictwem wyższego szczebla, z uwzględnieniem inspektorów ds. prawnych i teleinformatycznych organizacji, oraz tam, gdzie to stosowne, biur regionalnych i krajowych, inspektor ochrony danych powinien bardziej szczegółowo wyjaśnić, za co dokładnie odpowiadają różne jednostki i departamenty, z uwzględnieniem w szczególności tego, w jakich celach każda z jednostek i każdy z departamentów potrzebuje i faktycznie przetwarza dane osobowe, jakiego rodzaju architektura technologii wewnętrznych i zewnętrznych jest

wykorzystywana oraz czy obejmuje to zewnętrzne usługi lub rozwiązania technologiczne (z uwzględnieniem chmury obliczeniowej). W tym miejscu wstępny zakres pokrywa się częściowo z przeprowadzeniem spisu operacji przetwarzania danych osobowych w Zadaniu 1. Przy czym na wstępnym etapie odpowiednie operacje przetwarzania danych osobowych należy jedynie zidentyfikować w szerokim tego słowa znaczeniu, nawiązując do celu każdej z operacji oraz zastosowanych technologii. Ponadto inspektor ochrony danych powinien na wstępie uzyskać także wstępne spojrzenie na to, jakie dokładnie **zadania** i **obowiązki** każda jednostka lub każdy departament posiada w odniesieniu do każdej operacji przetwarzania danych osobowych, tj. powinien ustalić, kto jest „**właścicielem**" każdej operacji (stosując terminologię EDPS).

PRZYKŁADY[302]**:**

Hiszpański organ ochrony danych, AEDP, podaje następujące **przykłady oficjalnych (ustawowo wymaganych) rejestrów danych osobowych prowadzonych przez władze lokalne:**

- Rejestr populacji
- Rejestr osób zobowiązanych do zapłaty lokalnych podatków
- Rejestr odbiorców świadczeń (np. świadczeń mieszkaniowych lub świadczeń dla osób niepełnosprawnych)
- Rejestr klientów usług społecznych (np. opieki społecznej dla dzieci)
- Rejestr mandatów (np. mandatów za parkowanie)
- Rejestr wydanych zezwoleń i licencji (np. na prowadzenie baru)
- Rejestr lokalnych jednostek i inspektorów policji
- Rejestr osób zarejestrowanych w lokalnym urzędzie pracy
- Rejestr dzieci objętych lokalną edukacją
- Rejestr osób, którym wydano oficjalne dokumenty (np. akty urodzenia, małżeństwa, zgonu)
- Rejestr osób pochowanych na lokalnych cmentarzach
- Rejestr użytkowników bibliotek prowadzonych przez władze lokalne
- Rejestr osób, które zgodziły się otrzymywać powiadomienia o wydarzeniach kulturalnych.

Oraz oczywiście:

- Sprawozdania
- Zasoby ludzkie
- Itp.

Organ ochrony danych podaje następujące **przykłady przepisów i rozporządzeń stanowiących podstawę przetwarzania danych osobowych w związku z niektórymi z** wyżej wymienionych **rejestrów danych osobowych prowadzonych przez hiszpańskie władze lokalne:**[303]

Rejestr:	Podstawa prawna:
• Rejestr populacji	ustawa o lokalnych rejestrach populacji
• Rejestr osób zobowiązanych do zapłaty lokalnych podatków	ustawa o lokalnych *haciendas*
• Dane zasobów ludzkich	Przepisy dotyczące tej działalności

W niektórych przypadkach mogą istnieć inne podstawy prawne przetwarzania, np.:

Rejestr:	Inne podstawy prawne:
• Rejestr osób, które zgodziły się otrzymywać powiadomienia o wydarzeniach kulturalnych	Zgoda i lokalne rozporządzenie
• Rejestr użytkowników bibliotek prowadzonych przez władze lokalne	Umowa i lokalne rozporządzenie

[302] W oparciu o: *Protección de Datos y Administración Local* (Ochrona danych a administracja lokalna) przewodnik wydany przez hiszpański organ ochrony danych, AEPD, 2017, str. 8 (tłumaczenie i edycja), https://www.aepd.es/media/guias/guia-proteccion-datos-administracion-local.pdf.

[303] AEPD, Sectoral Guide on Data Protection and Local Administration (poprzedni przypis), str. 11.

Ponadto istotne jest, że na tym etapie inspektor ochrony danych (przy pomocy pracowników działu informatycznego i bezpieczeństwa) dokładnie zapoznaje się także z **technicznymi systemami teleinformatycznymi, architekturą i politykami stosowanymi w swojej organizacji:** wykorzystywanymi komputerami (lub, jeżeli są w dalszym ciągu stosowane, ręcznymi systemami katalogowania) oraz czy obejmują one urządzenia przenośne i/lub komórkowe (i/lub osobiste „własne urządzenia" odpowiednich pracowników - do których należy stosować politykę „Bring you own device [BYOD]"); czy komputery osobiste i urządzenia są stosowane online czy tylko offline, na miejscu czy także poza biurem; jakie stosuje się oprogramowanie zabezpieczające i szyfrowanie oraz czy jest ono w pełni aktualne; jakie łącza i obiekty zewnętrzne są wykorzystywane (z uwzględnieniem serwerów chmury, w szczególności jeżeli znajdują się one poza UE/EOG, np. w USA, w którym to przypadku należy sprawdzić odpowiednie ustalenia i umowy dotyczące przekazywania danych); czy jakąkolwiek część przetwarzania realizują podmioty przetwarzające (w którym to przypadku należy przejrzeć zawarte z nimi umowy)[304]; jakie są fizyczne zabezpieczenia (drzwi, pomieszczenia, hasła do sieci i komputerów, itp.); czy wdrożono polityki bezpieczeństwa i szkolenia itp. itd. Na wstępnym etapie nie trzeba rozpatrywać i rozstrzygać tak wielu kwestii, ale należy przynajmniej je **odnotować, nakreślić i zarejestrować.**

Następnie inspektor ochrony danych powinien spróbować wyjaśnić wszystkie powiązania **zewnętrzne**, jakie jego organizacja posiada z innymi organizacjami. Z zasady istnieją **dwa typy** powiązań: (a) organizacje (siostrzane/macierzyste/córki), z jakimi organizacja inspektora ochrony danych posiada formalne powiazania zazwyczaj (w sektorze publicznym) w ramach ogólnej **struktury hierarchicznej.** Organ lokalny może formalnie bezpośrednio podlegać organowi regionalnemu, który z kolei podlega kontroli lub nadzorowi prowincjonalnego lub federalnego organu państwowego, który na najwyższym szczeblu działa w ramach ogólnokrajowej agencji publicznej podlegającej krajowemu ministerstwu. Istnieć będą jednak poważne różnice w ustaleniach w każdym kraju lub nawet w ramach kraju, z uwzględnieniem różnic dotyczących względnej autonomii różnych organów, a także w odniesieniu do ustanawiania ich operacji przetwarzania danych osobowych oraz zarządzania takimi operacjami i właśnie dlatego inspektor ochrony danych powinien dokładnie zapoznać się z konkretnymi ustaleniami dotyczącymi jego własnej organizacji.

Ramy dla wszystkich odpowiednich organów publicznych należących do określonej hierarchii zostaną w znacznej mierze określone w **formalnym prawie** na kilku poziomach: konstytucji, ustaw, instrumentów ustawowych (drugorzędnego, wiążącego orzecznictwa lub nieumocowanych ustawowo **ustaleń administracyjnych**, umów[305], wytycznych i oświadczeń dotyczących polityki itp. Przetwarzanie danych osobowych przez organizację inspektora ochrony danych może być także przedmiotem **kodeksu postępowania**, który również może przybierać wiele form. Inspektor ochrony danych powinien w pełni i szczegółowo w miarę możliwości zrozumieć takie zasady, ustalenia i kodeksy oraz procesy, poprzez które je przyjęto, stosuje się, przegląda i zmienia, w razie potrzeby przy pomocy inspektorów prawnych w swojej organizacji (i/lub poprzez udział w odpowiednich kursach, jeżeli nie posiada pełnej wiedzy w momencie objęcia stanowiska).

---

[304] Hiszpański organ ochrony danych, AEPD, w ramach wkładu w opracowanie niniejszego Podręcznika, podaje **przykłady** operacji przetwarzania, które są często zlecane przez władze lokalne podmiotom zewnętrznym (tj. w których przetwarzaniem zajmuje się podmiot przetwarzający):

- Przygotowanie list płac [*ciąg dalszy na odwrocie*]
- Niszczenie dokumentów lub nośników
- Kontrola kamer wideo
- Zarządzanie procesem pobierania podatków
- Utrzymanie sprzętu komputerowego
- Przetwarzanie danych z gminnego rejestru populacji:
- Przetwarzanie danych o podatkach gminnych:
- Przetwarzanie danych zasobów ludzkich: w odniesieniu do przepisów o służbach publicznych.
- Subskrypcja poprzez usługę oferowaną przez radę miasta na swojej stronie internetowej umożliwiającą otrzymywanie komunikatów o działalności kulturalnej.
- Zapisy się do banku pracy.

(AEDP wymienia także chmurę obliczeniową, o której była już mowa powyżej).

[305] Takie umowy mogą obejmować umowy z organami publicznymi, w ramach których jeden organ publiczny przetwarza dane osobowe w imieniu drugiego organu publicznego, tj. działa jako podmiot przetwarzający dla tego drugiego organu. Zob. dyskusja w kontekście umów zawieranych pomiędzy administratorami danych, administratorem a przetwarzającym oraz umów o przekazie danych.

W organizacji działać będą także inni inspektorzy ochrony danych należący do odpowiedniej hierarchii, a nasz inspektor ochrony danych powinien w pełni z nimi współpracować w ramach **sieci inspektorów ochrony danych.** Jeżeli taka sieć jeszcze nie istnieje, inspektor ochrony danych powinien zmierzać w kierunku jej utworzenia. Wszyscy inspektorzy ochrony danych powinni oczywiście ustanowić **bliskie i dobre powiązania z krajowym organem ochrony danych,** z uwzględnieniem pracowników wyższego szczebla w ramach tego organu odpowiedzialnych za organy publiczne/rodzaj organów publicznych, do jakiego należy organizacja danego inspektora ochrony danych.

Ustalenia poczynione przez francuski organ ochrony danych, CNIL, dla sieci krajowej inspektorów ochrony danych oparte na dedykowanym extranecie to dobry przykład wspierania tego typu sieci i interakcji przez organ ochrony danych[306].

Następnie istnieją powiązania z **zewnętrznymi organizacjami, które mieszczą się poza hierarchią organizacji inspektora ochrony danych.** Mogą one obejmować inne **organy publiczne w innej hierarchii,** na przykład mogą istnieć powiązania pomiędzy placówkami szkolnymi a instytucjami opieki społecznej albo policją lub pomiędzy władzami szkolnymi w jednym kraju a podobnymi organizacjami w innym kraju. Ponownie istnieć będą (lub powinny) **przepisy** obejmujące takie powiazania z tego typu organami lub inne **formalne, wiążące ustalenia i umowy** (takie jak ustalenia i umowy dotyczące dzielenia się danymi pomiędzy instytucjami szkolnymi a organizacjami opieki społecznej). Inspektor ochrony danych powinien uzyskać wszelkie dane dotyczące takich ustaleń za każdym razem, gdy obejmują lub mogą obejmować przetwarzanie danych osobowych oraz powinien dokonać ich przeglądu, by sprawdzić, czy właściwie odzwierciedlają, potwierdzają i wprowadzają wymagania RODO i innych właściwych krajowych przepisów i zasad o ochronie danych oraz bardziej ogólnych przepisów o prawach człowieka[307]. Inspektor ochrony danych nie może kwestionować niewystarczających przepisów lub ustaleń prawnych jako takich, ale może - i powinien - zawiadomić swojego pracodawcę i prawdopodobnie odpowiedni organ ochrony danych, że jego zdaniem dane przepisy są niewystarczające.

Czasami powiązania i współpraca pomiędzy formalnie odrębnymi podmiotami oparta jest na **nieformalnych i nieupublicznionych ustaleniach.** Jednak jest to rozwiązanie problematyczne z punktu widzenia ochrony danych.

Jak zauważyła Grupa Robocza Art. 29 w swojej opinii na temat koncepcji administratora danych i podmiotu przetwarzającego[308]:

> Notuje się rosnącą tendencję w kierunku rozróżnienia organizacyjnego w większości odpowiednich sektorów. W sektorze prywatnym podział ryzyka finansowego oraz innych rodzajów ryzyka doprowadził do bieżącej dywersyfikacji korporacyjnej, którą jedynie wspierają fuzje i przejęcia. W sektorze publicznym podobne zróżnicowanie ma miejsce w kontekście decentralizacji lub wyodrębniania departamentów tematycznych i agencji wykonawczych. W obydwu sektorach coraz większy nacisk kładzie się na rozwój łańcuchów dostawy oraz dostawy usług pomiędzy organizacjami oraz na podwykonawstwo lub zlecanie usług podmiotom zewnętrznym w celu skorzystania z korzyści specjalizacji oraz ewentualnych korzyści skali. W efekcie zauważalny jest rozwój różnych usług oferowanych przez usługodawców, którzy nie zawsze uważają się za odpowiedzialnych. Ze względu na wybory organizacyjne przedsiębiorstw (oraz ich wykonawców lub podwykonawców) odpowiednie bazy danych mogą być umieszczane w jednym lub kilku krajach w ramach Unii Europejskiej lub poza nią.

Prowadzi to do trudności związanych z podziałem odpowiedzialności oraz przypisywaniem kontroli. Grupa Robocza stwierdziła, że zaangażowane podmioty powinny zagwarantować wystarczającą jasność co do podziału odpowiedzialności oraz skutecznego przypisania (różnych form i poziomów) kontroli, co w praktyce oznacza, że podmioty te powinny ***omówić*** te sprawy, ***uzgodnić*** takie podziały odpowiedzialności i przypisaną kontrolę oraz ***zarejestrować*** to w formie **formalnego porozumienia**,

[306] Zob. pkt 2.3.3, „*Formalne szkolenie i certyfikacja*", powyżej i przypis 456 poniżej.
[307] Zob. wyrok Europejskiego Trybunału Praw Człowieka w sprawie *Copland przeciwko Zjednoczonemu Królestwu* z 3 kwietnia 2007 r., w którym Trybunał uznał, że niejasno sformułowane postanowienie w ustawie przyznającej organowi publicznemu szerokie kompetencje w pewnym obszarze (dotyczy edukacji wyższej i dalszej) nie stanowiło „prawa" w rozumieniu Europejskiej Konwencji Praw Człowieka: http://hudoc.echr.coe.int/eng?i=001-79996 (patrz w szczególności par. 47.).
[308] Grupa Robocza Art. 29, Opinion 1/2010 on the concepts of "controller" and "processor" (WP169, przyjęta 16 lutego 2010 r.) str. 6, http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf.

które może (i na żądanie oczywiście powinno) zostać przekazane właściwemu organowi ochrony danych oraz (możliwe że w uproszczonej formie) osobom, których dane dotyczą oraz opinii publicznej.

W ramach wstępnego zadania podlegającego na określaniu zakresu inspektor ochrony danych powinien ponownie **sprawdzić**, czy istnieją tego typu formalne porozumienia i, jeżeli tak jest, czy (a) naprawdę odzwierciedlają praktyczne podziały obowiązków oraz (b) w pełni spełniają wymagania RODO. W przypadku braku formalnego porozumienia inspektor ochrony danych powinien **doradzić,** aby je pilnie sporządzono (oraz powinien uczestniczyć w ich omówieniu, zawarciu i sporządzeniu). Jeżeli poczyniono jedynie nieformalne ustalenia, inspektor ochrony danych powinien **poradzić**, by zastąpiono je formalnym porozumieniem.

Co więcej, jeżeli tego typu powiązania i ustalenia z innymi podmiotami obejmują współpracę pomiędzy administratorami i/lub administratorem i podmiotem przetwarzającym, powinny zostać oparte na (zgodnymi z RODO) **umowami pomiędzy administratorami i/lub pomiędzy administratorem i podmiotem przetwarzającym**. Natomiast jeżeli tego typu powiązania i ustalenia z innymi podmiotami obejmują przekazywanie danych osobowych do krajów spoza UE/EOG (tak zwanych „krajów trzecich"), przekazywanie takie powinno być oparte na odpowiednich (zgodnych z RODO) **klauzulach o przekazie danych** (albo standardowych klauzulach zatwierdzonych przez odpowiedni organ ochrony danych lub przez Europejską Radę Ochrony Danych lub doraźnych klauzulach zgodnych z RODO).

Tam, gdzie tego typu umowy lub klauzule już istnieją, inspektor ochrony danych powinien **dokonać ich przeglądu,** by sprawdzić, czy są zgodne z RODO. Natomiast jeżeli tego typu umowy lub klauzule nie istnieją, ale powinny zostać sporządzone, inspektor ochrony danych powinien **doradzić**, by je pilnie zawarto.

Takie zadania inspektora ochrony danych związane z formalnymi porozumieniami, umowami pomiędzy administratorami oraz pomiędzy administratorem i podmiotem przetwarzającym oraz klauzulami o przekazywaniu danych (oraz w innych powiązanych obszarach) omówiono bardziej szczegółowo w pkt. 3.x. W tym miejscu wystarczy wspomnieć, że inspektor ochrony danych powinien **ustalić** te kwestie w ramach wstępnego ustalania zakresu, by później się nimi zająć.

W końcu organizacja inspektora ochrony danych będzie posiadać **powiązania z zewnętrznymi dostawcami towarów i usług (z sektora publicznego i prywatnego)**, od zleconego podmiotowi zewnętrznemu przetwarzania danych, rachunkowości i zarządzania stroną internetową po dostawy do stołówki, utrzymanie i naprawy, wsparcie medyczne i socjalne dla pracowników, itp. Wykonywana w tym zakresie praca opierać się będzie na **umowach** (zwyczajnych umowach cywilnych lub specjalnych umowach publiczno-prywatnych). Umowy takie stanowić będą podstawę (oraz powinny wyraźnie uwzględnić wszystkie aspekty) przetwarzania danych osobowych przez strony umowy, począwszy od gromadzenia odpowiednich danych poprzez ich przekazywanie i wykorzystanie aż po ich ostateczne zniszczenie lub usunięcie. Jeżeli drugi podmiot jest administratorem w swoim własnym imieniu, umowy takie (lub przynajmniej ich postanowienia dotyczące ochrony danych) będą stanowić - w kontekście ochrony danych - **zawarte pomiędzy administratorami umowy o przetwarzaniu danych osobowych** Jeżeli drugi podmiot działa jedynie jako podmiot przetwarzający dla organizacji inspektora ochrony danych, umowa będzie **umową pomiędzy administratorem a podmiotem przetwarzającym.** Jeżeli zgodnie z umową dane osobowe są przekazywane poza UE/EOG (z reguły na obsługiwany przez wykonawcę serwer „chmury"), umowy takie stanowią **umowy przekazania danych osobowych.**

Na wstępnym etapie inspektor ochrony danych powinien **ustalić**, czy istnieją tego typu umowy oraz następnie bezpośrednio po określeniu zakresu **dokonać ich przeglądu** i tam, gdzie ich brakuje lub są one niewystarczające w rozumieniu RODO, poradzić, by je sporządzono lub skorygowano.

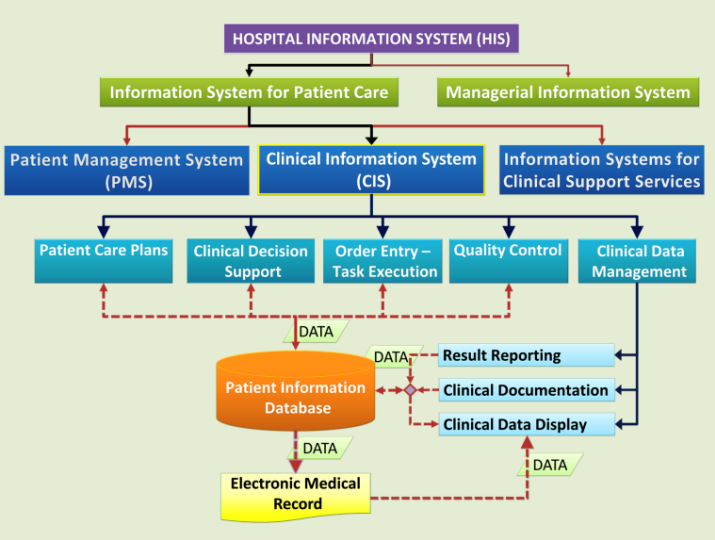
Szeroko pojęte odwzorowanie realizowanych przez organizację czynności przetwarzania

Gdy inspektor ochrony danych ustali już ogólny zakres przetwarzania danych w swojej organizacji (jak opisano powyżej), będzie w stanie sporządzić ogólny schemat czynności przetwarzania danych osobowych, jako zasadniczy krok w kierunku stworzenia szczegółowego rejestru takich czynności oraz wszystkich poszczególnych operacji przetwarzania danych osobowych wykonywanych w ramach Zadania 1. W ten sposób powinien powstać wykres podobny do tego poniżej sporządzonego przez Dr.

Abdollaha Salleha, określającego funkcjonalne elementy klinicznego systemu informacyjnego („*Functional Components of a Clinical Information System*") (który zastosowano na pierwszym szkoleniu T4DATA w prezentacji włoskiego organu ochrony danych, *Garante della Privacy*)[309].

PRZYKŁAD:

Wykres czynności przetwarzania danych osobowych organizacji [tutaj szpitala]



Źródło: Dr Abdollah Salleh, https://drdollah.com/hospital-information-system-his/

Legenda:
Szpitalny system informacyjny

System informacyjny dla pacjentów – System informacji zarządczej

System zarządzania pacjentami – System informacji klinicznej – Systemy informacyjne dla Służb wsparcia klinicznego

Plany opieki nad pacjentami – Wsparcie decyzji klinicznych – Wprowadzanie zamówień – realizacja zadań – Kontrola jakości – Zarządzanie danymi klinicznymi

DANE

Baza danych pacjentów

Sprawozdania z wyników – Dokumentacja kliniczna – Prezentacja danych klinicznych

Elektroniczny rejestr medyczny

Należy zauważyć, że powyższy wykres jest bliżej związany z operacjami przetwarzania danych osobowych niż wyżej zaprezentowany schemat organizacyjny szpitala.

[309] Luigi Carrozzi, prezentacja w trakcie pierwszej sesji szkoleniowej „T4DATA", czerwiec 2018 r., slajdy zatytułowane „*Practical Guidance for DPOs – The register of data processing operations*".

Zadania organizacyjne:

ZADANIE 1: Tworzenie rejestru operacji przetwarzania danych osobowych

Z zastrzeżeniem ograniczonego zwolnienia, które omówiono poniżej, zgodnie z art. 30 RODO każdy administrator musi prowadzić „**rejestr** czynności przetwarzania danych osobowych", za które odpowiada, obejmujący różne szczegóły każdej operacji, takie jak imię i nazwisko administratora (oraz można dodać „właściciela") operacji, cel operacji, kategorie osób, których dane dotyczą, danych osobowych i odbiorców, itp. Zadanie prowadzenia rejestru operacji przetwarzania jest blisko powiązane z omówioną w pkt. 2.2 zasadą rozliczalności poprzez ułatwienie skutecznego nadzoru ze strony odpowiedniego organu ochrony danych („organu nadzorczego"), jak podkreślono w motywie (82) RODO[310]:

> ***Dla zachowania zgodności*** z niniejszym rozporządzeniem, administrator lub podmiot przetwarzający **powinni prowadzić rejestry czynności przetwarzania**, za które są odpowiedzialni.
>
> 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.

Innymi słowy, jak ujmuje to włoski organ ochrony danych, *Garante*[311]*:*

> **Rejestr stanowi rozwiązanie pozwalające wykazać przestrzeganie RODO.**

Odwołanie do „operacji przetwarzania leżących w gestii (administratora)" sugeruje, że rejestr taki musi obejmować **wszystkie** tego typu operacje przetwarzania, co faktycznie wyraźnie przewidziano w niemieckiej wersji RODO[312]. Ma to także sens, ponieważ, jak podkreśla *Garante*[313]:

> Wynikający z rejestru ogólny obraz aktywów informacyjnych, „danych osobowych", oraz powiązanej operacji przetwarzania stanowi **pierwszy krok do stosowania zasady rozliczalności,** ponieważ umożliwia ocenę zagrożenia dla praw i wolności jednostek oraz wdrożenie odpowiednich środków technicznych i organizacyjnych mających zapewnić odpowiadający takiemu zagrożeniu poziom bezpieczeństwa.

Chociaż, podobnie jak w przypadku większości innych wymogów RODO, jest to formalnie zadanie administratora, nie zaś inspektora ochrony danych, w praktyce to inspektor ochrony danych będzie odpowiedzialny za realizację tych zadań (w bliskiej współpracy z odpowiednimi pracownikami administratora) albo będzie przy najmniej w nie mocno zaangażowany i będzie je nadzorować. Jak ujmuje to Grupa Robocza Art. 29[314]:

> W praktyce często to inspektor ochrony danych tworzy i prowadzi powyższe rejestry w oparciu o dane otrzymane od różnych departamentów organizacji odpowiedzialnych za przetwarzanie danych osobowych. Taka procedura została ustalona na mocy wielu obowiązujących przepisów państw członkowskich i przepisów o ochronie danych osobowych mających zastosowanie do instytucji i organów UE[315].
>
> Artykuł 39(1) określa minimalną listę zakresu obowiązków inspektora ochrony danych. W związku z tym nic nie stoi na przeszkodzie, aby administrator lub podmiot przetwarzający powierzył inspektorowi prowadzenie, w imieniu administratora albo podmiotu przetwarzającego, rejestru czynności przetwarzania danych. Taki rejestr powinien być uznany za jedno z narzędzi umożliwiających inspektorowi ochrony danych realizację jego zadań w zakresie monitorowania przestrzegania przepisów, informowania administratora lub podmiotu przetwarzającego i doradzania im.

---

[310] Luigi Carrozzi, prezentacja w trakcie pierwszej sesji szkoleniowej „T4DATA", czerwiec 2018 r. slajdy zatytułowane „Practical Guidance for DPOs – The register of data processing operations".
[311] *Idem*.
[312] "*Jeder Verantwortliche und gegebenenfalls sein Vertreter führen ein Verzeichnis **aller Verarbeitungstätigkeiten**, die ihrer Zuständigkeit unterliegen.*" (podkreślenie dodane przez autorów Podręcznika).
[313] Luigi Carrozzi (przypis 236 powyżej) (podkreślenie oryginalne).
[314] Wytyczne Grupy Roboczej Art. 29 dotyczące inspektorów ochrony danych (przypis 242 powyżej), ust. 4.4 (*Rola inspektora ochrony danych w rejestrowaniu czynności przetwarzania)* str. 18.
[315] Art. 24(1)(d) Rozporządzenia (WE) 45/2001 [oryginalny przypis].

> Niezależnie od powyższego, rejestr prowadzony zgodnie z art. 30 powinien umożliwić administratorowi i organowi nadzorczemu (na wniosek) kontrolę wszystkich procesów przetwarzania danych w danej organizacji. Jest zatem warunkiem niezbędnym w celu zapewnienia zgodności i przydatnym narzędziem przy rozliczalności.

W przypadku nowego inspektora ochrony danych wymaga to, po pierwsze (nadzorowanie) sporządzenia **spisu** wszystkich operacji przetwarzania w organizacji, które mogą obejmować przetwarzanie danych osobowych oraz powiązań z innymi organizacjami. Wymaga to rozważenia, o jakie tu chodzi - co nie zawsze jest proste[316].

Wstępny, podstawowy spis można przygotować w tym samym czasie, gdy ustalany jest szerszy zakres organizacji oraz jej kontekst operacyjny w ramach wyżej opisanego wstępnego zadania (Zadanie 0). Z zastrzeżeniem niżej opisanego zwolnienia, kolejnym krokiem powinno być sporządzenie ***pełnego spisu*****.**

Pełny spis powinien prowadzić do stworzenia **rejestru** (zbioru **rejestrów**) wszystkich realizowanych przez administratora operacji przetwarzania danych osobowych, o których mowa w art. 30 (omówionym poniżej w części zatytułowanej *„Zawartość i struktura wpisów w rejestrze*", który powinien być następnie (oraz po przeglądzie i ocenie wspomnianej w Zadaniu 2 i 3) aktualizowany przez inspektora ochrony danych (lub inspektor ochrony danych powinien przynajmniej zapewnić jego aktualność) - patrz tekst poniżej w części zatytułowanej „(*bieżące) Monitorowanie zgodności"* po Zadaniu 4.

Zwolnienie:

Art. 30(5) zwalnia **przedsiębiorców lub podmioty zatrudniające mniej niż 250 osób i przetwarzające dane osobowe jedynie sporadycznie**[317], z obowiązku prowadzenia rejestru swoich operacji przetwarzania danych osobowych. Jednak zwolnienie to nie ma zastosowania, jeżeli:

- przetwarzanie realizowane przez takie przedsiębiorstwo lub taki podmiot *„może powodować **ryzyko naruszenia praw lub wolności osób, których dane dotyczą**"* (należy zauważyć, że nie musi to być „wysokie ryzyko", takie jak ryzyko uruchamiające potrzebę przeprowadzenia oceny skutków dla ochrony danych (Zadanie 4) - wszelkie ryzyko dla praw i wolności osób, których dane dotyczą, nawet małe, wymagałoby zarejestrowania (i przeanalizowania) operacji administratora;
- przetwarzanie nie ma charakteru **sporadycznego** lub
- przetwarzanie obejmuje **wrażliwe dane lub dane dotyczące wyroków skazujących i naruszeń prawa**.

Jeżeli chodzi o dwa pierwsze warunki, w kontekście oceny skutków dla ochrony danych (która będzie konieczna, gdy istnieje prawdopodobieństwo wysokiego ryzyka dla praw i wolności osób fizycznych - patrz Zadanie 4), Grupa Robocza Art. 29 opisuje „**ryzyko**" jako[318]:

> scenariusz opisujący wydarzenie i jego [negatywne] konsekwencje szacowane pod względem stopnia wagi zdarzenia i prawdopodobieństwa,

oraz wyjaśnia, że[319]:

> odniesienie do „**praw i wolności"** osób, których dane dotyczą, dotyczy przede wszystkim prawa do prywatności, ale może także obejmować inne podstawowe prawa, takie jak wolność słowa, wolność myśli, swoboda przemieszczania się, zakaz dyskryminacji, prawo do wolności, sumienia i religii.

[316] Zobacz Opinię 4/2007 Grupy Roboczej Art. 29 w sprawie pojęcia danych osobowych (WP136), przyjęta w dniu 20 czerwca 2007 r. zob. link: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf.
[317] Naszym zdaniem warunek, że mały podmiot musi przetwarzać dane osobowe sporadycznie wynika z (omówionego w tekście Podręcznika) postanowienia, że zwolnienie to nie ma zastosowania, jeżeli przetwarzanie przez małe podmioty nie ma „sporadycznego charakteru".
[318] Wytyczne Grupy Roboczej Art. 29 dotyczące oceny skutków dla ochrony danych (przypis 351 poniżej), str. 6.
[319] *Idem*, pogrubienie dodane przez autorów Podręcznika.

W kwietniu 2018 r. Grupa Robocza Art. 29 wydała Stanowisko w sprawie art. 30 ust. 5 RODO[320], w którym podkreślono, że:

> brzmienie art. 30 ust. 5 jasno stanowi, że trzy rodzaje przetwarzania, do których wyłączenia nie mają zastosowania, są alternatywne („lub"), a wystąpienie któregokolwiek z nich samodzielnie pociąga za sobą obowiązek prowadzenia rejestru przetwarzania zajęcia.
>
> Dlatego administratorzy danych lub podmioty przetwarzające, chociaż dysponują mniej niż 250 pracownikami, mogą przetwarzać dane, co może spowodować ryzyko (nie tylko wysokie) dla praw osób, których dane dotyczą, lub przetwarzać dane osobowe sporadycznie lub przetwarzając specjalne kategorie danych zgodnie z art. 9 ust. 1 lub dane dotyczące wyroków skazujących na podstawie art. 10 są zobowiązane do prowadzenia rejestru czynności przetwarzania. Organizacje takie muszą jednak prowadzić rejestr czynności przetwarzania tylko dla rodzajów przetwarzania wymienionych w art. 30 ust. 5. Na przykład mała organizacja prawdopodobnie będzie regularnie przetwarzać dane dotyczące swoich pracowników. W związku z tym takiego przetwarzania nie można uznać za „sporadyczne", dlatego należy je włączyć do rejestru czynności przetwarzania[321]. Inne działania związane z przetwarzaniem, które w rzeczywistości są „sporadyczne", nie muszą być jednak uwzględniane w rejestrze działań związanych z przetwarzaniem, pod warunkiem, że jest mało prawdopodobne, aby powodowały ryzyko dla praw i wolności osób, których dane dotyczą, i nie obejmowały specjalnych kategorii dane [tak zwane „dane szczególnie chronione"] lub dane osobowe związane z wyrokami skazującymi i przestępstwami.

Przykład:

W **Chorwacji** szczegółowe informacje dotyczące służb cywilnych i pracowników organów publicznych należy na mocy prawa przesłać do centralnego systemu zwanego rejestrem pracowników sektora publicznego. Wymóg ten ma zastosowanie także w odniesieniu do najmniejszych podmiotów publicznych, takich jak małe lokalne gminy, które mogą zatrudniać niewiele osób. Przetwarzanie danych tych kilku pracowników przez bardzo małą gminę nie ma więc „okazjonalnego" charakteru i nie podlega zwolnieniu z obowiązku prowadzenia rejestru.

W razie wątpliwości w tych sprawach administrator powinien skorzystać z porady inspektora ochrony danych, a inspektor ochrony danych powinien opowiedzieć się za stworzeniem w marginalnych przypadkach pełnego rejestru, a nie ryzykować, że organizacja zostanie posądzona o naruszenie zadań przewidzianych w art. 30(1) - (4).

Uwagi:

1. By odpowiedzieć na pytanie, czy rejestr operacji przetwarzania danych osobowych musi być dostępny dla każdego (online lub w inny sposób), czy też nie, zob. Zadanie 12 *„Zadania informowania i podnoszenia świadomości".*
2. Tworzenie rejestru jako takiego nie obejmuje jeszcze oceny zgodności zarejestrowanych operacji z RODO. Odbywa się to w ramach Zadania 2, ale oczywiście rejestr powinien zostać zmieniony i zaktualizowany, gdy i kiedy mają miejsce zmiany w zarejestrowanych w nim operacjach przetwarzania - patrz *„Monitorowanie przestrzegania prawa: powtarzanie Zadań 1 - 3 (i 4) na bieżąco* na końcu Zadania 4 (tuż przed Zadaniem 5).

Zawartość i struktura zapisów w rejestrze:

RODO wyróżnia rejestry administratorów i podmiotów przetwarzających.

Zawartość i struktura zapisów w rejestrze administratora

[320] Dokument Grupy Roboczej Art. 29, przedstawiający stanowisko w sprawie odstępstw od obowiązku prowadzenia rejestrów czynności przetwarzania zgodnie z art. 30 ust. 5 RODO, 19 kwietnia 2018 r. dostępny pod adresem: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=624045. Dokument ten nie został wyraźnie potwierdzony przez Europejską Radę Ochrony Danych, kiedy poparł szereg bardziej formalnych „Opinii" Grupy Roboczej Art. 29 (EDPB, Zatwierdzenie 1/2018, zob. Przypis 248 powyżej), ale można go uznać za miarodajny w tej kwestii.

[321] Grupa Robocza Art. 29 uważa, że działanie związane z przetwarzaniem można uznać za „sporadyczne" tylko wtedy, gdy nie jest ono przeprowadzane regularnie i ma miejsce poza zwykłą działalnością lub działalnością administratora lub podmiotu przetwarzającego. Zobacz wytyczne Grupy Roboczej Art. 29 dotyczące art. 49 rozporządzenia 2016/679 (WP262). [oryginalny przypis]

Zgodnie z art. 30(1) RODO **rejestr** operacji przetwarzania danych osobowych *administratora* musi obejmować zbiór wpisów dotyczących każdej operacji, a każdy wpis musi obejmować następujące informacje (zwroty w nawiasach kwadratowych i pochyłą czcionką dodano):

a. imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także gdy ma to zastosowanie – przedstawiciela administratora oraz inspektora ochrony danych;

b. cel przetwarzania;

c. opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych [*z uwzględnieniem informacji, czy którekolwiek z tych danych znalazły się w spisie „szczególnych kategorii danych"/wrażliwych danych*];

d. kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;

e. gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49(1) akapit drugi, dokumentacja odpowiednich zabezpieczeń;

f. jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;

g. jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32(1).

Wykaz ten nie uwzględnia **podstawy prawnej** przetwarzania odpowiednich danych (art. 6 w odniesieniu do niewrażliwych danych, art. 9 w odniesieniu do wrażliwych danych), ani instrumentów prawnych stosowanych w umowach z podmiotami przetwarzającymi lub do przekazywania danych, ale są to tak zasadnicze kwestie w związku z ustaleniem legalności i zgodności z RODO każdej operacji przetwarzania, że należałoby je uwzględnić w rejestrze w odniesieniu do każdej operacji przetwarzania danych osobowych (definiowanej poprzez odwołanie do celu przetwarzania), z uwzględnieniem należytej weryfikacji ważności rzekomej i odnotowanej podstawy prawnej.

PRZYKŁADOWY FORMAT PODSTAWOWEGO REJESTRU PRZETWARZANIA DANYCH ADMINISTRATORA[322]

Należy zauważyć, że dla każdej odrębnej operacji należy stworzyć osobny wpis.

Część 1 - Informacje na temat administratora, itp.

DANE KONTAKTOWE **ADMINISTRATORA**: Imię i nazwisko, adres, e-mail, telefon
DANE KONTAKTOWE **WSPÓŁADMINISTRATORA***: Imię i nazwisko, adres, e-mail, telefon
DANE KONTAKTOWE **PRZEDSTAWICIELA***: Imię i nazwisko, adres, e-mail, telefon
(*) *Jeżeli dotyczy*
DANE KONTAKTOWE **INSPEKTORA OCHRONY DANYCH**: Imię i nazwisko, adres, e-mail, telefon

Część 2 - Podstawowe informacje na temat operacji przetwarzania danych osobowych[323]

[322] Poszerzony na podstawie szablonu przedstawionego przez Carrozziego (przypis 236 powyżej) z uwzględnieniem edycji (np. w formacie portretu, a nie panoramy) oraz dodanych wpisów dotyczących nazwy operacji, podstawy prawnej przetwarzania, odpowiednich zabezpieczeń przekazu danych i szczegółów dotyczących technologii i bezpieczeństwa (zgodnie z dalszymi rekomendacjami Carrozziego).
UWAGA: Przykładowy format bardziej szczegółowego (15-stronicowego) rejestru przetwarzania danych osobowych załączono po omówieniu niniejszego zadania.

[323] Powyższy przykładowy schemat ma na celu jedynie ogólnie zilustrować wymagania dotyczące rejestrowania. **Przykładowy szczegółowy rejestr przetwarzania danych osobowych,** o którym mowa w poprzednim przypisie i który załączono do tego zadania, wymaga istotnych dodatkowych szczegółów, np. dla każdej z kategorii danych osobowych - celu, znaczenia i źródła danych, itp.

1. Nazwa operacji przetwarzania danych osobowych[324]	
2. Odpowiedzialna jednostka („właściciel")	
3. Cel operacji przetwarzania danych osobowych	
4. Kategorie osób, których dane dotyczą	
5. Kategorie danych osobowych	
6. Czy obejmuje to wrażliwe dane?	
7. Podstawa prawna przetwarzania*: * Zob.: art. 6 RODO - niewrażliwe dane, art. 9 - wrażliwe dane	
8. Czy dane będą przekazywane do kraju trzeciego lub organizacji międzynarodowej?	
9. W przypadku przekazywania danych, o którym mowa w drugim paragrafie art. 49(1) RODO, czy istnieją właściwe zabezpieczenia?	
10. Terminy usunięcia	
11. Dane systemów, aplikacji i procesów (katalogi papierowe/elektroniczne; desktop suite/centralnie zarządzana aplikacja/usługa w chmurze/lokalna sieć; transmisje danych, itp.) oraz powiązane środki (zabezpieczenia) techniczne i organizacyjne	
12. Czy przetwarzanie obejmuje wykorzystanie podmiotu przetwarzającego? Jeśli tak, podaj pełne dane i kopię odpowiedniej umowy (umów).	

[324] Z perspektywy prawa ochrony danych każdą operację przetwarzania danych osobowych najlepiej zdefiniować na podstawie celu, jakiemu służy (zgodnie z pkt 2). Jednak w wielu organizacjach ludzie wykonujący takie operacje będą często posiadać ich konkretną nazwę funkcjonalną/wewnętrzną, chociaż te dwa oznaczenia będą się oczywiście zazębiać i mogą być identyczne.

Zawartość i struktura zapisów w rejestrze podmiotu przetwarzającego[325]

Zgodnie z art. 30(1) RODO **rejestr** operacji przetwarzania danych osobowych *podmiotu przetwarzającego* musi obejmować zbiór **wpisów** dotyczących każdej operacji, a **każdy wpis musi obejmować następujące informacje:**

a. imię i nazwisko lub nazwę oraz dane kontaktowe podmiotu przetwarzającego lub podmiotów przetwarzających oraz każdego z administratorów, w imieniu którego podmiot przetwarzający działa, a także gdy ma to zastosowanie przedstawiciela administratora lub podmiotu przetwarzającego oraz inspektora ochrony danych;

b. kategorie operacji przetwarzania realizowanych w imieniu każdego administratora;

c. gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49(1) akapit drugi, dokumentacja odpowiednich zabezpieczeń;

d. jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32(1).

Poniżej ponownie przedstawiamy przykładowy format rejestru, jaki podmiot przetwarzający powinien prowadzić, by spełnić wyżej opisane wymagania.

PRZYKŁADOWY FORMAT PODSTAWOWEGO REJESTRU PRZETWARZANIA DANYCH PODMIOTU PRZETWARZAJĄCEGO[326]

Należy zauważyć, że dla każdej odrębnej operacji dla każdego odrębnego administratora należy stworzyć osobny wpis.

Część 1 - Informacje na temat podmiotu przetwarzającego i podwykonawcy (podwykonawców) przetwarzania

DANE KONTAKTOWE **PODMIOTU PRZETWARZAJĄCEGO**: Imię i nazwisko, adres, e-mail, telefon
DANE KONTAKTOWE **INSPEKTORA OCHRONY DANYCH**: Imię i nazwisko, adres, e-mail, telefon
DANE KONTAKTOWE **PODWYKONAWCY PRZETWARZANIA**: Imię i nazwisko, adres, e-mail, telefon
DANE KONTAKTOWE **INSPEKTORA OCHRONY DANYCH**: Imię i nazwisko, adres, e-mail, telefon
DANE KONTAKTOWE **PODWYKONAWCY PRZETWARZANIA**: Imię i nazwisko, adres, e-mail, telefon
DANE KONTAKTOWE **INSPEKTORA OCHRONY DANYCH**: Imię i nazwisko, adres, e-mail, telefon

* *Jeżeli dotyczy*

[325] Należy zauważyć, że coraz trudniej jest w pełni odróżnić podmioty przetwarzające od administratorów. Często podmioty, które świadczyły bezpośrednie usługi przetwarzania (działając na zlecenie administratora, który ustalał środki i cele), obecnie przyjmują na siebie znacznie większe obowiązki i mogą stać się „współadministratorami". Dzieje się tak szczególnie w przypadku dostawców usług w chmurze, z których część oferuje nawet „*Sztuczną inteligencję i uczenie maszynowe (AI/ML) poprzez usługę Machine-Learning-as-a-Service (MLaaS)*", zob. http://www.techmarketview.com/research/archive/2018/04/30/machine-learning-as-a-service-market-overview-technology-prospects. Jak opisano w ramach *Wstępnego zadania*, ustalenia pomiędzy podmiotami uczestniczącymi w takich złożonych ustaleniach powinny być jasno i właściwie odnotowane. Formularze zawierające zapis odpowiednich operacji przetwarzania należy analizować i zmieniać, by dopasować je do takich (uzgodnionych i spisanych) ustaleń pomiędzy podmiotami. Podmioty, które są czymś więcej niż po prostu podmiotami przetwarzającymi, powinny korzystać ze szczegółowego formularza, o którym mowa w następnym przypisie.

[326] Ponownie poszerzony w stosunku do szablonu przedstawionego przez Carrozziego (przypis 236 powyżej) z uwzględnieniem edycji.

Część 2 - Informacje na temat administratora konkretnej operacji przetwarzania danych

DANE KONTAKTOWE **ADMINISTRATORA**: Imię i nazwisko, adres, e-mail, telefon
DANE KONTAKTOWE **WSPÓŁADMINISTRATORA***: Imię i nazwisko, adres, e-mail, telefon
DANE KONTAKTOWE **PRZEDSTAWICIELA***: Imię i nazwisko, adres, e-mail, telefon
(*) ***Jeżeli dotyczy***
DANE KONTAKTOWE **INSPEKTORA OCHRONY DANYCH**: Imię i nazwisko, adres, e-mail, telefon

Uwaga: Relacje pomiędzy administratorem a podmiotem przetwarzającym oraz pomiędzy podmiotem przetwarzającym a podwykonawcą przetwarzania muszą być oparte na pisemnej umowie zgodnej z wymogami art. 28 RODO. Podmioty przetwarzające powinny zachować kopie odpowiednich umów wraz z wypełnionym formularzem.

Część 3 - Szczegóły operacji przetwarzania danych osobowych

1. Kategoria (rodzaj) przetwarzania, jakie jest realizowane na rzecz administratora w związku z ogólną operacją przetwarzania danych, w tym:	
- kategorie osób, których dane dotyczą;	
- kategorie danych osobowych oraz	
- informacja, czy obejmuje to wrażliwe dane.	
2. Czy dane będą przekazywane do kraju trzeciego lub organizacji międzynarodowej?	
3. W przypadku przekazywania danych, o którym mowa w drugim paragrafie art. 49(1) RODO, jakie właściwe zabezpieczenia zapewniono?	
4. Dane systemów, aplikacji i procesów (rodzaj katalogów elektronicznych; desktop suite/centralnie zarządzana aplikacja/usługa w chmurze/lokalna sieć; transmisje danych, itp.) oraz powiązane środki (zabezpieczenia) techniczne i organizacyjne	
5. Czy przetwarzanie wiąże się z wykorzystaniem podwykonawcy podmiotu przetwarzającego? Jeśli tak, podaj pełne dane i	

kopię odpowiedniej umowy (umów).	

Zawartość i struktura rejestru:

Inspektor ochrony danych powinien skonstruować **rejestr** w oparciu o wpisy, jakie otrzymuje w odniesieniu do każdej odrębnej operacji przetwarzania danych osobowych. Z reguły najlepiej posortować je według **organizacji** oraz w ramach organizacji według **właścicieli.** Dla każdego z wpisów inspektor ochrony danych powinien posiadać całą odpowiednią dokumentację (wskazaną w szablonach formularzy).

Inspektor ochrony danych powinien odnotować w rejestrze, kiedy każdy z wpisów otrzymano, kiedy dana operacja przetwarzania była przedmiotem przeglądu (w ramach niżej opisanego Zadania 2), jaki był rezultat takiego przeglądu oraz jakie środki naprawcze podjęto, a także wskazać termin kolejnego przeglądu (np. rocznego).

- o – O – o -

Załączono: Przykładowy format szczegółowego rejestru przetwarzania danych osobowych[327].

[327] Bardziej szczegółowy wzór rejestru danych osobowych opublikował także polski organ ochrony danych - Urząd Ochrony Danych Osobowych (UODO) - na swojej stronie internetowej w języku polskim, https://uodo.gov.pl/pl/123/214 (pierwszy link na dole strony).

Załącznik:

PRZYKŁADOWY FORMAT SZCZEGÓŁOWEGO REJESTRU CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH

Dla każdej odrębnej operacji przetwarzania danych osobowych należy zastosować osobny formularz.

UWAGA: Jeżeli istnieje konieczność doprecyzowania lub wyjaśnienia jakiejś sprawy, należy dodać numer w odpowiednim polu i załączyć stronę z odpowiednimi danymi lub objaśnieniami, z uwzględnieniem odwołania do tego numeru.

I. OGÓLNE: * oznacza pola obowiązkowe (jeżeli dotyczy)

Administrator danych: (Główny administrator danych)* (Nazwa, siedziba i adres, numer wpisu w rejestrze, itp.)	
Podmioty powiązane (Wszystkie podmioty, z którymi administrator danych jest powiązany w związku z tą operacją, np. spółki matki/córki lub powiązane organy publiczne; podmioty przetwarzające uczestniczące w danej operacji)	
Jednostka organizacyjna: („Właściciel")* (np. ZL, Księgowość, Prace badawczo-rozwojowe, Sprzedaż, Wsparcie Klienta)	
Osoba kontaktowa w jednostce:	
PODSTAWOWY CEL CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH*: *Możliwie najbardziej precyzyjne określenie*	
Czy dane osobowe są wykorzystywane lub ujawniane w innym (drugorzędnym) celu?* ***Możliwie najbardziej precyzyjne określenie oraz link lub odwołanie do powiązanego rejestru.***	
Czy dana czynność wykonywana jest dla wszystkich podmiotów powiązanych w podobny sposób? Lub osobno i/lub inaczej dla różnych podmiotów?* ***Należy określić.*** ***Jeżeli czynności są różne dla różnych podmiotów, należy dla każdego z nich wypełnić osobny formularz.***	
Ogólnie, z iloma osobami fizycznymi (osobami, których dane dotyczą) organizacja jest powiązana (jeżeli znane)?*	[*Należy podać liczbę lub wpisać „nieznana"*]
Data przedłożenia niniejszego formularza inspektorowi ochrony danych*:	
Przegląd formularza i czynności przetwarzania przez inspektora ochrony danych:	[*tak/nie i data - wprowadza inspektor ochrony danych*]
Termin weryfikacji/aktualizacji formularza:	[*określa inspektor ochrony danych]*

II. SZCZEGÓŁY CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH

II.1 Dane i źródła danych [Uwaga: Wszystkie pola są obowiązkowe (jeżeli dotyczy), chyba że wskazano inaczej]

1. Jakie dane osobowe lub kategorie danych osobowych są gromadzone i wykorzystywane w ramach danej czynności?	*Zaznacz V tam, gdzie to stosowne:*	**Kiedy, jak i od kogo dane uzyskano?** **Np.** (osoba, której dane dotyczą) - DWP, po zatrudnieniu osoby - osoba, której dane dotyczą, po zapisie na badania
- Imię i nazwisko (nazwiska)		
- Data urodzenia:		
- Adres domowy		
- Służbowy numer telefonu		
- Prywatny numer telefonu		
- Służbowy adres poczty elektronicznej		
- Prywatny adres poczty elektronicznej		
Dodatkowe dane należy uzupełnić poniżej, jeżeli dotyczy*: ** Patrz także poniżej, pkt 2, wrażliwe dane*		
W razie potrzeby należy dodać kolejne wiersze		
2. Czu gromadzone dane i rejestr czynności <u>uwzględnia lub pośrednio ujawnia</u> którekolwiek z następujących szczególnych kategorii danych osobowych („wrażliwe dane")?	*Wpisz V jeżeli dane są wyraźnie gromadzone i wykorzystywane dla celów danej czynności; Wpisz V i dodaj („pośrednio") jeżeli dane są pośrednio ujawniane (w razie potrzeby wyjaśnij w notatce)*	**Kiedy i od kogo takie dane uzyskano?** **Np.** (osoba, której dane dotyczą) - DWP, po zatrudnieniu osoby - osoba, której dane dotyczą, po zapisie na badania
- Pochodzenie rasowe lub etniczne		
- Poglądy polityczne lub przynależność polityczna		
- Poglądy religijne lub filozoficzne		
- Członkostwo w związkach zawodowych		
- Dane genetyczne		
- Dane biometryczne		
- Dane dotyczące stanu zdrowia		

- Dane dotyczące orientacji seksualnej lub życia intymnego		
- Informacje o wyrokach karnych lub wykroczeniach		
- Identyfikator krajowy* * Np. numer ubezpieczenia, NIP		
- Dane o zadłużeniu/ocenie kredytowej		
- Dane dotyczące małoletnich		
3. Jeżeli wiadomo lub ustalono: Jak długo są (szczególne i inne) dane zatrzymywane? Co się dzieje potem?* * Należy podać okres lub zdarzenie, np.: „7 lat" lub „do 5 lat po rozwiązaniu stosunku pracy". Należy także wyjaśnić, co się dzieje z danymi, np. usunięcie/zniszczenie lub anonimizacja. **UWAGA: W przypadku stosowania różnego okresu zatrzymania w odniesieniu do różnych danych, należy taką informację podać.**		

II.2 Ujawnianie danych

4. Które z powyższych danych są ujawnianie którym stronom trzecim? I w jakich celach? **UWAGA: Dotyczy to także danych udostępnianych w szczególności bezpośrednio, internetowo.** **Zob.: ujawnienie obejmujące przekazanie do krajów trzecich, pkt II.5 poniżej.**	**Odbiorca, miejsce i kraj ustanowienia:**	**Cele ujawnienia:**
WSZYSTKIE DANE PODANE W II.1		
***LUB:* Następujące dane:** (Należy skopiować dane z 1 i 2 powyżej)		
-		
-		
-		
-		
-		
-		
-		
-		
-		
-		
-		
-		
-		
-		
-		
-		
-		
-		
-		

W razie potrzeby należy dodać kolejne wiersze		

II.3 Podstawa prawna przetwarzania

5. Na jakiej podstawie prawnej dane są przetwarzane? **UWAGA: W przypadku różnych podstaw prawnych dla różnych danych lub w różnych celach (podstawowym, drugorzędnym lub nowym, niepowiązanym) należy taką informację podać (w razie potrzeby poprzez skopiowanie i wklejenie listy danych z powyższych punktów poniżej wraz z przeniesieniem różnych podstaw prawnych do drugiej kolumny).**	*Zaznacz odpowiednią podstawę prawną i w stosownym przypadku dodaj objaśnienie w następnej kolumnie.*	**Objaśnienie:**
- Osoba, której dane dotyczą wyraziła zgodę na przetwarzanie **UWAGA: Patrz także pytania 6-9 poniżej.**		
- Przetwarzanie jest konieczne dla celów umowy pomiędzy Państwa organizacją a osobą, której dane dotyczą (lub w celu podjęcia działań na życzenie osoby, której dane dotyczą, przed zawarciem umowy, np. w celu uzyskania referencji)		
- Przetwarzanie jest niezbędne do zapewnienia zgodności z obowiązkiem prawnym, któremu podlega Państwa organizacja* Np. przepisy o zatrudnieniu lub prawo podatkowe - *należy podać odpowiednie prawo/przepis*		
- Przetwarzanie jest konieczne dla ochrony żywotnych interesów osób, których dane dotyczą, lub innych osób		
- Przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym* ** Należy określić źródło zadania (z reguły prawo)*		
- Przetwarzanie jest wykonywane w ramach funkcji organu publicznego ** Należy określić źródło zadania (z reguły prawo)*		
- Przetwarzanie jest konieczne w uzasadnionym interesie Państwa organizacji (lub innego podmiotu), nad którym nie przeważają interesy osób, których dane dotyczą. Np. marketing adresowany do własnych klientów lub zapobieganie oszustwom - należy wymienić.		

ZGODA - dodatkowe szczegóły:	
6. Jeżeli dane są przetwarzane na podstawie zgody osób, których dane dotyczą, w jaki sposób i kiedy taka zgoda jest uzyskiwana? **UWAGA: Jeżeli zgoda jest wydawana na papierze lub w formie elektronicznej, należy przedstawić kopię odpowiedniego tekstu/link.**	
7. Jakie dowody wyrażenia zgody są przechowywane? Np. czy kopie są przechowywane w formie papierowej lub prowadzony jest rejestr zgód elektronicznych?	
8. Jak długo dowody takie są zatrzymywane?	
9. Jeżeli w kontekście umowy Państwa organizacja prosi o więcej danych, niż jest to konieczne dla wykonania umowy, czy osoba, której dane dotyczą, została poinformowana, że nie musi takich dodatkowych danych przekazywać? **UWAGA: Należy wpisać „nie dotyczy" lub, jeżeli dotyczy, przekazać kopię odpowiedniego tekstu/linku**	

II.4 Informowanie osób, których dane dotyczą [UWAGA: Informacja taka nie jest obowiązkowa, ale jest pomocna w ocenie i korekcie wewnętrznych zasad ochrony danych]

10. Czy osoby, których dane dotyczą, są informowane o następujących kwestiach? Jeżeli tak, kiedy i jak?	*Należy wpisać tak/nie (lub „nie dotyczy")* **UWAGA: W stosownym przypadku można wpisać „jest to oczywiste w kontekście" i/lub „osoba, której dane dotyczą już taką informację otrzymała"**	Należy wyjaśnić kiedy i w jaki sposób to się odbywa. **Należy przedstawić kopie not informacyjnych lub linków.**
- Państwa organizacja jest administratorem czynności przetwarzania danych osobowych?		
- Dane Państwa organizacji (np. nazwa i numer wpisu w rejestrze)?		
- W stosownym przypadku dane Państwa przedstawiciela w UE?		
- Dane kontaktowe inspektora ochrony danych?		
- Główny cel przetwarzania?		
- Dodatkowy cel, w jakim Państwa organizacja chce		

(lub może chcieć) przetwarzać dane?		
- Jeżeli dane nie zostały uzyskane bezpośrednio od osoby, której dane dotyczą, źródło lub źródła danych oraz czy są to ogólnodostępne źródła (takie jak rejestry państwowe)?		
- Odbiorcy lub kategorie odbiorców danych? **UWAGA: porównaj Q4, powyżej**		
- Czy dane są (mają zostać) przekazywane do kraju spoza UE/EOG (np. na *serwer chmury w USA*)? **UWAGA: Dotyczy to także danych udostępnianych (w szczególności bezpośrednio, internetowo) podmiotom spoza UE/EOG.**		
- Jeżeli dane te są w taki sposób przekazywane, jakie zabezpieczenia wdrożono oraz gdzie osoby, których dane dotyczą, mogą uzyskać ich kopie? **UWAGA: Zabezpieczenia można zapewnić w ramach umowy o przekazie danych lub poprzez kodeksy prywatności lub pieczęcie prywatności.**		
- Przez jak długo dane będą zatrzymywane?		
- O ich prawach do żądania dostępu, skorygowania lub usunięcia danych, wnioskowania o ich zablokowanie, wyrażenia sprzeciwu wobec przetwarzania?		
- O ich prawie do wniesienia skargi do odpowiedniego organu ochrony danych?		
11. Jeżeli wszystkie dane lub część danych jest przetwarzana na podstawie zgody, czy osoby, których dane dotyczą, zostały poinformowane o następujących kwestiach?		
- Że mogą wycofać swoją zgodę w dowolnym momencie (oraz w jaki sposób) (bez wpływu na prawomocność wcześniejszego przetwarzania)?		

12. Jeżeli przekazanie danych jest wymagane ustawowo lub na podstawie umowy (lub istnieje wymóg zawarcia umowy), czy osoby, których dane dotyczą, zostały poinformowane o następujących kwestiach?	*Należy wpisać tak/nie (lub „nie dotyczy")* **UWAGA: W stosownym przypadku można wpisać „jest to oczywiste w kontekście" i/lub „osoba, której dane dotyczą już taką informację otrzymała"**	Należy wyjaśnić kiedy i w jaki sposób to się odbywa. **Należy przedstawić kopie not informacyjnych lub linków.**
- Czy są zobowiązane przekazać dane oraz jakie konsekwencje wynikają z ich nieprzekazania?		
13. Jeżeli wszystkie dane lub część danych przetwarzanych jest na podstawie kryterium „uzasadnionego interesu", czy osoby, których dane dotyczą, zostały o takim uzasadnionym interesie poinformowane?		Należy przedstawić krótkie podsumowanie kryteriów stosowanych w celu przeprowadzenia testu równoważącego w odniesieniu do podstawowych praw i swobód osób, których dane dotyczą, wynikających z art. 6(1)f RODO.
14. Jeżeli osoby, których dane dotyczą, będą podlegać automatycznemu procesowi decyzyjnemu lub profilowaniu, czy zostały poinformowane o następujących kwestiach?		Należy przedstawić krótkie podsumowanie logiki stosowanej w automatycznym procesie decyzyjnym i profilowaniu.
- Że taki proces decyzyjny lub profilowanie będą miały miejsce?		
- W szerokim tego słowa znaczeniu, jakiego rodzaju „logika" jest stosowana?		
- Jakie jest znaczenie oraz jakie są przewidywane skutki automatycznego procesu decyzyjnego lub profilowania?		

II.5 Transgraniczny przepływ danych [Uwaga: Wpis w polu 17 nie jest obowiązkowy, ale jest przydatny dla celów oceny wewnętrznej]

15. Czy którekolwiek z danych są przekazywane do kraju trzeciego (tj. kraju spoza UE/EOG (lub sektora w kraju trzecim) albo do organizacji międzynarodowej, w	*Należy wpisać tak/nie oraz odpowiednie kraje.* *Jeżeli przekazywane są tylko niektóre, nie wszystkie, dane, należy określić, jakiej kategorii danych to dotyczy.*	*Należy objaśnić cel przekazu danych, np. w ramach własnych operacji Państwa organizacji (np. w związku ze stosowaniem oprogramowania chmury) lub w ramach ujawniania danych stronom*

przypadku której *uznano*, że zapewnia „odpowiedni" stopień ochrony zgodnie z art. 45 RODO?		*trzecim (należy wymienić stronę/strony).*
WSZYSTKIE DANE PODANE W II.1		
***LUB:* Następujące dane:** (Należy skopiować dane z 1 i 2 powyżej)		
-		
-		
-		
-		
-		
-		
-		
-		
-		
-		
-		
-		
W razie potrzeby należy dodać kolejne wiersze		

16. Czy którekolwiek z danych są przekazywane do kraju trzeciego (tj. spoza UE/EOG (lub sektora w kraju trzecim) albo do organizacji międzynarodowej, w przypadku której nie uznano, że zapewnia „odpowiedni" stopień ochrony zgodnie z art. 45 RODO?	*Należy wpisać tak/nie oraz odpowiednie kraje. Jeżeli przekazywane są tylko niektóre, nie wszystkie, dane, należy określić, jakiej kategorii danych to dotyczy.*	*Należy objaśnić cel przekazu danych, np. w ramach własnych operacji Państwa organizacji (np. w związku ze stosowaniem oprogramowania chmury) lub w ramach ujawniania danych stronom trzecim (należy wymienić stronę/strony).*	*Na podstawie jakiego zabezpieczenia lub odstąpienia odbywa się takie przekazanie danych? Należy podać numer z listy w *__Uwaga__ poniżej oraz przedstawić kopię odpowiedniego dokumentu*
UWAGA: *Jeżeli dane są przekazywane w różnych celach do różnych odbiorców w różnych krajach, należy odpowiedzieć na pytania osobno dla każdego z kontekstów przekazywania danych.*			
WSZYSTKIE DANE PODANE W II.1			
***LUB:* Następujące dane:** (Należy skopiować dane z 1 i 2 powyżej)			
-			
-			
-			
-			

-			
-			
-			
W razie potrzeby należy dodać kolejne wiersze			

*** UWAGA:** Zgodnie z RODO przekazanie danych do krajów, które nie zapewniają „odpowiedniej" ochrony, może mieć miejsce wyłącznie wtedy, gdy wprowadzono „odpowiednie zabezpieczenia", wymienione w lewej kolumnie poniżej lub jeżeli zastosowanie ma odstąpienie wymienione w prawej kolumnie.

Zabezpieczenia zgodnie z art. 46 RODO:	Odstąpienia od art. 49 RODO, jeżeli zabezpieczenia przewidziane w art. 46 nie są dostępne (patrz: Wytyczne Europejskiej Rady Ochrony Danych w tym względzie: restrykcyjne stosowanie i restrykcyjna interpretacja):
1. międzynarodowy instrument pomiędzy organami publicznymi, 2. wiążące reguły korporacyjne; 3. zatwierdzone standardowe klauzule ochrony danych, 4. Kodeks postępowania; 5. certyfikacja; 6. zatwierdzone doraźne klauzule;	7. zgoda; 8. umowa pomiędzy administratorem danych a osobą, której dane dotyczą; 9. umowa pomiędzy administratorem danych a stroną trzecią; 10. niezbędne z ważnych względów interesu publicznego; 11. niezbędne dla roszczeń prawnych; 12. niezbędne do ochrony istotnych interesów osoby, której dane dotyczą, lub innych osób; 13. dane są przekazywane z ogólnie dostępnego rejestru opinii publicznej.

17. Czy wprowadzono zasady postępowania z wyrokiem sądu lub trybunału oraz decyzją organu administracyjnego kraju trzeciego, które mogą zostać nałożone na administratora lub podmiot przetwarzający, wymagając od niego przekazania lub ujawnienia danych osobowych? (Zob. art. 48 RODO)	*Należy wpisać tak/nie i jeżeli tak, należy przedstawić kopię wytycznych.*

III. BEZPIECZEŃSTWO I POUFNOŚĆ

UWAGA: Jeżeli odpowiedzi na poniższe pytania są różne dla różnych danych, należy odpowiedzieć na nie osobno dla każdego odrębnego zestawu danych.	*Należy podać następujące szczegóły:*
Czy dane wymienione w pkt. II.1 są utrzymywane na papierze, czy w wersji elektronicznej? Jeżeli na papierze, to czy są one utrzymywane w ramach zorganizowanego ręcznego zbioru danych (folder z danymi)?	
Gdzie (fizycznie) są dane przechowywane? (Państwa biura? Na serwerach u głównego administratora danych? Na serwerach powiązanej organizacji? Na serwerach strony trzeciej (np. dostawcy usługi w chmurze)?	
Jakie kroki podjęto w celu ochrony przed nieupoważnionym dostępem do fizycznego miejsca przechowywania/dostępności danych?	

Czy wprowadzono politykę bezpieczeństwa danych, która to reguluje? *(Jeżeli tak, należy przekazać kopię).*	
Jaki sprzęt jest stosowany do przetwarzania danych? Kto odpowiada za zarządzanie takim sprzętem i jego bezpieczeństwo?	
Czy jakiekolwiek dane są przechowywane na przenośnych nośnikach/urządzeniach? Jakiego rodzaju są to nośniki/urządzenia? Kto jest w ich posiadaniu?	
Czy jakiekolwiek osoby mogą uzyskać dostęp do urządzeń zawierających dane osobowe w celu dostępu do danych i ich przetwarzania? Jeżeli tak, czy wprowadzono politykę BYOD w tym zakresie? *Należy przekazać kopię polisy.*	
Czy wszystkie osoby upoważnione do dostępu do danych osobowych podlegają obowiązkowi zachowania poufności (na mocy ustawy lub zestawu norm zawodowych albo umowy)? *Należy podać dane lub kopie odpowiednich norm lub klauzul umownych.*	
Jakie oprogramowanie/aplikacje są stosowane do przetwarzania danych? (np. MS Office, centralnie zarządzana aplikacja, usługa w chmurze, itp.)	
- Czy oprogramowanie to podlega zarządzaniu lokalnemu czy centralnemu? W przypadku zarządzania centralnego, jaki jest podmiot centralny? Jeżeli nie są to Państwo, czy istnieje formalne porozumienie pomiędzy takim podmiotem a Państwa organizacją co do użytkowania takiego oprogramowania? *Należy przekazać kopię takiego porozumienia.*	
- Czy oprogramowanie wykorzystuje „chmurę”? Jeżeli tak, kim jest dostawca chmury oraz gdzie posiada swoją siedzibę? Gdzie znajduje się fizycznie serwer chmury? Czy dane na serwerze chmury są w pełni szyfrowane? Jak (tj. przy użyciu jakiej techniki szyfrowania)? *Należy przekazać kopię umowy, na mocy której przetwarzanie takie ma miejsce.*	
- Kto odpowiada za oprogramowanie (tj. kto pełni funkcję „administratora”)? (Państwo? Ktoś inny z Państwa organizacji? Ktoś w podmiocie centralnym, z którym jesteście Państwo powiązani? Ktoś inny?)	
Czy dane są w którymkolwiek momencie/w jakichkolwiek okolicznościach elektronicznie	

transmitowane na inny nośnik, system lub inne urządzenie?	
Jeżeli są elektronicznie transmitowane, odbywa się to: - przez internet? Jeżeli tak, czy dane są szyfrowane? Jak (tj. przy użyciu jakiej techniki szyfrowania?) - przy użyciu FTP? Jakie zabezpieczenie jest stosowane? - VPN? Jakie zabezpieczenie jest stosowane? - inne - *należy określić*	

- o – O – o -

ZADANIE 2: Przegląd operacji przetwarzania danych osobowych

Dla inspektora ochrony danych, po stworzeniu rejestru operacji przetwarzania danych osobowych w swojej organizacji (Zadanie 1), kolejnym krokiem jest przeprowadzenie dogłębnego przeglądu wszystkich zarejestrowanych operacji przetwarzania danych, by sprawdzić, czy spełniają one wymagania RODO pod każdym istotnym względem, z uwzględnieniem:

- określenia celu i ograniczeń;
- ważności zgody (i istnienia dokumentu potwierdzającego jej wydanie) lub zastosowania innej podstawy prawnej przetwarzania;
- przetwarzanych danych osobowych i ich znaczenia oraz potrzeby w związku z określonym celem;
- jakości danych (dokładności, aktualności, itp. danych, a także minimalizacji i pseudonimizacji danych);
- informacji przekazanych osobie, której dane dotyczą, z własnej inicjatywy administratora (gdy dane są gromadzone od takiej osoby lub w inny sposób albo na żądanie - także w odniesieniu do danych gromadzonych od osób odwiedzających stronę internetową);
- długości okresu zatrzymywania danych w możliwej do zidentyfikowania formie oraz wszelkich informacji dotyczących pozbawiania elementów pozwalających na identyfikację;
- bezpieczeństwa technicznego, organizacyjnego i fizycznego danych (z uwzględnieniem ograniczenia fizycznego dostępu i ograniczenia dostępu technicznego [nazwa użytkownika, hasła, PINy, itp.], szyfrowanie, itp.);
- przekazywanie danych za granicę (oraz prawne i inne umowne lub inne ustalenia)
- itd.

W świetle powyższych ustaleń inspektor ochrony danych powinien być w stanie **ocenić:**

- czy można powiedzieć, że operacja przetwarzania ***jako całość*** jest zgodna z nadrzędną zasadą zgodności z prawem i rzetelności.

(Należy zauważyć, że taka ocena zgodności z RODO jest niezależna od oceny ryzyka, opisanej w Zadaniu 3).

Wpisy poszczególnych operacji przetwarzania danych osobowych utworzone w Zadaniu 1 (w szczególności, jeżeli utworzono je w bardziej szczegółowym formacie[328]) powinny stanowić podstawę przeglądu i doprowadzi do zadania przez inspektora ochrony danych właściwych pytań, z uwzględnieniem w szczególności:

- Czy wystarczające jasne jest, który podmiot jest **administratorem** operacji przetwarzania danych osobowych oraz, jeżeli w procesie uczestniczą inne podmioty, jakie jest ich odpowiedni status (np. ***współadministrator, podmiot przetwarzający*** lub odrębny ***niezależny*** administrator)? Jeżeli nie jest to oczywiste, czy zawarto **formalne porozumienia** objaśniające te kwestie (patrz: Zadanie 1)?
- Czy jest wystarczająco jasne, która jednostka organizacyjna jest „**właścicielem**" operacji przetwarzania danych osobowych (tj. kto faktycznie ponosi codzienną odpowiedzialność za przetwarzanie)? Czy zostało to określone w **formalnym dokumencie** (np. konkretnych instrukcjach wydanych przez administratora dla danej jednostki)?
- Czy **cel** lub **cele** operacji przetwarzania danych osobowych zostały wystarczająco precyzyjnie określone? Gdzie (tj. w jakiego rodzaju **dokumencie**)? Jeżeli dane osobowe wykorzystywane w operacji przetwarzania są wykorzystywane w więcej niż jednym celu, jaki jest ***podstawowy cel*** i jaki jest ***drugorzędny cel***? Czy taki drugorzędny cel jest ***kompatybilny*** z podstawowym celem lub są to odrębne cele?

[328] Jak przedstawiono w przykładowym formacie szczegółowego rejestru czynności przetwarzania danych osobowych załączonym do Zadania 1.

Uwaga: Oceniając kompatybilność przetwarzania w drugorzędnym celu z podstawowym celem, inspektor ochrony danych musi wziąć pod uwagę sprawy wymienione w art. 6(4) RODO.

Czy wszystkie cele, w których przetwarzane są dane osobowe, są w pełni uzasadnione i zgodne z prawem?

- Czy przetwarzane dane osobowe są **odpowiednie, stosowne i niezbędne** w podstawowym celu? W jaki sposób zapewnia się, by były one **dokładne** i **aktualne** w danym celu oraz jakie ustalenia poczyniono, by to zapewnić oraz by ***sprostować, zaktualizować*** lub ***usunąć*** niedokładne lub nieaktualne informacje?

  Czy podjęte środki są adekwatne i wystarczające? Czy byłoby możliwe osiągnięcie tego samego celu przy mniejszym ryzyku dla prywatności i innych praw danej jednostki?

- Jakie dane osobowe są wykorzystywane lub ujawniane w drugorzędnych celach lub faktycznie w nowych, niepowiązanych celach (z reguły stronie trzeciej)? Czy przetwarzane dane osobowe są **odpowiednie, stosowne i niezbędne** w takich drugorzędnych lub nowych, niepowiązanych celach? (Jeżeli wszystkie dane gromadzone w jednym [podstawowym] celu zostały ujawnione bezmyślnie w drugorzędnym celu lub nowym, niepowiązanym celu, mogą być zbyt obszerne dla takiego drugorzędnego lub niepowiązanego celu albo drugorzędnych lub niepowiązanych celów. Czy wzięto to pod uwagę?)

  Uwaga: Patrz szczegółowy formularz czynności przetwarzania danych osobowych, II.2.

  Czy wszystkie drugorzędne cele, w których przetwarzane są dane osobowe, są w pełni uzasadnione i zgodne z prawem?

- W jaki sposób zapewnia się, by dane wykorzystywane lub ujawniane w drugorzędnym lub nowym, niepowiązanym celu były **dokładne** i **aktualne** w danym celu w momencie pierwszego wykorzystania lub ujawnienia w tym celu oraz jakie ustalenia poczyniono, by to zapewnić ich **dokładność i aktualność** po pierwszym wykorzystaniu lub ujawnieniu oraz by ***sprostować, zaktualizować*** lub ***usunąć*** je, jeżeli i gdy okażą się niedokładne lub nieaktualne? Czy podjęte odpowiednie środki są adekwatne i wystarczające?

  Uwaga: Jeżeli dane są wykorzystywane lub ujawniane w więcej niż jednym drugorzędnym lub nowym celu, na powyższe pytania należy odpowiedzieć osobno dla każdego z takich celów.

- **Kiedy, jak, od kogo i w jakiej formie** uzyskano **jakie** dane osobowe? Na przykład: osoba, której dane dotyczą, departament rządowy, (były) pracodawca itp.; np. na papierze, w formie elektronicznej, itp.

  Uwaga: Na pytanie to należy odpowiedzieć zarówno w odniesieniu do **niewrażliwych,** jak i **wrażliwych danych,** a jeżeli różne dane uzyskano z różnych źródeł, należy to zaznaczyć. Patrz: szczegółowy formularz przetwarzania danych osobowych, II.1 i II.2.

  Czy takie źródła danych są odpowiednie? Czy pewne dane, które uzyskano od stron trzecich, można było lepiej uzyskać od samych osób, których dane dotyczą?

- **Jak długo** dane osobowe (niewrażliwe i wrażliwe) są **zatrzymywane? Co dzieje się na koniec tego okresu?** (Np. ***wymazanie, zniszczenie, anonimizacja*** *lub* ***pseudonimizacja,*** przy czym to ostatnie oznacza, że dane są w dalszym ciągu zatrzymywane w możliwej do zidentyfikowania formie)[329]. Jeżeli dane są zatrzymywane w anonimowej lub spseudonimizowanej formie,

[329] Należy zauważyć, że zgodnie z RODO (a także Dyrektywą o ochronie danych z 1995 roku) dane osobowe można uznać za zanonimizowane, jeżeli nikt, tj. nie tylko administrator, nie może ich już powiązać z konkretną jednostką (ale także np. współpracownicy, krewni lub znajomi, którzy mogą znaleźć dane, jeśli zostaną udostępnione w domniemanej nieokreślonej formie w Internecie lub na papierze). W tym względzie inspektorzy ochrony danych powinni wiedzieć, że coraz więcej danych, które mogą wydawać się „nieosobowe" lub o których mówi się, że „przekazano je anonimowo" można coraz częściej (ponownie) powiązać z konkretnymi osobami. W szczególności dane w rzekomo „anonimowych" bazach danych „Big Data" stają się często w nieoczekiwany i niepokojący sposób ponownie identyfikowalne, w szczególności w przypadku powiązania lub „dopasowania" różnych baz danych. Jeżeli nawet baza danych nieosobowych jest wykorzystywana do tworzenia „profili" (typowych konsumentów konkretnego produktu lub typowych pacjentów, lub typowych przestępców albo terrorystów) i profile takie są następnie stosowane w bazie danych, by wyodrębnić osoby spełniające ich kryteria, wtedy takie przetwarzanie może mieć bardzo poważny wpływ na takie osoby, którym może zostać odmówione ubezpieczenie lub praca albo dostęp do

dlaczego? (np. w celach badawczych lub historycznych? Jeżeli tak, przetwarzanie w takim celu powinno być przedmiotem osobnej oceny pod kątem kompatybilności z RODO).

Uwaga: Okres zatrzymywania można określić jako konkretny czas lub jako zdarzenie np.: „7 lat" lub „do 5 lat po rozwiązaniu stosunku pracy". Należy zauważyć, że istnieją **formalne standardy** dotyczące rekomendowanych metod usuwania/niszczenia różnych kategorii danych i nośników danych[330]. Inspektor ochrony danych powinien sprawdzić, czy są one przestrzegane (w szczególności, jeśli chodzi o wrażliwe informacje w sensie prawnej ochrony danych lub w szerszym sensie społecznym lub politycznym.

Czy okresy zatrzymywania danych są właściwe? Lub może są zbyt długie? Czy sposoby usuwania/niszczenia danych są zgodne ze standardami krajowymi i międzynarodowymi? Jeżeli dane są zatrzymywane dłużej niż wskazuje normalny okres zatrzymania w zanonimizowany lub spseudonimizowany sposób: (i) czy jest to stosowne dla celu takiego przedłużonego okresu zatrzymania? Czy dane zatrzymane w spseudonimizowanej formie mogą być zatrzymane w pełni anonimowej formie i w dalszym ciągu być wystarczające w szczególnym celu? Na ile prawdziwe jest twierdzenie, że wszystkie dane są „anonimizowane"? (Należy zauważyć, że pełna anonimizacja jest coraz trudniejsza do osiągnięcia, w szczególności w dużych zbiorach danych oraz w szczególności gdy zbiory danych można łączyć lub powiązać z innymi zbiorami danych).

- Które z powyższych danych są ujawnianie, i którym **stronom trzecim?** I **w jakich celach**? Czy ujawniane dane są ***odpowiednie, stosowne i niezbędne*** w tych celach, ***dokładne i aktualne?*** Jeżeli tak, w jaki sposób zapewnia się, by sytuacja ta nie uległa zmianie?

Uwaga: Odpowiedzi na powyższe pytania mogą częściowo nawiązywać do odpowiedzi na wcześniejsze pytania.

- **Na jakiej podstawie prawnej** dane osobowe są przetwarzane?

Uwaga:

W przypadku niewrażliwych danych podstawę prawną musi stanowić jedna z podstaw wymienionych w art. 6 RODO, a w przypadku wrażliwych danych - jedna z podstaw wymienionych w art. 9 RODO.

Należy zauważyć, że podstawa przetwarzania w formie „uzasadnionego interesu" (art. 6(1)(f)) nie ma zastosowania do przetwarzania jakichkolwiek danych (w tym niewrażliwych danych) przez organy publiczne w trakcie realizacji swoich zadań (art. 6(1), ostatnie zdanie) i administrator nie może na jej podstawie - ani w sektorze publicznym, ani w prywatnym, przetwarzać wrażliwych danych (art. 9).

Ponadto, jeżeli przetwarzanie oparte jest na art. 6(1)(c) lub (e) („przetwarzanie [jakie] jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze", „przetwarzanie [jakie] jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi"), musi być oparte na prawie Unii lub państwa członkowskiego EU (art. 6(3)). Jeżeli jako podstawę prawną wskazano obydwa te prawa, inspektor ochrony danych musi sprawdzić, czy dane prawo spełnia wymagania określone w art. 6(3) RODO.

Czy wskazana podstawa prawna przetwarzania jest właściwa? Czy spełniono odpowiednie warunki stosowania takiej podstawy prawnej (np. jeżeli chodzi o zgodę, co zostało omówione poniżej)?

Należy zauważyć, że podstawa prawna przetwarzania w podstawowym celu może być inna niż podstawa prawna przetwarzania (z uwzględnieniem ujawnienia) jakichkolwiek danych w drugorzędnym lub nowym, niepowiązanym celu, a ważność wskazanej podstawy prawnej należy ocenić osobno dla każdego z celów.

---

lotu lub nawet kraju (albo co gorsza) na podstawie skutecznie niemożliwych do zakwestionowania algorytmów. Zob: Douwe Korff i Marie Georges, Passenger Name Records, data mining & data protection: the need for strong safeguards, raport dla Komitetu Konsultacyjnego Rady Europy w sprawie ochrony danych, czerwiec 2015, dokument Rady Europy T-PD(2015)11, pkt I.iii, *The dangers inherent in data mining and profiling*: https://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD(2015)11_PNR%20draft%20report%20Douwe%20Korff%20&%20Marie%20Georges_15%2006%202015.pdf

[330] Patrz na przykład:

- DIN - Niemiecki Instytut Standaryzacji, Urządzenia biurowe - niszczenie nośników danych, DIN 66399, październik 2012 r.
- Specjalna publikacja NIST 800-88 wer. 1, Wytyczne dotyczące neutralizacji nośników, grudzień 2014 r. http://dx.doi.org/10.6028/NIST.SP.800-88r1.
- Amerykańska Agencja Bezpieczeństwa/Central Security Service, Media Destruction Guidance, https://www.nsa.gov/ia/mitigation_guidance/media_destruction_guidance/index.shtml.

- Jeżeli dane są przetwarzane na podstawie **zgody** osób, których dane dotyczą:
  - ***jak i kiedy*** zgodę taką się uzyskuje (np. w formie papierowej lub elektronicznej, poprzez bezpośrednie zapytanie lub poproszenie osoby o zaznaczenie odpowiedniej kratki)?[331]
  - jakie ***dowody*** wyrażenia zgody są przechowywane (np. papierowe kopie, rejestry)?
  - w jaki sposób i jak długo dowody takie są ***zatrzymywane***?
  - jeżeli w kontekście umowy organizacja prosi o więcej danych niż jest to konieczne dla wykonania umowy, czy osoba, której dane dotyczą, ***została poinformowana, że nie musi takich dodatkowych danych przekazywać?***
- Czy **osoby, których dane dotyczą, są informowane** o wszystkich sprawach, o których należy je poinformować (patrz art. 13 i 14 RODO - pkt II.4 szczegółowego formularza przetwarzania danych osobowych), a jeżeli tak, kiedy i w jaki sposób?

  Czy przekazywane są wszystkie odpowiednie informacje? Czy jest to wykonywane w najlepszym możliwym formacie? W najlepszym czasie? Czy obowiązkowe do wypełnienia pola łatwo odróżniają się od opcjonalnych do wypełnienia pól?
- Czy którekolwiek z danych są **przekazywane do kraju trzeciego (tj. spoza UE/EOG** (lub sektora w kraju trzecim) albo do **organizacji międzynarodowej**, w przypadku której uznano, że zapewnia „odpowiedni" stopień ochrony zgodnie z art. 45 RODO?

  Czy odpowiednia decyzja stwierdzająca odpowiedni poziom ochrony faktycznie obejmuje przetwarzanie? Czy jest w dalszym ciągu ważna (patrz: ustalenie przez Trybunał Sprawiedliwości UE, że decyzja stwierdzająca odpowiedni poziom ochrony „Safe Harbor" była nieważna)?
- Czy którekolwiek z danych są **przekazywane do kraju trzeciego (tj. spoza UE/EOG** (lub sektora w kraju trzecim) albo **do organizacji międzynarodowej**, w przypadku której **nie** uznano, że zapewnia „odpowiedni" stopień ochrony zgodnie z art. 45 RODO? Jeżeli tak, na podstawie jakiego zabezpieczenia lub odstąpienia odbywa się takie przekazanie danych?

  Uwaga: Zgodnie z RODO przekazanie danych do krajów, które niezapewniają „odpowiedniej" ochrony może mieć miejsce wyłącznie wtedy, gdy wprowadzono „**odpowiednie zabezpieczenia**", wymienione w art. 46 RODO, lub jeżeli zastosowanie ma wymienione w art. 48 RODO odstąpienie (patrz pkt II.5 szczegółowego formularza przetwarzania danych, pytanie 16).

  Czy wskazane zabezpieczenie lub odstąpienie jest poprawne? Czy spełnia ono wszystkie wymagania określone w odpowiednim artykule (art. 46 lub 48)?
- Czy wprowadzono zasady postępowania z wyrokiem sądu lub trybunału oraz decyzją organu administracyjnego kraju trzeciego, które mogą zostać nałożone na administratora lub podmiot przetwarzający, wymagając od niego przekazania lub ujawnienia danych osobowych?

  Uwaga: Zgodnie z art. 48 RODO wyroki i decyzje krajów trzecich „mogą zostać uznane lub być egzekwowalne wyłącznie, gdy opierają się na umowie międzynarodowej, takiej jak umowa o wzajemnej pomocy prawnej, obowiązującej między wzywającym państwem trzecim a Unią lub państwem członkowskim, bez uszczerbku dla innych podstaw przekazania na mocy niniejszego rozdziału". Jest to sprawa trudna do oceny dla właścicieli oraz wielu administratorów i podmiotów przetwarzających i konieczne są wytyczne dotyczące sposobu, w jaki właściciele, administratorzy i podmioty przetwarzające powinny postąpić w przypadku, gdy staną przed tego typu wyrokiem lub decyzją. Podmioty przetwarzające i właściciele powinni co najmniej bezzwłocznie przekazać taką sprawę najwyższemu kierownictwu administratora oraz inspektorowi ochrony danych.

  Jeżeli istnieją odpowiednie wytyczne, czy są one adekwatne (np. jeżeli zostały przyjęte przed wejściem w życie RODO, możliwe że nie wspominają udziału inspektora ochrony danych w tej sprawie, ponieważ w momencie ich sporządzenia możliwe, że nie było takiego inspektora)?

[331] Należy zauważyć, że proste stwierdzenie na stronie internetowej mówiące, że *„Korzystając z niniejszej strony, wyrażasz zgodę na gromadzenie i wykorzystywane twoich danych osobowych"* nie oznacza już zgodnie z RODO wystarczającej i ważnej zgody. Nie tylko brakuje tutaj wystarczających informacji na temat wykorzystania danych, co sprawia, że „zgoda" jest nieważna, ponieważ nie jest „świadoma". Ale także wątpliwe jest, czy dalsze korzystanie ze strony jako takiej może stanowić *„jednoznaczne okazanie woli"* przez osobę, której dane dotyczą, by wyrazić taką zgodę (zob. definicja zgody w art. 4(11) RODO).

Jeżeli nie istnieją jeszcze żadne wytyczne w tym zakresie, należy je pilnie opracować w konsultacji z inspektorem ochrony danych.

- Jakie wprowadzono formalne, organizacyjne, praktyczne i techniczne środki, by zapewnić bezpieczeństwo i poufność danych?

  Uwaga: Zgodnie z art. 32 RODO administratorzy i podmioty przetwarzające muszą wdrożyć odpowiednie środki techniczne i organizacyjne, aby zapewnić poziom bezpieczeństwa odpowiadający ryzyku, jakie stwarza przetwarzanie danych w stosunku do praw i wolności osób fizycznych (z uwzględnieniem w szczególności osób, których dane dotyczą). Artykuł ten wymienia różne środki, takie jak pseudonimizacja i szyfrowanie, klauzule poufności, środki techniczne zapewniające integralność, dostępność i odporność stosowanych systemów oraz zdolności do przywrócenia danych.

  Kwestia ta zostanie szerzej omówiona w Zadaniu 3 (ocena ryzyka). Jednak **wstępny zarys** podjętych (lub niepodjętych) środków należy uzyskać już w kontekście Zadania 2, by **wstępnie wskazać**, czy zastosowane środki są „odpowiednie", 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" (art. 32).

  Wiele (chociaż nie wszystkie) z tego typu środków uwzględniono w uznawanych standardach międzynarodowych, takich jak te wymienione poniżej. Należy jednak zauważyć, że nie zawsze obejmują one wszystkie istotne kwestie, np. z reguły koncentrują się na bezpieczeństwie w większym stopniu niż na minimalizacji danych lub ograniczeniu celu[332].

  Jednak mimo to, **inspektorzy ochrony danych powinni znać tego typu standardy** i **sprawdzać, czy ich organ ochrony danych lub Europejska Rada Ochrony Danych nie wydała w ich sprawie (pozytywnego lub negatywnego) komentarza (albo uzupełnień)**[333]:

  - ISO/IEC 27001:2013 Kodeks praktyki dla kontroli informacji
  - ISO/IEC 29100 - Technologia informatyczna - Techniki bezpieczeństwa - Ramy prywatności
  - ISO/IEC 27018 - Kodeks postępowania dotyczący ochrony danych osobowych w chmurach obliczeniowych funkcjonujących jako podmioty przetwarzające dane osobowe
  - ISO/IEC 29134 - Wytyczne dotyczące oceny skutków dla ochrony danych
  - ISO/IEC 29151 - Kodeks postępowania dotyczący ochrony możliwych do zidentyfikowania danych osobowych
  - JIS 15001:2006 - Wymagania dotyczące systemu zarządzania ochroną danych osobowych
  - BS 10012:2017 - Specyfikacja systemu zarządzania danymi osobowymi

  Więcej standardów jest w przygotowaniu:

  - ISO 20889 - Poprawiające prywatność techniki pozbawiania elementów pozwalających na identyfikację danych
  - ISO 29184 - Internetowe informacje o prywatności oraz zgoda
  - ISO 27552 Zmiana ISO/IEC 27001 dla zarządzania prywatnością – Wymagania → Nowy tytuł: Rozszerzenie do ISO/IEC 27001 i ISO/IEC 27002 w odniesieniu do zarządzania danymi osobowymi - Wymagania i wytyczne
  - UNI Reference practice – Wytyczne dotyczące zarządzania danymi osobowymi w środowiskach teleinformatycznych zgodnie z RODO

  Jeżeli w przetwarzaniu wykorzystywana jest chmura, należy zwrócić uwagę, czy uwzględniono kwestie wymienione w wytycznych „Trusted Cloud – Data Protection Profile for Cloud Services (TCDP)" wydanych przez projekt pilotażowy wspierany przez niemiecki rząd „Certyfikacja

[332] Kilka lat temu organy ochrony danych zauważyły, że dokument ISO w sprawie bezpieczeństwa, który obejmował kody PIN, nie określa liczby i rodzaju znaków, z jakich należy korzystać. Od tej pory organy ochrony danych stosują politykę możliwie najszerszej współpracy z grupami ISO, których działalność dotyczy kwestii ochrony danych.

[333] Źródło: Alessandra de Marco, prezentacja na pierwszej sesji szkoleniowej „T4DATA", czerwiec 2018 rok, slajdy „*Existing standards (on security and privacy)*" i „*Standards (on privacy) not yet finalised*".

ochrony danych dla usług w chmurze" (chociaż do tej pory w dalszym ciągu zwany on jest niemiecką ustawą federalną o ochronie danych sprzed RODO, bardziej niż RODO)[334].

Na tym etapie inspektor ochrony danych powinien sprawdzić, czy administrator i/lub właściciele procesu znają powyższe standardy oraz próbują je stosować, a jeżeli tak, to czy istnieją w tym zakresie stosowne certyfikaty. Kwestia, czy są one faktycznie w pełni przestrzegane lub w rzeczywistości powinny być może zostać bardziej szczegółowo omówiona w Zadaniu 3 (ocena ryzyka).

Niniejszy przegląd jest pierwszym przykładem sprawowanej przez inspektora ochrony danych funkcji monitorowania przestrzegania prawa (opisanej dalej w Zadaniu 4).

Jeżeli inspektor ochrony danych w jakimkolwiek względzie uważa, że operacja przetwarzania danych osobowych nie spełnia któregokolwiek z wymogów RODO, jest zobowiązany **zawiadomić** o nieprawidłowościach odpowiedzialną osobę lub odpowiedzialne osoby w ramach organizacji oraz zaproponować działania naprawcze (z uwzględnieniem, jeżeli to konieczne, wstrzymania danej operacji). Jeżeli jego rada nie zostanie wprowadzona w życie, inspektor ochrony danych powinien przekazać sprawę najwyższemu kierownictwu (patrz poniżej: punkt zatytułowany „*Zadania doradcze*").

Należy zauważyć, że niniejszy ogólny przegląd czynności przetwarzania stanowi osobną kwestię w stosunku do naruszenia ochrony danych osobowych, które omówiono w Zadaniu 6 („*Postępowanie z naruszeniem ochrony danych osobowych*"). Jak wyjaśniono tam, naruszenie takie należy *natychmiast* zgłosić kierownictwu najwyższego szczebla.

Inspektor ochrony danych powinien prowadzić pełne **rejestry** wszystkich swoich przeglądów, ocen oraz tego typu porad.

- o – O – o -

[334] Zob. https://tcdp.de/data/pdf/14_TCDP_v1.0_EN.pdf (patrz w szczególności wykaz standardów na str. 14 – 16). Wersja dostępna w momencie pisania (wer. 1.0) pochodzi z września 2016 roku, ale autorzy mają nadzieję, że po stworzeniu opartych na RODO standardów kontroli i procedur certyfikacji, „*certyfikaty TCDP zostaną przekształcone zgodnie z Ogólnym rozporządzeniem o ochronie danych dla usług w chmurze*" (str. 7). Patrz także dyskusja na temat czynników ryzyka itp. określonych przez Europejskiego Inspektora Ochrony Danych w odniesieniu do usług w chmurze w Zadaniu 3.

ZADANIE 3: Ocena ryzyka wynikającego z operacji przetwarzania danych osobowych

Jak wspomniano w pkt. 2.2.1, RODO nakłada na administratorów ogólny obowiązek uwzględnienia „charakteru, zakresu, kontekstu i celów przetwarzania oraz **ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia**" wynikającego z każdej operacji przetwarzania danych osobowych oraz wdrożenia „odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem" (art. 24(1); patrz także: art. 25(1))).

Inspektor ochrony danych:

> wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.
>
> (art. 39(2))

Zapewnienie zgodności z powyższymi wymaganiami wymaga ustalenia odpowiedniego ryzyka. Należy to wykonać w ramach spisu operacji przetwarzania danych osobowych oraz tworzenia ich rejestru (Zadanie 1) i w szczególności wraz z ich przeglądem (Zadanie 2).

RODO nie wymaga jednoznacznie udziału inspektora ochrony danych w ogólnych ocenach ryzyka. Przewiduje jedynie taki udział w przypadku bardziej dogłębnej oceny skutków dla ochrony danych (art. 35(2) - patrz Zadanie 4 poniżej). Jednak w praktyce zalecany byłby (przynajmniej) udział inspektora ochrony danych w tego typu ogólniejszych ocenach ryzyka. W rzeczywistości ocena będzie często zależeć od opinii inspektora.

Należy zauważyć, że ryzyko podlegające ocenie to nie tylko wąsko rozumiane ryzyko bezpieczeństwa, tj. prawdopodobieństwo i wpływ **naruszenia danych**[335], ale raczej ryzyko dla **praw i wolności osób, których dane dotyczą, (i innych jednostek)** jakie może wynikać z operacji przetwarzania. Obejmuje to nie tylko ich ogólne prawa do prywatności i życia prywatnego, a także ich konkretne prawa osoby, której dane dotyczą, ale także w zależności od sytuacji prawo do wolności wypowiedzi, wolności przemieszczania się, wolności od dyskryminacji, wolności od władzy autorytarnej oraz prawo do życia w demokratycznym społeczeństwie bez nienależytego nadzoru ze strony swojego własnego kraju lub innych krajów i prawo do skutecznych środków prawnych. Koncepcja ta jest szeroka[336].

Ogólna ocena ryzyka powinna także uwzględniać ustalenia z Zadania 2. Na przykład, jeżeli ustalono, że mimo tego, że konkretna operacja przetwarzania była jako taka zgodna z prawem (tj. posiadała właściwą podstawę prawną i służyła uzasadnionemu interesowi), gromadzono i przechowywano w odpowiednim celu niewłaściwe i nadmierne dane - wbrew zasadzie „minimalizacji danych"- można powiedzieć, że operacja taka rodzi „ryzyko" sama w sobie, tj. że błędnie wykorzystywano niewłaściwe i niepotrzebne dane. W takiej sytuacji odpowiednim środkiem pozwalającym uniknąć ryzyka byłoby wstrzymanie gromadzenie niewłaściwych i niepotrzebnych danych oraz wymazanie już posiadanych tego typu danych. Innym przykładem byłoby wykorzystywanie w dalszym ciągu nadających się do identyfikacji danych w przetwarzaniu statystycznym, które można przeprowadzić przy użyciu pseudonimizowanych lub nawet w pełni anonimowych danych. W takim przypadku odpowiednim środkiem byłoby zapewnienie właściwej (poważnej) pseudonimizacji lub (lepiej) pełnej anonimizacji wykorzystywanych danych.

Wszystko to podkreśla, że dla celów ogólnego przeglądu (Zadanie 2) oraz oceny ryzyka (Zadanie 3) administrator - w praktyce inspektor ochrony danych - musi przyjrzeć się bliżej **wszystkim aspektom każdej odrębnej operacji i funkcji przetwarzania danych.**

Jak zaproponował włoski organ ochrony danych, *Garante*, przydatnym rozwiązaniem jest stosowanie podejścia przyjętego przez ENISA (Europejską Agencję ds. Sieci i Bezpieczeństwa Informacji), które z kolei oparte jest na ogólnie przyjętym standardzie ISO 27005: *„Zagrożenia wykorzystują słabe strony*

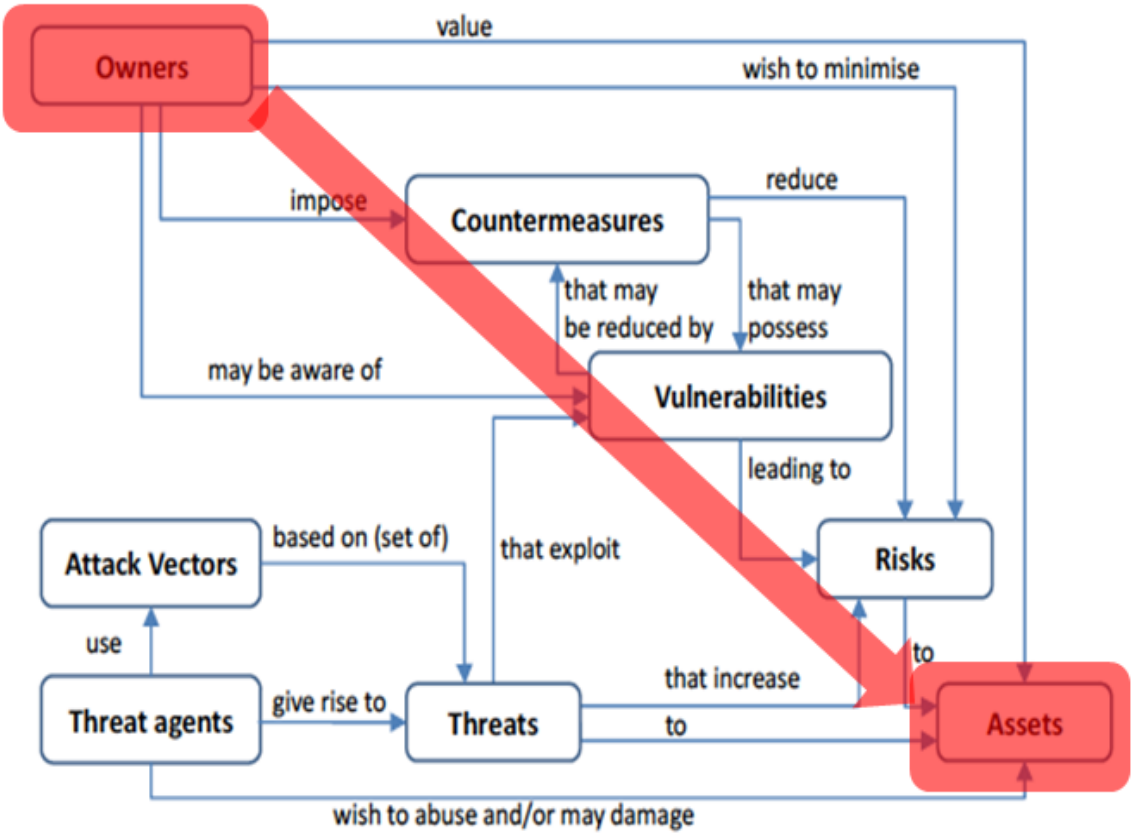
[335] **„Naruszenie ochrony danych osobowych"** jest definiowane w RODO jako „naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych." (art. 4(12)). Zob. Zadanie 6 poniżej.

[336] Zob. dyskusja na temat znaczenia „ryzyka" i „wysokiego ryzyka" w Zadaniu 1 („*Zwolnienia*") oraz Zadaniu 4.

aktywów, by szkodzić organizacji", a także bardziej szczegółowe potraktowanie zwrotu **ryzyko**, jako składającego się z następujących ***elementów:***

Aktywa (Podatność, Kontrola), **Zagrożenie** (Profil Agenta Zagrożenia, Prawdopodobieństwo) oraz **Oddziaływanie.**

Elementy ryzyka oraz ich powiazania można zilustrować w następujący sposób:



Źródło: Threat Landscape Report 2016, Wykres 4: The elements of risk and their relationships according to ISO 15408:2005, https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016. Zob. także: Raport ENISA z 2017 roku, https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017.

Legenda:
Właściciele narzucają mogą stwierdzić — *Wartość* ***środki zaradcze*** *które można ograniczyć* — *chęć ograniczenia do minimum ograniczają które mogą posiadać*
zagrożenia
Wektory ataku wykorzystują — *w oparciu o (zestaw) które zwiększają* — *które wykorzystują prowadzące do* — ***ryzyka***
czynniki zagrożenia *prowadzą do powstania* ***zagrożenia*** *w stosunku do* — ***aktywów***
chcą nadużyć i/lub zniszczyć

Garante podkreśla także, że **właściwa ocena ryzyka obejmuje cztery etapy**[337]**:**

1. Zdefiniowanie operacji przetwarzania i jej kontekstu.
2. Zrozumienie i ocena oddziaływania.
3. Ustalenie możliwych zagrożeń i ocena ich prawdopodobieństwa (prawdopodobieństwa wystąpienia zagrożenia).

[337] Giuseppe d'Acquisto, prezentacja na pierwszej sesji szkoleniowej „T4DATA" na temat bezpieczeństwa danych, czerwiec 2018 rok, slajd *„Risk assessment (a focus on security)"*.

4. Ocena ryzyka (łącząca prawdopodobieństwo wystąpienia zagrożenia oraz oddziaływanie).

Pierwszy etap (zdefiniowanie operacji przetwarzania i jej kontekstu) został wykonany w ramach Zadania 1 i 2.

Drugi etap obejmuje **ustalenie różnych poziomów oddziaływania,** które może obejmować cztery niżej opisane poziomy[338]:

POZIOM oddziaływania	Opis
Niski	Jednostki mogą natrafić na kilka niewielkich niedogodności, które pokonają bez żadnych problemów (czas spędzony na ponowne wprowadzanie informacji, irytacja, rozdrażnienie, itp.).
Średni	Jednostki mogą natrafić na znaczące niedogodności, które będą w stanie pokonać pomimo kilku trudności (dodatkowe koszty, odmowa dostępu do usług, strach, brak zrozumienia, stres, niewielkie dolegliwości fizyczne, itp.).
Wysoki	Jednostki mogą napotkać na znaczące konsekwencje, które powinny być w stanie pokonać, aczkolwiek z poważnymi trudnościami (sprzeniewierzenie środków, umieszczenie na czarnej liście przez instytucje finansowe, szkody majątkowe, utrata pracy, wezwanie do sądu, pogorszenie stanu zdrowia, itp.).
Bardzo wysoki	Jednostki, które mogą napotkać na znaczące lub nawet nieodwracalne konsekwencje, których nie są w stanie pokonać (niezdolność do pracy, długoterminowe dolegliwości psychiczne lub fizyczne, śmierć, itp.).

Garante wspomina **cztery główne obszary oceny**, jeżeli chodzi o **bezpieczeństwo danych**, tj.

A. Sieć i zasoby techniczne (sprzęt i oprogramowanie komputerowe)
B. Procesy/procedury związane z operacją przetwarzania danych
C. Różne strony i osoby uczestniczące w operacji przetwarzania
D. Sektor działalności i skala przetwarzania

W odniesieniu do każdego z obszarów oceny zadaje **pięć pytań**. Odpowiedź twierdząca wskazuje na ryzyko, co zaprezentowano w tabeli na kolejnej stronie[339].

Osoba oceniająca ryzyko bezpieczeństwa może na podstawie tych odpowiedzi obliczyć następnie **prawdopodobieństwo wystąpienia zagrożenia** w sposób wskazany na dwóch wykresach zamieszczonych poniżej tabeli na kolejnej stronie.

Wynik ten można powiązać z wynikiem oceny oddziaływania, co daje **ogólny wynik oceny ryzyka**, wskazany na kolejnym schemacie.

CZTERY GŁÓWNE OBSZARY OCENY, JEŻELI CHODZI O BEZPIECZEŃSTWO DANYCH:

A. Sieć i zasoby techniczne:	B. Procesy i procedury	C. Strony i ludzie zaangażowani w operację	D. Sektor i skala działalności
1. Czy jakakolwiek część przetwarzania danych	**6.** Czy rola i obowiązki dotyczące	**11.** Czy przetwarzanie danych wykonywane	**16.** Czy uważasz swój sektor działalności za

[338] *Idem*, slajd „*Understanding and evaluating impact*".
[339] *Idem*, slajdy na temat tych czterech głównych obszarów oceny wraz z dalszymi objaśnieniami, dlaczego w każdym z przypadków odpowiedź twierdząca na pytanie rodzi ryzyko bezpieczeństwa.

osobowych odbywa się przez internet?	przetwarzania danych osobowych są niejednoznaczne lub niejasno zdefiniowane?	jest przez nieokreśloną liczbę pracowników?	podatny na cyberataki?
2. Czy można zapewnić dostęp do wewnętrznego systemu przetwarzania danych osobowych przez internet (np. dla pewnych użytkowników lub grup użytkowników)?	**7.** Czy możliwe do zaakceptowanie użytkowanie sieci, systemu i zasobów fizycznych w ramach organizacji jest dwuznaczne lub niejasno zdefiniowane?	**12.** Czy jakakolwiek część operacji przetwarzania danych wykonywana jest przez wykonawcę/stronę trzecią (podmiot przetwarzający dane)?	**17.** Czy twoja organizacja ucierpiała z powodu cyberataku lub innego naruszenia bezpieczeństwa w ciągu ostatnich dwóch lat?
3. Czy system przetwarzania danych osobowych jest powiązany z innym wewnętrznym (w ramach organizacji) lub zewnętrznym systemem lub serwisem informatycznym?	**8.** Czy pracownikom wolno wnosić i użytkować swoje własne urządzenia podłączone do systemu przetwarzania danych osobowych?	**13.** Czy obowiązki stron/osób uczestniczących w przetwarzaniu danych osobowych są niejednoznaczne lub niejasno ustalone?	**18.** Czy w ostatnim roku otrzymałeś zgłoszenia i/lub skargi dotyczące bezpieczeństwa systemu informatycznego (wykorzystywanego do przetwarzania danych osobowych)?
4. Czy nieupoważnione osoby mogą łatwo uzyskać dostęp do środowiska przetwarzania danych?	**9.** Czy pracownikom wolno przekazywać, przechowywać lub w inny sposób przetwarzać dane osobowe poza obiektami organizacji?	**14.** Czy pracownicy uczestniczący w przetwarzaniu danych osobowych nie znają zasad bezpieczeństwa informacji?	**19.** Czy operacja przetwarzania dotyczy dużej ilości jednostek i/lub danych osobowych?
5. Czy system przetwarzania danych osobowych został zaprojektowany, wdrożony lub jest utrzymywany bez przestrzegania odpowiednich dobrych praktyk?	**10.** Czy czynności przetwarzania danych osobowych mogą być wykonywane bez utworzenia plików dziennika?	**15.** Czy osoby/strony uczestniczące w operacji przetwarzania danych zaniedbują bezpieczne przechowywanie i/lub niszczenie danych osobowych?	**20.** Czy istnieją jakiekolwiek dobre praktyki z zakresu bezpieczeństwa dotyczące konkretnie twojego sektora działalności, które nie są właściwie stosowane?

PRAWDOPODOBIEŃSTWO WYSTĄPIENIA ZAGROŻENIA (1):

Obszar oceny:	Liczba odpowiedzi „tak”	Poziom	Wynik
A. Sieć i zasoby techniczne:	0 – 1	Niski	**1**
	2 – 3	Średni	**2**
	4 – 5	Wysoki	**3**
B. Procesy i procedury	0 – 1	Niski	**1**
	2 – 3	Średni	**2**
	4 – 5	Wysoki	**3**
C. Strony i ludzie zaangażowani w operację	0 – 1	Niski	**1**
	2 – 3	Średni	**2**
	4 – 5	Wysoki	**3**
D. Sektor i skala działalności	0 – 1	Niski	**1**
	2 – 3	Średni	**2**
	4 – 5	Wysoki	**3**

Powyższe wyniki można następnie wprowadzić do następującego schematu podsumowującego:

PRAWDOPODOBIEŃSTWO WYSTĄPIENIA ZAGROŻENIA (2):

Ogólna SUMA wyników:	POZIOM PRAWDOPODOBIEŃSTWA wystąpienia zagrożenia:
4 – 5	**Niski**
6 – 8	**Średni**
9 – 12	**Wysoki**

W końcu, wyniki można połączyć z określonymi na pierwszym schemacie wynikami „poziomu oddziaływania”, by wskazać ogólne ryzyko:

OGÓLNA OCENA RYZYKA:

	POZIOM ODDZIAŁYWANIA			
PRAWDOPODOBIEŃSTWO WYSTĄPIENIA ZAGROŻENIA		**Niskie**	**Średnie**	**Wysokie/bardzo wysokie**
	Niskie			
	Średnie			
	Wysokie			

Legenda:

[ ] *Niskie ryzyko* [ ] *Średnie ryzyko* [ ] *Wysokie ryzyko*

NALEŻY JEDNAK ZAUWAŻYĆ, że powyższy schemat oceny ryzyka dotyczy głównie **ryzyk bezpieczeństwa danych**.

Jest to oczywiście główna kategoria ryzyka, którą należy ocenić i rozpatrzyć, i to nie tylko raz, ale stale, ponieważ ryzyko może ewoluować i ulegać z czasem mutacji. Zob. uwaga zatytułowana:

„Monitorowanie przestrzegania prawa: powtarzanie Zadań 1 - 3 (i 4) na bieżąco" na koniec omówienia Zadania 4, tuż przed Zadaniem 5, poniżej.

Jednak RODO wspomina także bardziej ogólnie „**ryzyko naruszenia praw i wolności osób fizycznych**" (patrz: art. 34, 35 i 36). Pierwszy z artykułów, art. 34, jasno przyjmuje, że naruszenie danych jako takie może prowadzić do tego typu ryzyka oraz nakłada istotne zasady radzenia sobie z tym ryzykiem, co zostało omówione w Zadaniu 4 (Ocena skutków dla ochrony danych), 5 (Zadanie dochodzeniowe), 10 (Współpraca z organem ochrony danych) oraz 12 (Zadanie informowania i podnoszenia świadomości).

Jednak należy zauważyć, że **„ryzyko naruszenia praw i wolności osób fizycznych" nie wypływa jedynie z naruszenia danych.** RODO przewiduje w art. 35(1), że tego rodzaju *„wysokie* ryzyko" może wynikać w szczególności z:

- systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną;
- przetwarzania na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1, lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10;

  lub
- systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.

W takich przypadkach *dokładnie dlatego, że takie operacje przetwarzania rodzą* ***z natury wysokie ryzyko*** *dla praw i wolności jednostek,* konieczna jest ocena skutków dla ochrony danych (a w niektórych przypadkach konsultacja z odpowiednim organem ochrony danych), co zostało omówione w następnym zadaniu.

Mówiąc konkretnie, oparte na profilach automatyczne podejmowanie decyzji może prowadzić do **nieuczciwych decyzji** (ponieważ nikt nie jest taki sam, jak inne osoby, i żaden system – miejmy nadzieję – nie wie wszystkiego o żadnej osobie) lub niedemokratycznych decyzji o **dyskryminujących i niemożliwych do zakwestionowania rezultatach**[340]**;** wykorzystanie wrażliwych danych może także prowadzić do **dyskryminacji** (celowej lub nie)[341]; wykorzystanie nawet pozornie niewinnych danych dotyczących sprzedaży może ujawnić intymne szczegóły dotyczące stanu zdrowia lub ciąży);[342] a systematyczne monitorowanie ludzi w miejscach publicznych może nieść za sobą **efekty zniechęcający do korzystania z takich podstawowych praw, jak prawo do wolności wypowiedzi, zrzeszania się i protestowania**.[343] W rzeczywistości ryzyko to można połączyć i następnie może ono mieć **wzajemnie wzmacniający** charakter, jak w przypadku stosowania technologii rozpoznawania twarzy przy monitorowaniu miejsc publicznych przez policję w celu „identyfikacji" groźnych ludzi i przewidywania złych zachowań[344].

Należy zauważyć, że aby takie ryzyko uległo materializacji, nie potrzeba naruszenia danych - ryzyko wynika z natury niebezpiecznych cech samych operacji przetwarzania, nawet jeżeli odbywa się ono zgodnie ze specyfikacją oraz bez naruszenia danych, o którym mowa w RODO. ***Nie uwzględnia tego***

[340] Zob. Douwe Korff & Marie Georges, Passenger Name Records, data mining & data protection: the need for strong safeguards, raport sporządzony dla report Komitetu Doradczego Rady Europy ds. Konwencji o ochronie jednostek w związku z automatycznym przetwarzaniem danych osobowych (T-PD), 2015, ust. I.iii, *The dangers inherent in data mining and profiling*, https://rm.coe.int/16806a601b

[341] To właśnie dlatego w europejskich instrumentach ochrony danych uwzględniono specjalne i szczególnie restrykcyjne zasady przetwarzania danych osobowych – zob. Uwaga w części 1, pkt 1.2.3 na str. 17 powyżej.

[342] Zob. *How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did*, Forbes, 16 lutego 2012 r. https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#2ea04af16668.

[343] Zob. cytat ze słynnego wyroku niemieckiego trybunału konstytucyjnego w sprawie *Census* na str. 10 Podręcznika.

[344] Zob. Douwe Korff, *First Do No Harm: he potential of harm being caused to fundamental rights and freedoms by state cybersecurity interventions*, ust. 2.4, *Preventive, predictive policing*, w: Ben Wagner, Matthias C. Kettemann i Kilian Vieth (red.), Research Handbook on Human Rights & Digital Technology: Global Politics, Law & International Relations, Ośrodek ds. Internetu i Praw Człowieka, Berlin, do publikacji pod koniec 2018 roku.

opracowany przez Garante i odtworzony powyżej schemat oceny ryzyka (bardzo przydatny w innych celach).

To samo dotyczy mniejszego „ryzyka naruszenia praw i wolności osób fizycznych" wynikającego z operacji przetwarzania, których nie wymieniono jako operacje z natury rodzące „wysokie ryzyko". Mowa tu w szczególności o operacjach przetwarzania, które nie spełniają wszystkich wymogów RODO.

PRZYKŁADY:

- Wykorzystywanie danych osobowych zgromadzonych w jednym celu w innym „niekompatybilnym" celu bez właściwej podstawy prawnej w związku z drugorzędnym przetwarzaniem i/lub bez właściwego poinformowania osób, których dane dotyczą, o planowanym drugorzędnym zastosowaniu ich danych - co byłoby jeszcze gorsze, gdyby ujawniano takie dane stronie trzeciej.

➢ W ten sposób odmawia się osobom, których dane dotyczą, możliwości wyrażenia zgody (lub sprzeciwu) wobec drugorzędnego przetwarzania, które może mieć na nie niekorzystny wpływ (np. w podaniach o pracę lub wnioskach kredytowych). Istnieje także dość duże prawdopodobieństwo, że dane osobowe uzyskane w jednym kontekście nie są wystarczająco dokładne lub odpowiednie do stosowania w całkiem innym kontekście.

- Zatrzymanie i/lub wykorzystywanie danych osobowych (z reguły gdy nie są one już potrzebne w pierwotnym celu) w formie pseudonimów lub w anonimowej formie (z reguły w celu dalszego wykorzystania w takiej formie w nowym, drugorzędnym celu).

➢ Biorąc pod uwagę rosnące ryzyko ponownej identyfikacji nawet rzekomo w pełni anonimowych danych[345], każde tego typu zatrzymanie i wykorzystywanie danych w formie pseudonimów lub rzekomo anonimowych danych należy traktować jako stworzenie zagrożenia dla praw i wolności osób, których dane dotyczą, (co może nawet prowadzić do „wysokiego ryzyka", wymagającego przeprowadzenia oceny skutków dla ochrony danych, którą omówiono w Zadaniu 4). Inspektor ochrony danych powinien starannie sprawdzić ryzyko ponownej identyfikacji takich danych w każdym konkretnym zastosowaniu oraz nałożyć w odpowiednich sytuacjach zdecydowane środki łagodzące (takie jak „zróżnicowana prywatność")[346] lub odmówić wydania pozwolenia na dalsze przetwarzanie danych.

- Wykorzystywanie nieistotnych lub nieaktualnych informacji - z możliwymi podobnymi negatywnymi konsekwencjami.

- Nieprzywiązywanie wagi do „interesów lub podstawowych praw i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem", w trakcie oceny, czy dane osobowe są przetwarzane zgodnie z zasadą „uzasadnionego interesu" (art. 6(1)(f) RODO).

➢ To z definicji stwarza zagrożenie dla interesów osób, których dane dotyczą. Zastosowanie kryterium „uzasadnionego interesu" jako podstawy prawnej przetwarzania zawsze wymaga więc od inspektora ochrony danych w ramach omawianego zadania szczególnie dokładnej analizy.

➢ **Uwaga:** Kryterium to nie może być uzależnione od organów publicznych w trakcie realizacji swoich zadań (art. 6(1), ostatnie zdanie), ale to nie oznacza, że problem ten nigdy nie będzie miał miejsca w sektorze publicznym, np. w odniesieniu do zadań niewymaganych ustawowo, takich jak wysyłanie do obywateli pocztą elektroniczną informacji o wydarzeniach kulturalnych, wykorzystywanie rejestrów populacji, albo w odniesieniu do działalności prywatnych podmiotów wykonujących zadania „w interesie publicznym".

[345] Proste podsumowanie kwestii dotyczących pozbawiania danych elementów pozwalających na identyfikację oraz ponownej identyfikacji – zob. dokument przedstawiony brytyjskiemu rządowi przez Foundation for Information Policy Research „Making Open Data Real", październik 2011 r. - www.fipr.org/111027opendata.pdf. Nawiązuje on do dokumentu: Paul Ohm, Broken promises of privacy: responding to the surprising failure of anonymization, 57 UCLA Law Review (2010) 1701, http://papers.ssrn.com/sol3/paperscfm?abstract_id=1450006.

[346] Zróżnicowana prywatność to istotny środek zapobiegania ponownej identyfikacji osób, których dane dotyczą, z baz danych, ale działa on tylko wtedy, gdy jest stosowany w kontrolowanym środowisku, w którym badacze mają ograniczone możliwości wysyłania zapytań do bazy danych, zob. link: https://privacytools.seas.harvard.edu/differential-privacy; https://people.eecs.berkeley.edu/~stephentu/writeups/6885-lec20-b.pdf. Nie daje on odpowiedzi na pytanie dotyczące okoliczności, w jakich dane osobowe są przekazywane opinii publicznej w rzekomo w pełni anonimowej formie, lub w której dużej bazie danych są w inny sposób łączone bez pełnej kontroli.

- Niewłaściwe poinformowanie osób, których dane dotyczą, o wszystkich szczegółach, jakie należy im przekazać zgodnie z art. 13 i 14 RODO.

➢ Może to spowodować, że osoby, których dane dotyczą, nie będą w stanie w pełni korzystać ze swoich praw wynikających z RODO (które oczywiście stanowią właśnie te „interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych", które należy chronić).

- Przekazanie danych osobowych do kraju trzeciego, w przypadku którego ustalono, że nie zapewnia „odpowiedniej" ochrony danych osobowych, bez wprowadzenia właściwych zabezpieczeń lub zestawu zatwierdzonych Wiążących reguł korporacyjnych lub bez zastosowania jednego z określonych odstępstw (zob. art. 46-48 RODO). Obejmuje to usługę w chmurze, która wykorzystuje serwer (albo serwery) znajdujący się w takim kraju trzecim.

➢ Jak wskazał Europejski Inspektor Ochrony Danych w swojej szczegółowej poradzie dotyczącej korzystania z usług w chmurze przez instytucje UE (z którą powinny się także zapoznać krajowe organy publiczne, ponieważ znaczna część tej porady może mieć również do nich zastosowanie), chmura obliczeniowa rodzi konkretne ryzyko, którym powinni się bardzo starannie zająć administratorzy danych (polegając na swoich inspektorach ochrony danych)[347]. Faktycznie, jego porada sugeruje, że chmura rozliczeniowa może być także traktowana jako rozwiązanie z natury rodzące wysokie ryzyko i tym samym wymagające przeprowadzenia oceny skutków dla ochrony danych. Wspomniano o tym w kolejnym zadaniu.

- Zlecanie przetwarzania danych osobowych przez organy publiczne podmiotom zewnętrznym, w szczególności, gdy dane takie mają wrażliwy charakter w ujętym w RODO sensie techniczno-prawnym („szczególne kategorie danych" - art. 9) lub są wrażliwe w ogólnym sensie, takie jak dane finansowe lub dane dotyczące spisu ludności.

➢ Europejski Inspektor Ochrony Danych zauważa, że korzystanie z usług w chmurze potęguje ryzyko z natury związane ze zlecaniem przetwarzania podmiotom zewnętrznym[348].

Jeżeli po przeprowadzeniu oceny, zdaniem inspektora ochrony danych operacja przetwarzania danych osobowych stwarza ryzyko dla odpowiednich interesów, jest on zobowiązany **zgłosić** takie ryzyko odpowiedzialnej osobie lub odpowiedzialnym osobom w ramach organizacji oraz zaproponować **łagodzące lub alternatywne działania.** Często zgodny z prawem cel można osiągnąć poprzez zastosowanie innych, mniej inwazyjnych środków albo poprzez zastosowanie mniejszej liczby (i mniej wrażliwych) danych, a w takich przypadkach inspektor ochrony danych powinien zdecydowanie to zaproponować. Jeżeli jego rada nie zostanie wprowadzona w życie, inspektor ochrony danych powinien **przekazać** sprawę najwyższemu kierownictwu (patrz poniżej: punkt zatytułowany „*Zadania doradcze*").

Inspektor ochrony danych powinien prowadzić pełne **rejestry** wszystkich swoich tego typu ocen ryzyka oraz swoich porad.

Jeżeli porada inspektora ochrony danych została zastosowana, rejestry będą „**wykazywać**, że przetwarzanie odbywa się zgodnie z tym Rozporządzeniem", tj. że ryzyko zostało faktycznie ocenione oraz że środki podjęte w świetle takiej oceny były odpowiednie dla tego typu ryzyka (art. Art. 24(1) oraz dyskusja na temat „obowiązku wykazania" zgodności z RODO w pkt 2.2 powyżej).

Należy zauważyć, że jeżeli ogólna ocena ryzyka wskazuje, że proponowane przetwarzanie rodzi prawdopodobnie „**wysokie ryzyko**" dla praw i wolności jednostek, inspektor ochrony danych powinien poinformować administratora, że konieczna jest pełna ocena skutków dla ochrony danych, którą omówiono w Zadaniu 4.

[347] Europejski Inspektor Ochrony Danych (EDPS), Wytyczne dotyczące korzystania z usług w chmurze przez instytucje i organy europejskie (Guidelines on the use of cloud computing services by the European institutions and bodies), marzec 2018, https://edps.europa.eu/sites/edp/files/publication/18-03-16_cloud_computing_guidelines_en.pdf. Zob. w szczególności Załącznik 4: Ryzyko dotyczące ochrony danych w przypadku usług w chmurze (Data protection-specific risks of cloud computing).

[348] Wytyczne Europejskiego Inspektora Ochrony Danych dotyczące korzystania z usług w chmurze przez instytucje i organy europejskie (Guidelines on the use of cloud computing services by the European institutions and bodies) (poprzedni przypis) „koncentrują się na korzystaniu z usług w chmurze oferowanych przez podmioty handlowe [ale] jako takie dotyczą także - naturalnie - kwestii wynikających z podzlecania usług informatycznych związanych z przetwarzaniem danych." (str. 5).

Należy zauważyć, że nawet jeżeli ocena skutków dla ochrony danych nie jest konieczna, inspektor ochrony danych musi w dalszym ciągu na bieżąco monitorować operacje przetwarzania danych osobowych przez administratora - patrz dyskusja w Zadaniu 4, w punkcie zatytułowanym *„Monitorowanie przestrzegania prawa: powtarzanie Zadań 1 - 3 (i 4) na bieżąco”.*

Należy także zauważyć, że często krajowi ustawodawcy podjęli już próbę rozwiązania problemu szczególnego ryzyka, jakie ich zdaniem wynika ze szczególnych czynności przetwarzania, w przepisach krajowych, co może być w większym zakresie kontynuowane w ramach „określonych klauzul” postanowień RODO.[349]

Przykłady:

W **Chorwacji** zabroniono przetwarzania danych genetycznych do obliczania ryzyka zachorowania oraz innych aspektów zdrowia osób, których dane dotyczą, w związku z zawarciem lub wykonaniem umów ubezpieczenia na życie oraz umów zawierających klauzule o przetrwaniu. Zakaz taki nie może zostać zniesiony na podstawie zgody osoby, której dane dotyczą (art. 20 ustawy wdrażającej RODO).

W innych krajach stosowanie ***danych biometrycznych*** oraz ***kamer telewizji przemysłowej*** także podlega określonym warunkom, takim jak wymóg szczególnie wyraźnej i jednoznacznej zgody, oraz ograniczeniom, takim jak limit dotyczące zatrzymywania danych.

Wszystkie tego typu warunki prawne należy oczywiście wziąć pod uwagę przy ocenie ryzyka - żaden administrator danych ani inspektor ochrony danych nie może oczywiście nigdy stwierdzić, że ryzyko jest możliwe do przyjęcia, mimo że nie spełniono szczególnych warunków i ograniczeń przewidzianych prawem.

- o – O – o -

[349] Zob. Część druga, pkt 2.2.

ZADANIE 4 Radzenie sobie z operacjami, które mogą powodować „wysokie ryzyko": przeprowadzanie oceny skutków dla ochrony danych

To, co powiedziano powyżej na temat ogólnej oceny ryzyka (Zadanie 3) dotyczy *a fortiori* operacji przetwarzania danych osobowych, które na podstawie takiej ogólnej oceny ryzyka uznano za mogące powodować „**wysokie ryzyko** naruszenia praw i wolności osób fizycznych" (art. 35(1)). RODO wyjaśnia, że sytuacja taka może mieć w szczególności miejsce, gdy stosowane są „nowe technologie".

Jeżeli wstępna ocena ryzyka przeprowadzona w Zadaniu 3 wskazała, że konkretna operacja przetwarzania danych osobowych faktycznie może powodować „wysokie ryzyko", wtedy administrator jest zobowiązany przeprowadzić **ocenę skutków dla ochrony danych** przed przystąpieniem do takiej operacji.

RODO przewiduje, że ocena skutków dla ochrony danych musi mieć miejsce w szczególności w przypadku w pełni zautomatyzowanego/opartego na profilowaniu procesu decyzyjnego, przetwarzania na dużą skalę wrażliwych danych lub monitorowania na dużą skalę miejsc dostępnych publicznie (art. 35(3)). Krajowe organy ochrony danych muszą także opracować wykaz rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny skutków dla ochrony danych na ich terytorium oraz mogą przyjąć wykazy operacji niepodlegających takiemu wymogowi. Obydwa wykazy należy przekazać Europejskiej Radzie Ochrony Danych i mogą zostać zakwestionowane przez inne organy ochrony danych w ramach przewidzianego w RODO „mechanizmu spójności" (art. 35(4) - (6)). RODO zezwala także Europejskiej Radzie Ochrony Danych na wydanie we własnym zakresie wykazu operacji podlegających i niepodlegających ocenie w oparciu o wykazy przekazane jej przez krajowe organy ochrony danych (które są zobowiązane to uczynić na mocy art. 64(1)(a) RODO).

W praktyce, to, co miało miejsce, to po pierwsze Grupa Robocza Art. 29 wydała szeroką poradę i wytyczne dotyczące oceny skutków dla ochrony danych, zarówno w swoich Wytycznych dotyczących inspektorów ochrony danych z grudnia 2016 roku, w wersji z kwietnia 2017 roku (WP243 wer. 1)[350], jak i w późniejszych, bardziej szczegółowych Wytycznych dotyczących oceny skutków dla ochrony danych, przyjętych 4 kwietnia 2017 r. oraz w skorygowanej formie 4 października 2017 r. (tj. w każdym przypadku przed stosowaniem RODO)[351]. W obydwu przypadkach wytyczne zostały zatwierdzone przez Europejską Radę Ochrony Danych w dniu wejścia w życie RODO, tj. 25 maja 2018 r.[352] Europejski Inspektor Ochrony Danych także przedstawił dalsze wytyczne w swoim dokumencie poświęconym rozliczalności[353], z uwzględnieniem wstępnego wykazu czynności przetwarzania, które jego zdaniem wymagają lub nie wymagają oceny skutków dla ochrony danych[354].

Skorygowane wytyczne dotyczące oceny skutków dla ochrony danych, przyjęte przez Grupę Roboczą Art. 29 i zatwierdzone przez EDPB, określają **dziewięć kryteriów**, jakie należy wziąć pod uwagę przy ustalaniu, czy czynność przetwarzania może powodować „wysokie ryzyko", tj.[355]:

> ***W większości przypadków*** administrator danych może przyjąć, że przetwarzanie spełniające **dwa kryteria** wymaga przeprowadzenia oceny skutków dla ochrony danych. Ogólnie rzecz ujmując, Grupa Robocza Art. 29 jest zdania, że im więcej kryteriów spełnia przetwarzanie, tym większe prawdopodobieństwo wystąpienia wysokiego ryzyka dla praw i swobód osób, których dane dotyczą, w związku z czym konieczne jest przeprowadzenie oceny skutków dla ochrony danych bez względu na środki, jakie administrator danych planuje przyjąć.

Kwestia ta została bardziej szczegółowo omówiona w punkcie zatytułowanym *„W jaki sposób ocenić, czy proponowana operacja przetwarzania może powodować „wysokie ryzyko",* gdzie przedstawiono

---

[350] Zob. przypis 242 powyżej.

[351] WP29 Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" dla celów Rozporządzenia 2016/679 (WP248 wer. 1, dalej zwane Wytycznymi Grupy Roboczej Art. 29 w sprawie oceny skutków dla ochrony danych), strona spisu treści, http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

[352] Zob. przypis 215 powyżej.

[353] EDPS, Accountability on the ground Part I: Records, Registers and when to do Data Protection Impact Assessments, (przypis 302 powyżej), ust. 4 *When to carry out a DPIA?,* str. 9-11.

[354] *Idem*, Załącznik 5.

[355] Wytyczne Grupy Roboczej Art. 29 dotyczące oceny skutków dla ochrony danych (przypis 351 powyżej), str. 11, dodano podkreślenie.

przykłady zaczerpnięte z Wytycznych Grupy Roboczej Art. 29 oraz dokumentu EDPS w podpunkcie zatytułowanym *„Czynniki wskazujące na istnienie <wysokiego ryzyka>”.*

W tym miejscu należy zauważyć, że większość krajowych organów ochrony danych (22 z 28)[356] przyjęło swoje własne wstępne listy i przekazało je do wglądu EDPB. EDPB dokonała ich przeglądu w świetle zatwierdzonych przez siebie Wytycznych Grupy Roboczej Art. 29 i 25 września wydała 22 na temat przedstawionych jej wykazów (na temat każdego projektu).[357] Głównym punktem poruszonym konsekwentnie przez EDPB w wyżej wspomnianych opiniach była skierowana do organów ochrony danych rekomendacja nieuwzględniania w wykazach czynności przetwarzania, w przypadku których ocena skutków dla ochrony danych jest obowiązkowa, jeżeli dana czynność spełnia tylko *jedno* z kryteriów ustalania prawdopodobieństwa „wysokiego ryzyka”, o których mowa w Wytycznych. Tak więc, na przykład, w swojej opinii na temat projektu wykazu przedłożonego przez Zjednoczone Królestwo EDPB stwierdza, że[358]:

> Wykaz przedstawiony przez Organ nadzorczy Zjednoczonego Królestwa do zaopiniowania przez państwa będące członkami Rady przewiduje, że przetwarzanie danych biometrycznych podlega z zasady obowiązkowi przeprowadzenia oceny skutków dla ochrony danych. Rada jest zdania, że samo przetwarzanie danych biometrycznych niekoniecznie rodzi wysokie ryzyko. Jednak przetwarzanie danych biometrycznych w celu unikalnej identyfikacji osoby fizycznej w powiązaniu z co najmniej jednym z pozostałych kryteriów takiej oceny wymaga. Rada wnioskuje do Organu nadzorczego Zjednoczonego Królestwa o odpowiednie skorygowanie wykazu poprzez dodanie pozycji określającej, że przetwarzanie danych biometrycznych w celu unikalnej identyfikacji osoby fizycznej wymaga oceny skutków dla ochrony danych wyłącznie wtedy, gdy jest powiązane z co najmniej jednym z pozostałych kryteriów, bez uszczerbku dla postanowień art. 35(3) RODO.

Oczywiście ocena skutków dla ochrony danych może, ale nie musi, zostać jednak przeprowadzona przez administratora danych, nawet jeżeli spełniono tylko jedno z kryteriów.

Wymóg przeprowadzenia oceny skutków dla ochrony danych można pominąć w przypadku, gdy prawo reguluje kwestie dotyczące danego rodzaju operacji, a w kontekście jego przyjęcia przeprowadzono ogólną ocenę skutków dla ochrony danych (art. 35(10)). Ponadto „dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę” (art. 35(1), ostatnie zdanie). Jak podsumowuje to Grupa Robocza Art. 29[359]:

> Kiedy ocena skutków dla ochrony danych nie jest wymagana? Gdy przetwarzanie najprawdopodobniej nie rodzi wysokiego ryzyka lub istnieje podobna ocena skutków dla ochrony danych, lub zostało ono zatwierdzone przed majem 2018 roku, lub posiada podstawę prawną, lub znajduje się w wykazie operacji przetwarzania, dla których ocena skutków dla ochrony danych nie jest wymagana.

Szczegółowe wskazówki na temat oceny skutków dla ochrony danych, z uwzględnieniem wskazówek metodologicznych, wydały także krajowe organy ochrony danych, z uwzględnieniem tego typu organów we Francji, Hiszpanii i Zjednoczonym Królestwie, a także niemiecki *Datenschutzzentrum* (zatwierdzony przez niemieckie organy ochrony danych)[360]. **Francuski** organ ochrony danych, CNIL, opracował nawet (we współpracy z innymi organami ochrony danych) oprogramowanie typu open source do oceny skutków dla ochrony danych, którego celem jest pomaganie administratorom danych w budowaniu i wykazywaniu zgodności z RODO. Jak wyjaśniono na stronie[361]:

---

[356] Austria, Belgia, Bułgaria, Czechy, Niemcy, Estonia, Grecja, Finlandia, Francja, Węgry, Irlandia, Włochy, Litwa, Łotwa, Malta, Holandia, Polska, Portugalia, Rumunia, Szwecja, Słowacja i Zjednoczone Królestwo.

[357] Wszystkie dostępne w ramach linków na stronie: https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_en

[358] EDPB, Opinia 22/2018 na temat projektu wykazu właściwego organu nadzorczego Zjednoczonego Królestwa w sprawie czynności przetwarzania podlegających wymogowi przeprowadzenia oceny skutków dla ochrony danych (art. 35.4 RODO), przyjęta 25 września 2018 roku, zob. link: https://edpb.europa.eu/sites/edpb/files/files/file1/2018-09-25-opinion_2018_art._64_uk_sas_dpia_list_en.pdf.

[359] Wytyczne Grupy Roboczej Art. 29 dotyczące oceny skutków dla ochrony danych (przypis 351 powyżej), strona spisu treści, str. 6.

[360] Zob. wykaz z linkami w Załączniku *1* do Wytycznych Grupy Roboczej Art. 29 dotyczących oceny skutków dla ochrony danych (przypis 351 powyżej). Metodologie oceny skutków dla ochrony danych omówiono bardziej szczegółowo poniżej.

[361] Dostępne wraz z informacjami w języku angielskim na stronie https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment.

Kto może korzystać z oprogramowania do oceny skutków dla prywatności?

Narzędzie to kierowane jest do administratorów danych, którzy odrobinę znają się na procesie oceny skutków dla prywatności. W tym względzie samodzielną wersję można pobrać i w łatwy sposób uruchomić na swoim komputerze.

Narzędzie to może być także wykorzystywane na serwerach organizacji w celu integracji z innymi narzędziami i systemami już wykorzystywanymi w ramach firmy.

Co to jest?

Narzędzie do oceny skutków dla prywatności zostało zaprojektowane w oparciu o trzy zasady:

- **Dydaktyczny interfejs do przeprowadzania oceny skutków dla prywatności -** narzędzie to bazuje na przyjaznym użytkownikowi interfejsie umożliwiającym proste zarządzanie ocenami skutków dla prywatności. W jasny sposób krok po kroku prezentuje metodologię oceny skutków dla prywatności. Kilka narzędzi wizualizacyjnych pozwala szybko zrozumieć ryzyko.
- **Baza wiedzy prawnej i technicznej** - narzędzie to uwzględnia kwestie prawne zapewniające zgodność przetwarzania i praw osób, których dane dotyczą, z prawem. Obejmuje także kontekstową bazę wiedzy dostępną na wszystkich etapach oceny, dostosowującą się do prezentowanych treści. Dane są pobierane z RODO, przewodnika po ocenie skutków dla prywatności oraz opracowanego przez CNIL Przewodnika bezpieczeństwa w odniesieniu do analizowanego aspektu przetwarzania.
- **Narzędzie modularne** - zaprojektowane, by pomóc w budowaniu zgodności, z możliwością dostosowania zawartości do konkretnych potrzeb i konkretnego sektora działalności, na przykład poprzez stworzenie modelu oceny, który można powielać i wykorzystywać dla szeregu podobnych operacji przetwarzania. Narzędzie jest publikowane w ramach darmowej licencji i umożliwia modyfikację kodu źródłowego w celu dodawania funkcji lub wprowadzenia go w narzędzia wykorzystywane w ramach organizacji.

W niniejszym Podręczniku nie ma miejsca na uwzględnienie wszystkich szczegółowych porad dotyczących oceny skutków dla ochrony danych przewidzianych w późniejszych, bardziej konkretnych (zatwierdzonych przez Europejską Radę Ochrony Danych) Wytycznych Grupy Roboczej Art. 29 dotyczących oceny skutków dla ochrony danych lub w wytycznych krajowych. **Zdecydowanie zachęca się czytelników do zapoznania się z Wytycznymi Grupy Roboczej Art. 29/Europejskiej Rady Ochrony Danych oraz tam, gdzie to stosowne, odpowiednimi poradami krajowymi oraz polegania na nich w swoich działaniach i przeprowadzanych konsultacjach**[362]**.**

Użytkownicy niniejszego Podręcznika oraz w szczególności inspektorzy ochrony danych powinni także wziąć pod uwagę krajowy obowiązkowy wykaz czynności podlegających ocenie skutków dla ochrony danych, opublikowany przez odpowiedni organ ochrony danych jako wykaz zawierający przykłady sytuacji, w których stosowanie powyższych wskazówek i porad prowadzi do konieczności wykonania oceny zarówno przez podmioty publiczne, jak i prywatne. Inspektorzy ochrony danych powinni nadzorować przeprowadzenie oceny przez właściwych administratorów danych za każdym razem, gdy uprawniają ich do tego wyżej wspomniane wykazy. Jeżeli w następnych miesiącach wydano także „białe wykazy" (zgodnie z art. 35(5) RODO), będą one pomocne, ponieważ wykluczają potrzebę angażowania administratora w przeprowadzanie oceny czynności przetwarzania niskiego ryzyka.

Poniżej krótko omówimy wytyczne w zakresie: **różnych ról i obowiązków administratora i inspektora ochrony danych**, kwestii, **w jaki sposób należy ocenić, czy proponowana operacja przetwarzania może spowodować „wysokie ryzyko", metodologii oceny skutków dla ochrony danych oraz tego, co należy zrobić z rejestrami oceny skutków dla ochrony danych**, w szczególności jeżeli stwierdzono, że pewnego

CNIL stosuje krótszy akronim PIA (także zacytowany w tekście powyżej), prawdopodobnie dlatego że ocena skutków dla ochrony danych wywodzi się z oceny skutków dla prywatności. Należy zauważyć, że narzędzie to zostało ostatnio zaktualizowane. Informacje na temat aktualizacji dostępne są tutaj (wyłącznie w języku angielskim): https://www.cnil.fr/fr/loutil-pia-mis-jour-pour-accompagner-lentree-en-application-du-rgpd. Na tej stronie CNIL informuje, że oprogramowanie jest dostępne w 14 językach: francuskim, angielskim, włoskim, niemieckim, polskim, węgierskim, fińskim, norweskim, hiszpańskim, czeskim, holenderskim, portugalskim, rumuńskim i greckim oraz że zostało zatwierdzone (przynajmniej warunkowo w wersji beta) przez organy ochrony danych Bawarii, Włoch, Finlandii, Węgier, Polski i Norwegii. Należy jednak zauważyć, że oprogramowanie to skupia się przede wszystkim na bezpieczeństwie technicznym i będzie głównie przydatne dla małych i średnich przedsiębiorstw, a nie dużych i bardziej złożonych podmiotów.

[362] Zob. przypisy 249, 318, 351 i 353 oraz główna porada do przeanalizowania w poprzednim przypisie.

ustalonego wysokiego ryzyka nie można w pełni złagodzić, stosując różne możliwe środki, w którym to przypadku RODO **wymaga konsultacji z odpowiednim organem ochrony danych** (art. 36).

Różne role i obowiązki administratora i inspektora ochrony danych w związku z oceną skutków dla ochrony danych

W swoich Wytycznych dotyczących inspektorów ochrony danych Grupa Robocza Art. 29 ponownie podkreśliła odrębne role i obowiązki administratora i inspektora ochrony danych, także w związku z oceną skutków dla ochrony danych. Napisała, że[363]:

> 4.2. Rola inspektora ochrony danych w ocenie skutków dla ochrony danych
>
> Zgodnie z artykułem 35(1) do obowiązków administratora, a nie inspektora ochrony danych, należy przeprowadzanie w określonych przypadkach oceny skutków dla ochrony danych. Jednak inspektor ochrony danych może odgrywać istotną rolę i wspierać administratora przy przeprowadzaniu takiej oceny. Zgodnie z zasadą ochrony danych w fazie projektowania, artykuł 35(2) nakłada na administratora obowiązek konsultowania się z inspektorem ochrony danych przy dokonywaniu oceny skutków dla ochrony danych. Natomiast z art. 39(1)(c) wynika obowiązek DPO „*udzielania na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wyników*".
>
> Grupa Robocza Art. 29 zaleca, że administrator powinien skonsultować się z inspektorem ochrony danych między innymi w następujących kwestiach[364]:
>
> - faktu, czy należy przeprowadzić ocenę skutków dla ochrony danych;
> - metodologii przeprowadzenia oceny skutków dla ochrony danych;
> - faktu, czy należy przeprowadzić wewnętrzną ocenę skutków dla ochrony danych czy też zlecić ją podmiotowi zewnętrznemu;
> - zabezpieczeń (w tym środków technicznych i organizacyjnych) stosowanych do łagodzenia wszelkich zagrożeń praw i interesów osób, których dane dotyczą;
> - prawidłowości przeprowadzonej oceny skutków dla ochrony danych i zgodności jej wyników z RODO (czy należy kontynuować przetwarzanie czy też nie oraz jakie zabezpieczenia należy zastosować).
>
> Jeśli administrator nie zgadza się z zaleceniami inspektora ochrony danych, dokumentacja oceny skutków dla ochrony danych powinna zawierać pisemne uzasadnienie nieuwzględnienia tych zaleceń[365].
>
> Grupa Robocza Art. 29 rekomenduje, by administrator jasno, np. w umowie z inspektorem ochrony danych, ale również w informacjach przekazywanych pracownikom, kierownikom i innym, wskazał zakres obowiązków inspektora ochrony danych w danej organizacji, w szczególności w kontekście przeprowadzania oceny skutków dla ochrony danych.

Późniejsze Wytyczne Grupy Roboczej Art. 29 dotyczące oceny skutków dla ochrony danych podkreślają także, że ocena taka musi zostać przeprowadzona przez „administratora wraz z inspektorem ochrony danych i podmiotami przetwarzającymi"[366].

W praktyce w szczególności w mniejszych organizacjach inspektor ochrony danych będzie często odgrywać wiodącą rolę w ocenie.

W jaki sposób ocenić, czy zaproponowana operacja przetwarzania danych może powodować „wysokie ryzyko"

[363] Wytyczne Grupy Roboczej Art. 29 dotyczące inspektorów ochrony danych (przypis 242 powyżej), pkt 4.2, str. 16 – 17, pochyła czcionka zgodnie z oryginałem, dodano podkreślenie w ostatnim paragrafie.

[364] Artykuł 39(1) w wersji angielskiej stanowi, że „do obowiązków DPO należy co najmniej" („DPO shall have 'at least' the following tasks"). W związku z tym nie ma przeciwwskazań, by zwiększyć zakres obowiązków DPO, albo doprecyzować te wskazane w art. 39(1). [oryginalny przypis]

[365] Art. 24(1) przewiduje, że „*Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane".* [oryginalny przypis, dodano pochyłą czcionkę]

[366] Zob. Wytyczne Grupy Roboczej Art. 29 dotyczące oceny skutków dla ochrony danych (przypis 351 powyżej), ust. III.D.b).

Grupa Robocza Art. 29/Europejska Rada Ochrony Danych wyjaśniają, że[367]:

> Spoczywający na administratorach obowiązek przeprowadzenia oceny skutków dla ochrony danych w niektórych okolicznościach należy rozumieć w odniesieniu do ich ogólnego obowiązku właściwego zarządzania ryzykiem wynikającym z przetwarzania danych osobowych - tj.

jak również zauważono powyżej, kwestia, czy należy wykonać ocenę skutków dla ochrony danych w naturalny sposób wynika z ogólnego obowiązku administratora - wykonywanego za „poradą", ale w praktyce z zasady w zależności od inspektora ochrony danych, by ocenić ryzyko nieodłącznie związane z realizowanymi przez administratora operacjami przetwarzania danych osobowych (Zadanie 3).

Następnie wyjaśniono koncepcję „ryzyka" oraz chronionych interesów, jakie należy wziąć pod uwagę[368]:

> „Ryzyko" jest scenariuszem opisującym wydarzenie i jego konsekwencje szacowane pod względem stopnia wagi zdarzenia i prawdopodobieństwa. „Zarządzanie ryzykiem" z drugiej strony można zdefiniować jako skoordynowane działania mające na celu kierowanie organizacją i kontrolowanie organizacji pod względem ryzyka.
>
> Artykuł 35 odnosi się do wysokiego ryzyka naruszenia „praw lub wolności osób fizycznych". Jak wskazano w oświadczeniu Grupy Roboczej Artykułu 29 ds. Ochrony Danych, odniesienie do "praw i wolności" osób, których dane dotyczą, dotyczy przede wszystkim prawa do prywatności, ale może także obejmować inne podstawowe prawa, takie jak wolność słowa, wolność myśli, swoboda przemieszczania się, zakaz dyskryminacji, prawo do wolności, sumienia i religii.

Grupa Robocza Art. 29 wskazuje na zawarte w art. 35(3) RODO przykłady postanowień, które z natury rodzą „wysokie ryzyko", gdy administrator stosuje zautomatyzowane i oparte na profilowaniu algorytmy do podejmowania decyzji wywołujących skutki prawne lub inne istotne skutki, gdy administrator przetwarza wrażliwe dane lub dane dotyczące wyroków skazujących i naruszeń prawa „na dużą skalę" lub gdy administrator systematycznie monitoruje miejsca dostępne publicznie „na dużą skalę". Prawidłowo dodaje też[369]:

> Jak wskazują słowa „w szczególności" we wprowadzającym zdaniu artykułu 35(3) RODO, chodzi tu o niewyczerpujący wykaz. Mogą istnieć operacje przetwarzania o „wysokim ryzyku", które nie są objęte tym wykazem, ale jednak wiążą się z podobnym wysokim ryzykiem Takie operacje przetwarzania również powinny podlegać ocenie skutków dla ochrony danych.

Grupa Robocza Art. 29 wymienia szereg czynników - w większości, ale nie w każdym przypadku, związanych z trzema przykładami zawartymi w art. 35 - które sugerują, że operacja przetwarzania rodzi „wysokie ryzyko" i dodatkowo podaje konkretne przykłady. Europejski Inspektor Ochrony Danych podaje dalsze przykłady, zarówno w swoim wstępnym wykazie operacji przetwarzania, które zawsze wymagają oceny skutków dla ochrony danych, jak i w szablonie, który można stosować do oceny, czy operacje przetwarzania, które nie figurują ani na liście „pozytywnej" (operacje, które zawsze wymagają oceny), ani na liście „negatywnej" (operacje, które nie wymagają oceny), powinny zostać poddane ocenie skutków dla ochrony danych[370]. Zaprezentowane przez Grupę Roboczą Art. 29 i Europejskiego Inspektora Ochrony Danych przykłady podano poniżej (po edycji, przy czym przykłady Grupy Roboczej Art. 29 usunięto z tekstu i przeniesiono do ramki, a przykłady Europejskiego Inspektora Ochrony Danych oznaczono*). Dodaliśmy jeszcze kilka dalszych przykładów (lub szczegółów albo zmian) mających w szczególności znaczenie dla administratorów w sektorze publicznym. Przykłady te zostały zapisane pochyłą czcionką.

Czynniki wskazujące na „wysokie ryzyko"[371]

---

[367] *Idem*, str. 6.

[368] *Idem*. Należy zauważyć także wcześniejsze odwołanie do ISO 31000:2009*, Zarządzanie ryzykiem - Zasady i Wytyczne*, International Organization for Standardization (ISO); ISO/IEC 29134 (projekt), *Technologia informatyczna – Techniki bezpieczeństwa – Ocena skutków dla prywatności – Wytyczne*, International Organization for Standardization (ISO) (Wytyczne Grupy Roboczej Art. 39 dotyczące ocena skutków dla ochrony danych, przypis 351, na str. 5).

[369] *Idem*, str. 9.

[370] „Pozytywne" i „negatywne" wykazy określono w Załączniku 5 do dokumentu Europejskiego Inspektora Ochrony Danych zatytułowanego „Accountability on the ground" (przypis 353 powyżej); szablon *Template for threshold assessment/criteria* znajduje się w Załączniku 6.

[371] Zob. Wytyczne Grupy Roboczej Art. 29 dotyczące oceny skutków dla ochrony danych (przypis 351 powyżej), str. 9-10 Główne uwagi dotyczące czynników także pochodzą z wspomnianych wytycznych. Należy zauważyć, że czynniki w pewnym stopniu

1. Ewaluacja lub ocena, w tym profilowanie i przewidywanie, szczególnie *„aspektów dotyczących efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się osoby, której dane dotyczą”* (motywy 71 i 91).

> **Przykłady:**
>
> Instytucja finansowa, która sprawdza swoich klientów w bazie kredytowej lub pod kątem prania brudnych pieniędzy albo finansowania terroryzmu lub oszustw.
>
> Bank sprawdzający transakcje zgodnie z odpowiednim prawem, by wykryć ewentualne oszukańcze transakcje*.
>
> Profilowanie pracowników na podstawie ich wszystkich transakcji w systemie zarządzania [*organizacji*] z uwzględnieniem automatycznego ponownego przydziału zadań*.
>
> Przedsiębiorstwo biotechnologiczne oferujące testy genetyczne bezpośrednio konsumentom w celu oceny i przewidywania ryzyka wystąpienia choroby lub zagrożenia dla zdrowia.
>
> Przedsiębiorstwo tworzące profile behawioralne lub marketingowe w oparciu o zakres korzystania ze strony internetowej.

2. Zautomatyzowane podejmowanie decyzji wywołujących skutki prawne lub podobne istotne skutki: przetwarzanie mające na celu podejmowanie decyzji dotyczących osób, których dane dotyczą, wywołujących „skutki prawne wobec osoby fizycznej” lub „w podobny sposób znacząco wpływających na osobę fizyczną” (artykuł 35 ust. 3 lit. a), w szczególności (ale nie tylko) w przypadkach, w których przetwarzanie może prowadzić do wyłączenia lub dyskryminacji osób.

> **Przykłady**[372]**:**
>
> Zautomatyzowana ocena personelu („jeżeli pracownik znajduje się w najniżej ocenionych 10% zespołu w szeregu spraw, bez dyskusji otrzyma „niezadowalającą” ocenę”)*.
>
> *Identyfikacja „możliwych” lub „prawdopodobnych” oszustów poprzez automatyczne przypisywanie podatnikom odpowiednich profili*[373]*.*
>
> *Ustalanie „możliwych” lub „prawdopodobnych” oszustów opieki społecznej na podstawie profilu znanych oszustów.*
>
> *Identyfikacja - na podstawie profilu - dzieci, w przypadku których istnieje zagrożenie, że będą otyłe lub zostaną członkami gangów albo przestępcami, lub dziewczynek, które „prawdopodobnie” zajdą w ciążę jako nastolatki*[374]*.*
>
> *Identyfikacja młodzieży i osób dorosłych zagrożonych „radykalizacją”.*

3. Systematyczne monitorowanie: przetwarzanie wykorzystywane do obserwacji, monitorowania i kontroli osób, których dane dotyczą, w tym dane zbierane poprzez *„systematyczne monitorowanie na dużą skalę miejsc dostępnych publicznie*” (artykuł 35 ust. 3 lit. c). Ten rodzaj monitorowania jest kryterium, ponieważ dane osobowe mogą być zbierane w okolicznościach,

---

zazębiają się lub mogą łączyć się, co zauważono w ramach czynników wspomnianych w punkcie zatytułowanym *„Operacje wysokiego ryzyka oparte na wielu czynnikach*”.

[372] Grupa Robocza Art. 29/Europejska Rada Ochrony Danych dodaje, że *„Przetwarzanie wywołujące niewielkie skutki lub niewywołujące skutków wobec osób nie odpowiada temu konkretnemu kryterium. Dalsze wyjaśnienia tych pojęć zostaną przedstawione w przygotowywanych Wytycznych GR Art. 29 dotyczących profilowania*.

[373] Rozwiązanie takie zostało zastosowane we **Włoszech** przez Włoską Agencję Skarbową, wykorzystującą narzędzie zwane *Redditometro.* Profile oparte są między innymi na założonych wydatkach odliczanych przez podatników wynikających - zgodnie z parametrami statystycznymi - z ich przypisania do konkretnej kategorii lub konkretnego obszaru geograficznego. Narzędzie profilujące było przedmiotem inspekcji włoskiego organu ochrony danych, *Garante.* Jedną z podstawowych kwestii była niska jakość danych oraz związany z tym wysokich wskaźnik błędów opartych na nierzetelnych, wyciągniętych na podstawie takich danych wnioskach. W oparciu o przeprowadzone dochodzenie *Garante* ustaliła, że realne dochody podatnika można obliczać wyłącznie na podstawie faktycznych i udokumentowanych wydatków, a nie poprzez odliczenie od statystycznych założeń poziomów wydatków. Zob. https://www.garanteprivacy.it/en/home/docweb/-/docweb-display/docweb/2765110.

[374] Zob. UK Foundation for Information Policy (FIPR), Childrens Databases - Safety & Privacy, badanie na zlecenie brytyjskiego Information Commissioner, 2006, https://www.cl.cam.ac.uk/~rja14/Papers/kids.pdf.

gdy osoby, których dane dotyczą, mogą nie być świadome faktu, kto zbiera ich dane i jak będą wykorzystane. Ponadto może być niemożliwe uniknięcie przez osoby fizyczne bycia przedmiotem takiego przetwarzania w często uczęszczanych (lub publicznie dostępnych) miejscach.

Przykłady:

Analiza ruchu w internecie ze złamaniem szyfrowania*.

Tajny system telewizji przemysłowej*.

Inteligentny system telewizji przemysłowej [*np. wykorzystanie oprogramowania rozpoznawania twarzy*] w miejscach dostępnych publicznie*.

Narzędzia zapobiegające utracie danych, łamiące szyfrowanie SSL*.

Przetwarzanie meta danych (np. czasu, charakteru i okresu trwania transakcji na rachunku bankowym) w celach organizacyjnych lub w celu uzyskania szacunkowych danych budżetowych[375].

4. Dane wrażliwe lub bardzo osobiste dane: obejmują szczególne kategorie danych określonych w artykule 9 (*dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne, dane biometryczne, dane dotyczące zdrowia lub kwestii medycznych, seksualności lub orientacji seksualnej*), a także dane osobowe dotyczące wyroków skazujących i przestępstw, o których mowa w art. 10. Poza wyżej wspomnianymi postanowieniami RODO, niektóre kategorie danych można uznać za zwiększające możliwe ryzyko naruszenia praw lub wolności osób fizycznych. Takie dane osobowe są traktowane jako wrażliwe (w powszechnym rozumieniu tego słowa), ponieważ są związane z gospodarstwem domowym i prywatnym życiem (*zob. trzeci przykład*) lub ponieważ wpływają na wykonanie podstawowego prawa (zob. *czwarty przykład*), lub ponieważ ich naruszenie wywiera poważny wpływ na codzienne życie osoby, której dane dotyczą (zob. *piąty przykład*). W tym zakresie istotny może być fakt, czy dane już zostały publicznie udostępnione przez osobę, której dane dotyczą, lub przez strony trzecie. Fakt, że dane osobowe są publicznie dostępne, może być uznany za czynnik przy ocenie [*biorąc pod uwagę to, czy osoba, której dane dotyczą, może w uzasadniony sposób oczekiwać, że dane takie mogą być wykorzystane przez inne osoby w pewnych celach – zob. siódmy przykład*].

Przykłady:

Szpital [*lub urząd opieki społecznej*] przechowujący rejestry medyczne pacjentów [*lub klientów opieki społecznej*].

Prywatny detektyw przechowujący dane wyroków skazujących lub przestępstw [*albo organ publiczny, taki jak instytucja szkolna, przechowujący takie dane w odniesieniu do swoich uczniów lub studentów*].

[*Organ publiczny lub podmiot prywatny (taki jak pracodawca)]* uzyskujący dostęp do dokumentów osobistych, poczty elektronicznej, dzienników lub notatek z e-czytników wyposażonych w funkcje robienia notatek, należących do pracowników [*lub wykorzystywanych przez pracowników w celach osobistych i służbowych, np. zgodnie z zasadą przynoszenia swoich własnych urządzeń].*

[*Organ publiczny lub podmiot prywatny (taki jak pracodawca)]* uzyskujący dostęp do bardzo osobistych informacji zawartych w aplikacjach typu „life-logging" lub *wykorzystujący informacje z mediów społecznościowych w kontekście, który może mieć istotny wpływ na daną osobę, takim jak wybór ludzi do pracy (albo wywiady o pracę).*

Przedrekrutacyjne badania medyczne i sprawdzenie rejestrów karnych*.

[375] Przykład ten pochodzi z **włoskiego,** zatwierdzonego przez EDPB wykazu operacji podlegających ocenie skutków dla ochrony danych.

Dochodzenia administracyjne i postępowania dyscyplinarne*.

Każde zastosowanie identyfikacji biometrycznej 1:n*.

Zdjęcia wykorzystywane przy użyciu oprogramowania do rozpoznawania twarzy lub w celu ingerowania w inne wrażliwe dane [*np. gdy mogą prowadzić do dyskryminacji w kontekście rekrutacji*]*.

5. Dane przetwarzane na dużą skalę: RODO nie definiuje pojęcia dużej skali, choć motyw 91 przedstawia pewne wskazówki[376]. W każdym przypadku GR Art. 29 zaleca uwzględnianie w szczególności następujących czynników przy określaniu, czy przetwarzanie jest prowadzone na dużą skalę:

   a. liczba osób, których dane dotyczą – konkretna liczba albo procent określonej grupy społeczeństwa;

   b. ilość danych i/lub zakres różnych przetwarzanych danych;

   c. okres lub trwałość czynności przetwarzania danych;

   d. zakres geograficzny przetwarzania.

Przykład:

[*Krajowe lub ewentualnie związane z UE*] bazy danych w zakresie nadzoru nad zdrowiem*.

Wymiana danych na dużą skalę pomiędzy administratorami danych sektora publicznego (np. ministerstwami, samorządami itp.) poprzez sieci elektroniczne[377].

Gromadzenie na dużą skalę informacji genealogicznych na temat rodzin osób należących do konkretnej grupy wyznaniowej[378].

Tworzenie bardzo dużych baz danych dotyczących stylu życia w celach marketingowych (które jednak mogą być wykorzystywane w innych celach).

Rejestrowanie przez partie polityczne sondaży dotyczących głosowania bardzo dużej liczby głosujących (lub gospodarstw domowych) w całym narodzie lub kraju na podstawie wywiadów prowadzonych bezpośrednio w domach i późniejszej analizy oraz wykorzystania takich danych[379].

6. Dokonano porównania lub połączenia zestawów danych: [*w szczególności, jeżeli pochodzą one]* z dwóch lub większej liczby operacji przetwarzania prowadzonych w różnych celach i/lub przez różnych administratorów danych w sposób, który wykracza poza racjonalne oczekiwania osoby, której dane dotyczą.

Przykład:

Potajemne sprawdzanie rejestrów kontroli dostępu, rejestrów komputerowych i deklaracji o elastycznym czasie pracy [*przez pracodawcę*] w celu wykrycia absencji*.

---

[376] Objaśnienie zawarte w motywie 91: *„operacje przetwarzania o dużej skali [to operacje], które służą przetwarzaniu znacznej ilości danych osobowych na szczeblu regionalnym, krajowym lub ponadnarodowym i które mogą wpłynąć na dużą liczbę osób, których dane dotyczą, oraz które mogą powodować wysokie ryzyko, na przykład (ze względu na swój szczególny charakter) [lub] gdy zgodnie ze stanem wiedzy technicznej stosowana jest na dużą skalę nowa technologia ..."*

[377] Przykład ten pochodzi z **włoskiego,** zatwierdzonego przez EDPB, wykazu operacji podlegających ocenie skutków dla ochrony danych.

[378] Zob. decyzja francuskiego organu ochrony danych (CNIL) w sprawie rejestru genealogicznego Mormonów, wydana w 2013 roku i przedstawiona na stronie https://www.nouvelobs.com/societe/20130613.OBS3162/les-mormons-autorises-par-la-cnil-a-numeriser-l-etat-civil-francais.html.

[379] Praktyka ta jest powszechna i faktycznie tradycyjne stosowana w Zjednoczonym Królestwie, o czym wspomniano w motywie 56 RODO. Zgodnie z tym motywem *„można zezwolić na przetwarzanie tych danych z uwagi na względy interesu publicznego pod warunkiem ustanowienia odpowiednich zabezpieczeń" (*pochyła czcionka dodana przez autorów Podręcznika). W takiej sytuacji potrzeba oceny, czy przetwarzanie naprawdę służy uzasadnionemu interesowi publicznemu oraz spełnia wymóg stosowania „odpowiednich zabezpieczeń", podkreśla potrzebę przeprowadzenia poważnej analizy ryzyka i oceny oddziaływania.

Urząd podatkowy dopasowuje swoje rejestry deklaracji podatkowych do rejestrów właścicieli drogich jachtów, by znaleźć osoby, które mogły popełnić oszustwo podatkowe[380].

7. Dane dotyczące osób wymagających szczególnej opieki (motyw 75): przetwarzanie tego rodzaju danych stanowi kryterium ze względu na zwiększony brak równowagi sił między osobą, której dane dotyczą, a administratorem danych, co oznacza, że osoba może nie być w stanie wyrazić zgody na przetwarzanie jej danych lub sprzeciwić się mu, albo nie może wykonywać swoich praw. Osoby wymagające szczególnej opieki to między innymi **dzieci** (które można uznać za niebędące w stanie świadomie i rozważnie wyrazić sprzeciwu lub zgody na przetwarzanie ich danych), **pracownicy**, wymagające szczególnej opieki i ochrony grupy społeczeństwa (**osoby psychicznie chore, osoby ubiegające się o azyl** lub **osoby starsze, pacjenci,** itp.) oraz w każdym przypadku, gdy można ustalić brak równowagi w relacji między pozycją osoby, której dane dotyczą a administratora.

Przykłady:

Wykorzystanie nadzoru wideo oraz systemów geolokacyjnych umożliwiających monitorowanie odległości pracowników[381].

W szczególności każde przetwarzanie danych osobowych którejkolwiek z wyżej wymienionych kategorii osób wymagających szczególnej opieki oraz na pewno przetwarzanie ich wrażliwych danych albo przetwarzanie na dużą skalę danych tych osób należy traktować jako z zasady mogące powodować „wysokie ryzyko".

8. Innowacyjne wykorzystanie lub zastosowanie rozwiązań technologicznych lub organizacyjnych. RODO wyjaśnia (art. 35(1) i motywy 89 i 91), że wykorzystanie nowej technologii, ustalonej „zgodnie ze stanem wiedzy technicznej" (motyw 91), może wywołać potrzebę dokonania oceny skutków dla ochrony danych. Jest tak, ponieważ wykorzystanie takiej technologii może obejmować nowoczesne formy zbierania i wykorzystywania danych, potencjalnie mogących wywołać wysokie ryzyko naruszenia praw lub wolności osób fizycznych. W istocie osobiste i społeczne konsekwencje zastosowania nowej technologii mogą być nieznane. Ocena skutków dla ochrony danych pomoże administratorowi danych zrozumieć takie rodzaje ryzyka i zaradzić im, a środki łagodzące powinny umożliwić osobom, których dane dotyczą oraz ogółowi społeczeństwa sprawdzenie, w jaki sposób, kiedy i w jakich celach nowe technologie są wykorzystywane, by można się było zabezpieczyć przed takimi technologiami, które podważają prawa i wolności jednostki oraz prowadzą do rządów autorytarnych lub masowego nadzorowania przez korporacje (lub współdziałającymi technologiami).

Uwaga: W wielu przypadkach pojawienia się nowych technologii lub praktyk, organy ochrony danych (lub Europejska Rada Ochrony Danych) mogą wydać albo możliwe, że już wydały, opinie, wytyczne lub rekomendacje, zaś inspektorzy ochrony danych powinni być wyczuleni na pojawienie się nowych dokumentów. Jeżeli uważają, że brak jest stosownych wytycznych, itp., powinni skonsultować się ze swoim organem ochrony danych. Zob. także Zadania 4, 8 i 10.

Przykłady:

Łączenie stosowania rozpoznawania odcisku palca i twarzy dla celów usprawnionej kontroli fizycznego dostępu[382].

[380] Miało to miejsce dawno temu w Holandii, przy założeniu, że duże jachty z reguły nabywane są przez oszustów podatkowych. Jedna osoba, sama czując się celem takich działań, szyderczo nazwała swój statek *„Na czarno".*

[381] Przykład ten pochodzi z **włoskiego,** zatwierdzonego przez EDPB wykazu operacji podlegających ocenie skutków dla ochrony danych.

[382] Grupa Robocza Art. 29 i kilka krajowych organów ochrony danych wydało szczegółową wskazówkę na ten temat, wymagając między innymi, żeby dane biologiczne były przechowywane na mikroczipach w urządzeniu osoby, której dane dotyczą, a nie centralnie przez administratora. Zob. Dokument roboczy Grupy Roboczej Art. 29 dotyczący biometryki (WP80, przyjęty 1 sierpnia 2003 roku), str. 6, zob. link: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp80_en.pdf.

Nowe technologie mające śledzić czas i obecność pracowników, z uwzględnieniem tych, które przetwarzają dane biometryczne oraz innych, takich jak śledzenie urządzeń mobilnych.[383]

Przetwarzanie danych generowanych poprzez aplikacje „internetu rzeczy" (*podłączone inteligentne urządzenia i rzeczy*), jeżeli mogłoby to mieć znaczny wpływ na codzienne życie osób i ich prywatność.

Maszynowe uczenie się*.

Podłączone samochody*.

Monitorowanie postów kandydatów w mediach społecznościowych*.

9. Gdy przetwarzanie samo w sobie „*uniemożliwia osobom, których dane dotyczą, wykonywanie praw lub korzystanie z usługi albo umowy*" (art. 22 i motyw 91). Dotyczy to operacji przetwarzania, którego celem jest umożliwienie, zmiana lub odmowa dostępu osób, których dane dotyczą, do usługi lub zawarcia umowy.

Przykłady:

Bank sprawdzający swoich klientów w bazie kredytowej w celu podjęcia decyzji, czy zaoferować im kredyt.

Instytucja finansowa lub agencja kredytowa biorąca pod uwagę różnicę wieku pomiędzy małżonkami w celu ustalenia wiarygodności kredytowej (co może naruszyć swobodne korzystanie z podstawowego prawa do małżeństwa - i zostało przez to zakazane we Francji przez francuski organ ochrony danych, CNIL, (która miał dostęp do systemu, ponieważ, podejmując decyzje na podstawie profili, musiała uzyskać uprzednią zgodę CNIL).

Bazy wyłączeń*.

Kontrola kredytowa*.

Operacje o wysokim ryzyku oparte na wielu czynnikach

Wyżej wymienione czynniki mogą zazębiać lub łączyć się, np. „systematyczne monitorowanie" może być powiązane lub połączone z automatycznym, opartym na profilowaniu, procesie decyzyjnym i może obejmować przetwarzanie „wrażliwych danych" na „dużą skalę". Grupa Robocza Art. 29 przedstawia szereg przykładów operacji opartych na takich kombinowanych czynnikach (lub kryteriach), w przypadku których konieczna jest ocena skutków dla ochrony danych, a także przykładów operacji, w których obecny jest jeden lub kilka czynników, ale które nie wymagają takiej oceny[384].

Przykłady przetwarzania	Możliwe istotne kryteria	Czy ocena jest wymagana?
Szpital przetwarzający dane genetyczne i dane dotycząca zdrowia swoich pacjentów (system informacyjny szpitala)	- Dane wrażliwe lub wysoce osobiste dane - Dane dotyczące osób wymagających szczególnej opieki - Dane przetwarzane na dużą skalę.	
Wykorzystanie systemu kamer do monitorowania zachowania kierowców na autostradach. Administrator zakłada wykorzystanie inteligentnego systemu analizy wideo w celu wyodrębnienia samochodów i automatycznego rozpoznania tablic rejestracyjnych.	- Systematyczne monitorowanie. - Innowacyjne wykorzystanie lub zastosowanie rozwiązań technologicznych lub organizacyjnych.	
Przedsiębiorstwo systematycznie monitorujące działania swoich pracowników, w tym	- Systematyczne monitorowanie. - Dane dotyczące osób wymagających szczególnej opieki	

[383] Zob. Opinia Grupy Roboczej Art. 29 2/2017 na temat przetwarzania danych w pracy (WP249, przyjęta 8 czerwca 2017 roku), ust. 5.5. Przetwarzanie operacji związanych z czasem i obecnością, str. 18 – 19, zob. link: www.ec.europa.eu/newsroom/document.cfm?doc_id=45631.

[384] Wytyczne Grupy Roboczej Art. 29 dotyczące oceny skutków dla ochrony danych (przypis 351 powyżej), str. 11-12.

stanowiska pracy pracowników, działania w internecie, itd.		Tak
Gromadzenie danych z publicznych mediów społecznościowych do generowania profili.	- Ewaluacja lub ocena - Dane przetwarzane na dużą skalę. - Dopasowanie lub łączenie baz danych. - Dane wrażliwe lub wysoce osobiste dane:	
Instytucja przeprowadzająca krajową ocenę kredytową lub tworząca bazę danych.	- Ewaluacja lub ocena. - Automatyczny proces decyzyjny niosący za sobą skutki prawne lub podobne istotne skutki. - Uniemożliwia osobom, których dane dotyczą, wykonywanie praw lub korzystanie z usługi albo umowy. - Dane wrażliwe lub wysoce osobiste dane:	
Przechowywanie w celach archiwizacyjnych wrażliwych danych osobowych w formie pseudonimów, w odniesieniu do osób wymagających szczególnej opieki w ramach projektów badawczych lub prób klinicznych.	- Dane wrażliwe. - Dane dotyczące osób wymagających szczególnej opieki. - Uniemożliwia osobom, których dane dotyczą, wykonywanie praw lub korzystanie z usługi albo umowy.	
Przetwarzanie danych osobowych pacjentów lub klientów przez pojedynczego lekarza, innego pracownika służby zdrowia lub prawnika (motyw 91).	- Dane wrażliwe lub wysoce osobiste dane. - Dane dotyczące osób wymagających szczególnej opieki.	Nie
Magazyn online wykorzystujący listę mailingową do wysyłania codziennej porcji ogólnych wiadomości do swoich abonentów za ich zgodą, z uwzględnieniem łatwej możliwości rezygnacji.	- Dane przetwarzane na dużą skalę.	
Strona internetowa handlu elektronicznego wyświetlająca ogłoszenia dotyczące części samochodów zabytkowych, z uwzględnieniem ograniczonego profilowania opartego na pozycjach przeglądanych lub zakupionych na własnej stronie, także z możliwością rezygnacji.	- Ewaluacja lub ocena.	

Metodologie przeprowadzania oceny skutków dla ochrony danych:

Celem oceny skutków dla ochrony danych jest:

(i) **ustalenie** konkretnego (wysokiego) ryzyka związanego z proponowaną operacją przetwarzania, uwzględniając charakter danych i przetwarzania, zakres, kontekst i cele przetwarzania oraz źródła ryzyka, nie tylko w normalnych okolicznościach, ale także w szczególnych okolicznościach oraz w krótkim, średnim i długim okresie[385];

(ii) **ocena** ustalonego (wysokiego) ryzyka, w szczególności jego pochodzenia, charakteru i cech szczególnych oraz prawdopodobieństwa i powagi[386];

(iii) ustalenie **środków**, jakie można podjąć, by złagodzić (wysokie) ryzyko, oraz które z nich są odpowiednie pod względem technologicznym oraz kosztów wdrożenia, a także zaproponowanie tych środków[387] oraz

(iv) **odnotowanie** ustaleń, oceny i podjętych środków (lub niepodjętych, z uwzględnieniem przyczyny), aby być w stanie „**wykazać przestrzeganie**" wymogów RODO wynikających z zasady „rozliczalności" w odniesieniu do ocenianej operacji przetwarzania[388].

[385] Zob. motyw 90.
[386] Zob. motyw 84 i ISO 31000.
[387] Zob. motyw 84.
[388] Grupa Robocza Art. 29 ujmuje to następująco: *„Ocena skutków dla ochrony danych to proces budowania i udawadniania zgodności."* – Wytyczne Grupy Roboczej Art. 29 dotyczące oceny skutków dla ochrony danych (przypis 351 powyżej), str. 4. Więcej szczegółów na temat zasady rozliczalności oraz związanych z nią zadań „wykazania przestrzegania" przedstawiono w Części 2 Podręcznika.

Art. 35(7) RODO przewiduje, że ocena skutków dla ochrony danych (jej rejestr) powinien zawierać „co najmniej":

> (a) systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez administratora;
>
> (b) ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów;
>
> (c) ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą, o którym mowa w ust. 1 oraz
>
> (d) środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazania przestrzegania niniejszego rozporządzenia, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, oraz innych osób, których sprawa dotyczy.

Grupa Robocza Art. 29 podkreśla, że[389]:

> Wszystkie istotne wymogi określone w RODO stanowią szerokie, ogólne ramy projektowania i dokonywania oceny skutków dla ochrony danych. Praktyczne wdrożenie takiej oceny będzie zależeć od wymagań określonych w RODO, które mogą być uzupełnione bardziej szczegółowymi wskazówkami praktycznymi. **To otwiera drogę do skalowalności. Oznacza to, że nawet administrator danych niewielkiej organizacji może zaprojektować i wdrożyć ocenę skutków dla ochrony danych odpowiednią do swoich operacji przetwarzania.**

Administratorzy mogą więc (w porozumieniu ze swoimi inspektorami ochrony danych) wybrać metodologię oceny skutków dla ochrony danych, jaka im pasuje. Mogą polegać na swoich doświadczeniach związanych z bardziej techniczną oceną ryzyka, np. zgodną z ISO 31000. Jednak Grupa Robocza Art. 29 prawidłowo zwraca uwagę na różną perspektywę oceny skutków dla ochrony danych w ramach RODO oraz oceny opartej na ISO (która w każdym przypadku ma węższy charakter i jest zorientowana na bezpieczeństwo)[390]:

> Ocena skutków dla ochrony danych zgodnie z RODO jest narzędziem zarządzania ryzykiem naruszenia praw osób, których dane dotyczą, a tym samym przyjmuje stanowisko tych osób. Z kolei zarządzanie ryzykiem w innych dziedzinach (np. bezpieczeństwa informacyjnego) koncentruje się na [zagrożeniach dla] organizacji.

Grupa Robocza Art. 29 przedstawia szereg opracowanych przez krajowe organy ochrony danych przykładów metodologii ochrony danych i oddziaływania na prywatność[391] oraz *„zachęca do opracowania sektorowych ram oceny skutków dla ochrony danych*". Grupa sama opublikowała Ramy dotyczące oceny skutków dla ochrony danych dla aplikacji RFID (DPIA Framework for RFID Applications) oraz Szablon oceny skutków dla ochrony danych dla inteligentnych systemów pomiaru (DPIA Template for Smart Grid and Smart Metering Systems)[392].

W tym miejscu musi wystarczyć odtworzenie określonych w Wytycznych Grupy Roboczej Art. 29 Kryteriów dopuszczalnej oceny skutków dla ochrony danych[393]:

Załącznik 2 - Kryteria akceptowalnej oceny skutków dla ochrony danych

> Grupa Robocza Art. 29 proponuje następujące kryteria, które administratorzy danych mogą wykorzystać do oceny, czy ocena skutków dla ochrony danych lub metodologia przeprowadzania takiej oceny są wystarczająco obszerne, aby zapewnić zgodność z RODO:

---

[389] Wytyczne Grupy Roboczej Art. 29 dotyczące oceny skutków dla ochrony danych (przypis 351 powyżej), str. 17 (pogrubienie dodane przez autorów Podręcznika).
[390] *Idem*.
[391] Zob. wykaz z linkami w Załączniku *1* do Wytycznych Grupy Roboczej Art. 29 dotyczących oceny skutków dla ochrony danych (przypis 351 powyżej).
[392] *Idem*, przypisy 32 i 33.
[393] *Idem*, Załącznik 2. Pogrubienia w głównych punktach dodane zostały dla jasności przez autorów Podręcznika.

- **Zapewniony jest systematyczny opis planowanych operacji przetwarzania** (artykuł 35(7)(a)):

- charakter, zakres, kontekst i cele przetwarzania są uwzględnione (motyw 90);
- dokumentowane dane osobowe, odbiorcy oraz okres przechowywania danych osobowych;
- dostarczony jest funkcjonalny opis operacji przetwarzania;
- zidentyfikowane są aktywa, na których opierają się dane osobowe (sprzęt, oprogramowanie, sieci, ludzie, dokumenty papierowe lub papierowe kanały transmisji);
- uwzględnia się zgodność z zatwierdzonymi kodeksami postępowania [*certyfikatami lub Wiążącymi regułami korporacyjnymi]* (art. 35 ust. 8)[394].

- Ocena niezbędności i proporcjonalności (art. 35(7)(b)):

- Określono środki mające na celu spełnienie wymogów rozporządzenia (art. 35(7)(d) i motyw 90), biorąc pod uwagę:
  - Środki wpływające na niezbędność i proporcjonalność przetwarzania w oparciu o:
    - konkretny, wyraźny i prawnie uzasadniony cel (art. 5(1)b));
    - zgodność przetwarzania z prawem (art. 6);
    - adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów (art. 5(1)(c));
    - ograniczenie okresu przechowywania (art. 5(1)(e));
  - Środki przyczyniające się do praw osób, których dane dotyczą:
    - informacje udzielone osobie, której dane dotyczą (art. 12, 13 i 14);
    - prawo dostępu i przekazywania danych (art. 15 i 20);
    - prawo do sprostowania i usunięcia (art. 16, 17 i 19);
    - prawo do sprzeciwu i ograniczenia przetwarzania (art. 18, 19 i 21);
    - relacje z podmiotami przetwarzającymi (art. 28);
    - zabezpieczenia dotyczące przekazywania danych (Rozdział V);
    - uprzednie konsultacje (art. 36).

- **Zarządzanie ryzykiem naruszenia praw lub wolności osób (artykuł 35(7)(c)):**

- Uwzględnienie źródła, charakteru, specyfiki i powagi tego ryzyka (porównaj motyw 84); lub dokładniej, w odniesieniu do każdego ryzyka (nieuprawnionego dostępu, niepożądanej modyfikacji i zniknięcia danych) z punktu widzenia osób, których dane dotyczą:
  - uwzględniono źródło ryzyka (motyw 90);
  - potencjalne skutki dla praw lub wolności osób, których dane dotyczą, są identyfikowane w przypadku nieuprawnionego dostępu, niepożądanej modyfikacji i zniknięcia danych;
  - zagrożenia, które mogłyby prowadzić do nieuprawnionego dostępu, niepożądanej modyfikacji i zniknięcia danych;
  - oszacowano prawdopodobieństwo i powagę tego ryzyka (motyw 90);
- ustalono środki planowane w celu zaradzenia ryzyku (artykuł 35(7)(d) i motyw 90);

- **Zaangażowanie zainteresowanych stron:**

- zasięgnięto konsultacji inspektora ochrony danych (artykuł 35(2));
- zasięgnięto opinii osób, których dane dotyczą, lub ich przedstawicieli (artykuł 35(9));

Co należy zrobić z rejestrem oceny skutków dla ochrony danych

[394] Wcześniej Grupa Robocza Art. 29 zauważa, że: *„Zgodność z kodeksem postępowania (art. 40) powinna być wzięta pod uwagę (art. 38(8)) podczas oceniania skutków przetwarzania danych. Może to być przydatne do wykazania, że zostały wybrane lub wprowadzone odpowiednie środki pod warunkiem, że kodeks postępowania jest odpowiedni do danej operacji przetwarzania. Należy także uwzględnić certyfikaty, pieczęcie i oznaczenia mające potwierdzać przestrzeganie przez administratorów i podmioty przetwarzające wymogów RODO (art. 42) oraz Wiążących reguł korporacyjnych (BCR)”.* Wytyczne Grupy Roboczej Art. 29 dotyczące oceny skutków dla ochrony danych (przypis 351 powyżej), str. 16.

Pierwszym i głównym celem rejestru oceny skutków dla ochrony danych (uwzględniającym wszystkie wyżej wymienione „kryteria") jest **udokumentowanie** przeprowadzenia właściwej i dogłębnej oceny skutków dla ochrony danych zgodnie z postanowieniami RODO (tj. spełniając powyższe kryteria).

Gdy ocena skutków dla ochrony danych ustala jednocześnie (wysokie) ryzyko oraz środki, jakie należy podjąć, by takiemu ryzyku zaradzić, i które są „odpowiednie", biorąc pod uwagę prawdopodobieństwo i powagę ryzyka oraz związane z takimi środkami koszty, a także gdy środki takie zostały faktycznie zatwierdzone i przyjęte (a taka zgoda i takie przyjęcie zostały również odnotowane), rejestr oceny skutków dla ochrony danych może dostarczyć ważny „element" w ogólnej demonstracji zgodności i „szczególnych środków" pozwalających to osiągnąć (chociaż nie oznacza to prawnego domniemania zgodności i inspektor ochrony danych w dalszym ciągu będzie musiał na bieżąco **sprawdzać i monitorować**, czy środki łagodzące są stosowane i są odpowiednie w świetle zmian praktycznych, organizacyjnych lub technologicznych. Zob. punkt zatytułowany „*Bieżące monitorowanie zgodności*").

Przykłady sytuacji, w których ocena skutków dla ochrony danych pozwoliła ustalić zarówno wysokie ryzyko, jak i środki łagodzące uznane (*w omawianym przypadku* **przez EuroPrise) za wystarczające, by zezwolić na przetwarzanie. W efekcie w obydwu przypadkach administrator był w stanie z dużym stopniem pewności stwierdzić, że wyniki oceny skutków dla ochrony danych potwierdziły, że przetwarzanie NIE wymaga konsultacji z właściwym organem ochrony danych[395]:**

1. Centrum opieki społecznej stosuje system biometryczny uwierzytelniania głosem, by zapobiegać oszustwom socjalnym.

Identyfikacja zagrożeń: Jak wskazała Grupa Robocza Art. 29, trzy z głównych rodzajów ryzyka wynikających z wykorzystania danych biometrycznych to: (i) fakt, że cech biometrycznych osoby nie można zastąpić (co oznacza, że w przypadku utraty narzędzia uwierzytelniającego opartego na surowych danych biometrycznych nie można wymienić), (ii) łatwość zastosowania danych biometrycznych w celu dopasowania innego zestawu danych oraz (iii) możliwość ukradkowego przechwycenia danych biometrycznych.

Środki łagodzące: W przypadku biometrycznego narzędzia uwierzytelniającego (na podstawie głosu) wykorzystywanego do zwalczania oszustw socjalnych stosowany jest unikalny *wzór* głosu tworzony z oryginalnych („surowych") danych biometrycznych, a nie surowych danych, które są niszczone po zapisaniu osoby, której dane dotyczą. Wzór głosu jest unikalny i nie można go wykorzystać do odtworzenia pierwotnych (surowych) danych biometrycznych. Narzędzie to rozwiązuje problem wszystkich trzech wyżej wspomnianych rodzajów ryzyka: (i) w przypadku sprzeniewierzenia wzoru głosu, w bardzo prosty sposób można odtworzyć nowy inny wzór (przy pomocy osoby, której dane dotyczą, którą trzeba będzie ponownie zapisać), (ii) różnych wzorów głosów wykorzystywanych w różnych sytuacjach przez to samo narzędzie nie można do siebie dopasować ani dopasować do innych danych głosowych lub wzorów głosu oraz (iii) wzór głosu tworzony jest w procesie bezpośredniego kontaktu.

2. Instytucja finansowa sprawdza lokalizację telefonu komórkowego klienta, by sprawdzić, że znajduje się on (mniej więcej) w tym samym miejscu, co karta bankowa klienta (która jest wykorzystywana do wykonania transakcji oznaczonej jako podejrzana).

Identyfikacja zagrożeń: Dokładne szczegóły czyjejś lokalizacji w konkretnym momencie mogą narazić daną osobę na ujawnienie wrażliwych kwestii, w związku z czym ujawnienie takich szczegółów stanowi poważną ingerencję w prywatność oraz życie prywatne takiej osoby, jak w przypadku potwierdzonym przez Europejski Trybunał Praw Człowieka w sprawie *Naomi Campbell*[396].

Środki łagodzące: W bankowym urządzeniu zapobiegającym oszustwom przy użyciu kart dane lokalizacyjne telefonu komórkowego są ograniczone, nawet przed przekazaniem użytkownikowi tego narzędzia (instytucji finansowej), do bardzo przybliżonego obszaru, z reguły kraju lub stanu. Wystarczy, że narzędzie działa skutecznie

[395] Przykłady te dotyczą produktów, które uzyskały europejską etykietę prywatności, dla celów której ocena prawna została przeprowadzona przez Douwe Korffa (patrz odpowiednio: https://www.european-privacy-seal.eu/EPS-en/4F-self-certification (składające się z czterech czynników narzędzie uwierzytelniające uwzględniające rozwiązanie biometryczne wykorzystujące głos); https://www.european-privacy-seal.eu/eps-en/valid-pos (narzędzie dopasowujące lokalizację podejrzanej transakcji wykonanej kartą bankową do (przybliżonej) lokalizacji telefonu komórkowego właściciela karty). W ocenie obydwa produkty pochwalono za wysokiego stopnia minimalizację danych oraz uwzględnione w projekcie cechy ochrony prywatności, a także za sposób, w jaki złagodziły ryzyko związane odpowiednio z wykorzystaniem danych biometrycznych i sprawdzeniem lokalizacji.

[396] Zob. orzecznictwo ETPC, *MGN przeciwko Zjednoczonemu Królestwu*, wyrok z 18 stycznia 2011 r. https://hudoc.echr.coe.int/eng#{%22tabview%22:[%22document%22],%22itemid%22:[%22001-102965%22]}.

(tj. jest w stanie zapewnić z wystarczającą pewnością, czy dana transakcja jest uczciwa, czy nie), do minimum ograniczając poziom ingerencji w związku z kontrolą lokalizacji.

Rejestr taki może zostać także udostępniony w trakcie **konsultacji** (lub sporządzony w oparciu o konsultacje) z udziałem zainteresowanych stron lub obywateli albo w odpowiedzi na **zapytania i skargi osób, których dane dotyczą, oraz** reprezentujących je **organizacji pozarządowych** (lub prasy). W tym względzie Grupa Robocza Art. 29 zauważa, że[397]:

> **Publikowanie oceny skutków dla ochrony danych nie jest wymagane przepisami RODO. Pozostaje w gestii administratora. Administratorzy danych powinni jednak rozważyć, co najmniej częściowe, opublikowanie oceny.**
>
> Celem takiego działania byłoby przyczynienie się do zwiększenia zaufania w stosunku do operacji przetwarzania danych u administratora, a także wykazanie rozliczalności i przejrzystości. ***Szczególnie dobrą praktyką jest publikowanie wyników oceny w przypadku, w którym operacja przetwarzania ma wpływ na społeczeństwo. Może to być szczególnie możliwe w przypadku, gdy organ publiczny przeprowadza ocenę skutków dla ochrony danych.***
>
> Opublikowana ocena nie musi zawierać całej oceny, zwłaszcza gdy ocena taka mogłaby zawierać konkretne informacje dotyczące zagrożeń dla bezpieczeństwa administratora danych lub ujawnić tajemnice handlowe lub poufne informacje handlowe. W takich okolicznościach opublikowana wersja mogłaby się składać tylko z podsumowania najważniejszych ustaleń oceny skutków dla ochrony danych lub nawet stwierdzenia, że ocena taka została przeprowadzona.

Rejestr oceny skutków dla ochrony danych ma szczególne znaczenie w procesie obsługi wynikających z oceny zapytań, bez względu na to, czy w ramach ogólnej funkcji nadzoru, czy też w reakcji na reklamację.

A konkretnie, jeżeli ocena skutków dla ochrony danych wskaże zarówno (wysokie) ryzyko, jak i brak środków, jakie można podjąć, by w wystarczającym zakresie takiemu ryzyku zaradzić (lub przynajmniej środków, które są „odpowiednie", uwzględniając prawdopodobieństwo i powagę ryzyka oraz koszty takich środków), administrator jest zobowiązany skonsultować się z **organem ochrony danych** (art. 36), **któremu należy przekazać rejestr z odpowiedniej oceny skutków dla ochrony prywatności**[398]**:**

> gdy ocena skutków dla ochrony danych ujawnia wysokie ryzyko szczątkowe, administrator danych będzie zmuszony zwrócić się o uprzednie konsultacje w celu przetwarzania do organu nadzorczego (art. 36(1)). W ramach takich konsultacji należy przekazać całą ocenę skutków dla ochrony danych (art. 36(3)(e)). Organ nadzorczy może udzielić porady[399] oraz nie narazi na zagrożenie tajemnic handlowych ani nie ujawni słabych stron bezpieczeństwa, z zastrzeżeniem zasad mających zastosowanie do każdego państwa członkowskiego w odniesieniu do dostępu publicznego do oficjalnych dokumentów.

Państwa członkowskie mogą także - na mocy swojego **prawa krajowego** - wymagać, by administratorzy konsultowali się z organem ochrony danych w związku z przetwarzaniem przez administratora „do celów wykonania zadania realizowanego przez administratora w interesie publicznym, w tym przetwarzania w związku z ochroną socjalną i zdrowiem publicznym" (art. 36(5)), co uczyniono w dwóch ostatnich przypadkach, np. we Francji i Włoszech.

Jeżeli organ ochrony danych jest niezadowolony z informacji zawartych w rejestrze oceny skutków dla ochrony danych (i/lub przekazanych w inny sposób), może **nakazać** administratorowi dostarczenie dodatkowych informacji, jakie uzna za konieczne, by ocenić daną sprawę (patrz: art. 58(1)(a)).

Zazwyczaj organ ochrony danych stara się **pomóc** administratorowi znaleźć rozwiązanie, tj. ustalić środki, które odpowiednio łagodziłyby ustalone (wysokie) ryzyko (zdaniem organu ochrony danych), oraz pod warunkiem że administrator zgadza się przyjąć takie środki (oraz że ich przyjęcie i dalsze stosowanie podlega kontroli i monitorowaniu przez inspektora ochrony danych), jakie rozwiązałyby problem (co powinno zostać odnotowane przez inspektora ochrony danych i oczywiście przez organ ochrony danych).

---

[397] Wytyczne Grupy Roboczej Art. 29 dotyczące oceny skutków dla ochrony danych (przypis 351 powyżej), str. 18 (pogrubienie oryginalne, pochyła czcionka i pogrubienie dodane przez autorów Podręcznika).

[398] *Idem*.

[399] Pisemne zgłoszenie do administratora jest konieczne wyłącznie wtedy, gdy organ nadzorczy jest zdania, że planowane przetwarzanie nie jest zgodne z art. 36(2) rozporządzenia. [oryginalny przypis].

Ewentualnie organ ochrony danych może albo **nakazać** administratorowi, wymagając przyjęcia określonych środków dla proponowanej operacji przetwarzania (patrz: art. 58(2)(d)), albo faktycznie **zakazać** proponowanego przetwarzania (art. 58(2)f)).

Inspektor ochrony danych powinien oczywiście ponownie zarejestrować tego typu nakaz oraz na bieżąco sprawdzać, czy jest on przestrzegany (oraz zarejestrować swoje ustalenia). Jak zawsze, poza sprawdzaniem, monitorowaniem i prowadzeniem rejestru, to administrator odpowiada za nieprzestrzeganie wymogów.

- o – O – o -

Monitorowanie przestrzegania prawa (z uwzględnieniem rozpatrywania skarg):

Zadanie 5: Powtarzanie Zadań 1 - 3 (i 4) na bieżąco

Jak wskazuje Grupa Robocza Art. 29 w swoich (zatwierdzonych przez Europejską Radę Ochrony Danych) Wytycznych dotyczących organów ochrony danych, art. 39(1)(b) nakłada na inspektora ochrony danych między innymi obowiązek monitorowania przestrzegania RODO. Motyw 97 doprecyzowuje, że „w monitorowaniu wewnętrznego przestrzegania niniejszego rozporządzenia administrator lub podmiot przetwarzający powinni być wspomagani przez inspektora ochrony danych”[400]. Sam zwrot „monitorowanie” oznacza, że nie jest to jednorazowa, ale stała odpowiedzialność.

Jednak zgodnie z naszą, zawartą w części drugiej (pkt 2.3.4) dyskusją na temat roli inspektora ochrony danych, Grupa Robocza Art. 29 (ponownie) podkreśla, że[401]:

> nie oznacza [to] osobistej odpowiedzialności inspektora ochrony danych w przypadkach naruszenia przepisów. Z rozporządzenia jasno wynika, że to administrator, a nie inspektor ochrony danych, *„wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać*” (art. 24(1)). Spełnianie wymogów rozporządzenia należy do obowiązków korporacyjnych administratora, a nie inspektora ochrony danych.

Grupa Robocza Art. 29 dalej twierdzi, że w ramach monitorowania przestrzegania przepisów inspektorzy ochrony danych mogą w szczególności na bieżąco:

- zbierać informacje w celu identyfikacji procesów przetwarzania;
- analizować i sprawdzać zgodność tego przetwarzania;
- informować, doradzać i rekomendować określone działania administratorowi albo podmiotowi przetwarzającemu.

Jak zauważono w odniesieniu do oceny skutków dla ochrony danych (Zadanie 4)[402]:

> Należy podkreślić, że aby zarządzać ryzykiem naruszenia praw i wolności osób fizycznych, ryzyko takie należy zidentyfikować, przeanalizować, oszacować, ocenić, rozwiązać (np. złagodzić ...) **i dokonywać jego regularnego przeglądu.**

Innymi słowy, Zadania 1-4 (lub gdy brak jest operacji mogących powodować„wysokiego ryzyka” Zadania 1-3) należy powtarzać na bieżąco oraz w szczególności, gdy organizacja zmienia lub wdraża nową operację przetwarzania danych osobowych. Jak ujmuje to Europejski Inspektor Ochrony Danych (w swojej poradzie dla inspektorów ochrony danych w instytucjach UE)[403]:

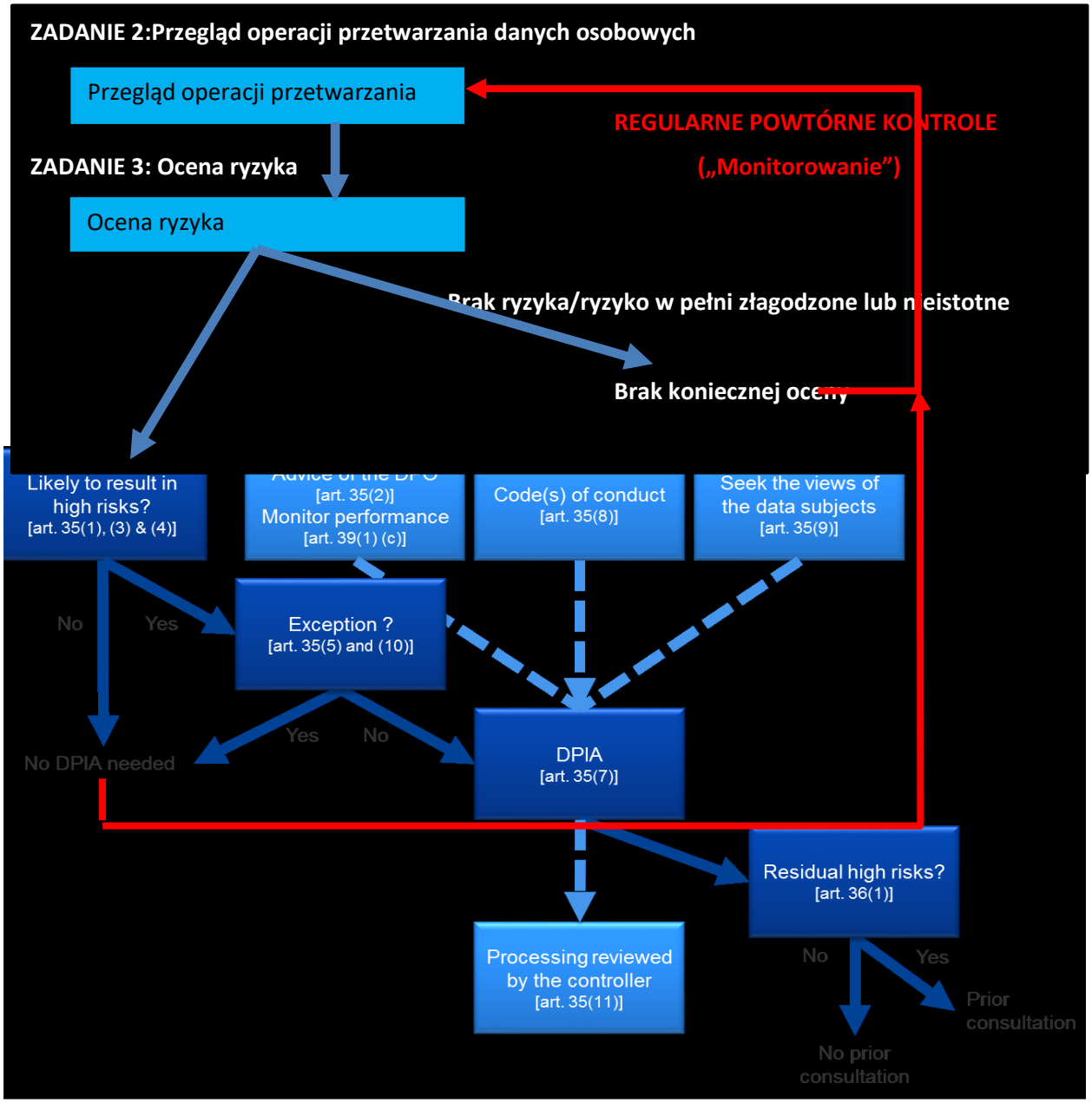
> Rejestry muszą odzwierciedlać realia operacji przetwarzania danej instytucji. Oznacza to konieczność zapewnienia ich aktualności. Gdy [instytucja] planuje zmiany w swoich operacjach przetwarzania, należy sprawdzić, czy rejestry także wymagają aktualizacji. Warto formalnie uwzględnić tego typu kontrolę w procesie zarządzania zmianą. Dobrym pomysłem jest także przeprowadzanie regularnych przeglądów niezależnie od planowanych zmian, by wychwycić zmiany, które mogłyby przejść niezauważone.

Grupa Robocza Art. 29 zilustrowała tą ostatnią część zdania na przydatnym, odtworzonym na odwrocie diagramie, który uzupełniono o wcześniejsze etapy (Zadania 2 i 3).

Diagram Grupy Roboczej Art. 29 dotyczący kroków, jakie należy podjąć w związku z oceną skutków dla ochrony danych[404], z uwzględnieniem wcześniejszych etapów (Zadania 2 i 3):

---

[400] Wytyczne Grupy Roboczej Art. 29 dotyczące inspektorów ochrony danych (przypis 242 powyżej), ust. 4.1 (*Monitorowanie zgodności z RODO)* str. 16,7.
[401] *Idem*, pochylona czcionka jak w oryginale.
[402] Wytyczne Grupy Roboczej Art. 29 dotyczące oceny skutków dla ochrony danych (przypis 351 powyżej), przypis 10 na str. 6 (pogrubienie dodane przez autorów Podręcznika).
[403] EDPS, Accountability on the ground (przypis 353 powyżej).
[404] Wytyczne Grupy Roboczej Art. 29 dotyczące oceny skutków dla ochrony danych (przypis 351 powyżej), str. 7.



Prawdopodobieństwo wysokiego ryzyka – Rada ze strony inspektora ochrony danych / Monitorowanie wyników – Kodeks(y) postępowania – Uzyskanie opinii osób, których dane dotyczą

Wyjątek? – Ocena skutków dla ochrony danych – Pozostałe wysokie ryzyko? – Sprawdzenie operacji przetwarzania przez administratora

Brak konieczności oceny skutków dla ochrony prywatności – uprzednie konsultacje – brak uprzednich konsultacji

Uwaga: Wyjątki wynikające z art. 35(5), wskazane na diagramie Grupy Roboczej Art. 29, dotyczą bezpieczeństwa krajowego, obronności, zapobiegania przestępstwom itp. Art. 35(10) przewiduje, że ocena skutków dla ochrony danych nie jest konieczna w odniesieniu do przetwarzania na mocy prawa, jeżeli ogólna ocena skutków dla ochrony danych takiego przetwarzania została wykonana przed podjęciem tego typu czynności (bez udziału inspektora ochrony danych).

W ramach swoich obowiązków „monitorowania przetwarzania prawa" inspektor ochrony danych powinien także upewnić się, że wie o wszystkich zmianach dotyczących ram regulacyjnych, umownych, itp. dotyczących jego organizacji, które zostały ustalone w ramach zadania wstępnego (Zadanie 0), tak aby był w stanie ustalić wpływ tego typu zmian (legalności i zgodności z RODO) na operacje przetwarzania danych osobowych w swojej organizacji, oraz że może wydać konkretne porady dla odpowiednich osób w organizacji (z uwzględnieniem najwyższego kierownictwa, jeżeli jest to wymagane).

W rzeczywistości inspektor ochrony danych powinien - tam, gdzie to stosowne wspólnie z innymi inspektorami ochrony danych w swojej sieci inspektorów ochrony danych i/lub wspólnie z organem ochrony danych oraz w porozumieniu z najwyższym kierownictwem - przyjmować stanowiska i opinie na temat proponowanych lub sugerowanych zmian w tego typu ramach, takich jak propozycje rządowe

zakładające, że organizacje, takie jak organizacja inspektora, będą zobowiązane lub zachęcane do dzielenia się danymi osobowymi w nowych celach, albo będą miały takie prawo.

- o – O – o -

ZADANIE 6: Postępowanie z naruszeniem ochrony danych osobowych

Dwie z najważniejszych innowacji wprowadzonych przez RODO w porównaniu do Dyrektywy o ochronie danych z 1995 roku to (i) ogólny wymóg informowania odpowiedniego (tj. „właściwego") organu ochrony danych o naruszeniu ochrony danych osobowych, mogącym zagrażać prawom i swobodom osób fizycznych oraz (ii) obowiązek informowania osób, których dane dotyczą, o takim naruszeniu, które może powodować „wysokie ryzyko" dla praw i wolności osób fizycznych.

Grupa Robocza Art. 29 wydała szczegółowe wytyczne dotyczące sposobu postępowania z naruszeniami ochrony danych osobowych[405], które zostały na pierwszym posiedzeniu zatwierdzone przez Europejską Radę Ochrony Danych[406]. Poniższa dyskusja jest w znaczącej mierze oparta właśnie na tych wytycznych. Przykłady także zaczerpnięto z wytycznych Grupy Roboczej Art. 29[407].

Informowanie odpowiedniego organu ochrony danych:

Idea zgłaszania naruszenia ochrony danych osobowych nie jest niczym nowym. Jak wspomniano w pkt 1.3.3 powyżej[408], obowiązek zgłoszenia naruszenia ochrony danych osobowych uwzględniono już w Dyrektywie o e-prywatności. Ograniczał się on jednak tam do dostawców sieci i usług łączności elektronicznej[409]. RODO stosuje taką samą definicję *„naruszenia ochrony danych osobowych",* jak ta zawarta w Dyrektywa o e-prywatności, jednak z poniższym ograniczeniem:

> 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(12))[410]

Wytyczne Grupy Roboczej Art. 29 szczegółowo wyjaśniają, co oznaczają odpowiednie zwroty oraz określają różne rodzaje naruszenia ochrony danych osobowych (*„naruszenie poufności"; „naruszenie integralności", „naruszenie dostępności")*[411].

Przykłady

Przykładem utraty danych osobowych może być zgubienie lub kradzież urządzenia zawierającego kopię obsługiwanej przez administratora bazy danych klientów. Kolejnym przykładem utraty może być zaszyfrowanie jedynej kopii danych osobowych przez oprogramowanie stosowane w przestępczości internetowej (ransomware, tj. złośliwe oprogramowanie szyfrujące dane administratora do czasu zapłacenia okupu) lub przez administratora przy użyciu utraconego klucza.

Przykłady utraty dostępności obejmują sytuacje, w których dane zostały usunięte albo przypadkowo, albo przez nieupoważnioną osobę lub w przypadku bezpiecznie zaszyfrowanych danych, gdy utracono klucz do ich odszyfrowania. W przypadku, gdy administrator nie jest w stanie przywrócić dostępu do danych, na przykład z kopii zapasowej, traktowane jest to jako trwała utrata dostępności.

Utrata dostępności może mieć także miejsce w przypadku poważnego zakłócenia w normalnym funkcjonowaniu organizacji, na przykład awarii zasilania, ataku, lub odmowy dostępu, który sprawia, że dane osobowe stają się niedostępne.

---

[405] WP29, Wytyczne w sprawie powiadomień o naruszeniu ochrony danych osobowych na mocy rozporządzenia 2016/679 (WP250 rev.01, przyjęte 3 października 2017 r., skorygowane i ponownie przyjęte 6 listopada 2018 r. (dalej: „Wytyczne Grupy Roboczej Art. 29 dotyczące zgłaszania naruszenia ochrony danych lub w niniejszym rozdziale „Wytyczne Grupy Roboczej Art. 29"): https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052.

[406] Zob. przypis 248 powyżej.

[407] Wytyczne Grupy Roboczej Art. 29 poruszają także kwestię obowiązku zgłaszania naruszenia na mocy innych instrumentów prawnych. Zob. część VI Wytycznych. Obwiązek ten nie jest jednak przedmiotem niniejszego Podręcznika.

[408] Zob. punkt zatytułowany *„Kluczowe cechy Rozporządzenia o e-prywatności"* w części zatytułowanej „Zgłaszanie naruszenia ochrony danych".

[409] Jak zauważono we Wprowadzeniu do Wytycznych Grupy Roboczej Art. 29, niektóre państwa członkowskie już posiadają szersze wymogi dotyczące zgłaszania naruszenia ochrony danych.

[410] Dyrektywa o e-prywatności dodawała po tych słowach zwrot *„w związku ze świadczeniem publicznie dostępnych usług łączności elektronicznej we Wspólnocie" (*art. 2(i)).

[411] Wytyczne Grupy Roboczej Art. 29, str. 7, w nawiązaniu do wcześniejszej (2014) Opinii Grupy Roboczej Art. 29 o zgłaszaniu naruszeń.

Naruszenie ochrony danych osobowych może stanowić nawet tymczasowa utrata dostępności:

> **Przykłady**
>
> W kontekście szpitala brak dostępu do kluczowych informacji na temat pacjentów, nawet tymczasowy, może stanowić ryzyko dla praw i wolności osób fizycznych, np. prowadzić do odwołania operacji i zagrożenia dla życia pacjentów.
>
> Natomiast jeżeli z powodu kilkugodzinnego braku dostępu do swoich systemów (np. na skutek przerwy w dostawie prądu) spółka medialna nie może wysłać newslettera do abonentów, istnieje małe prawdopodobieństwo ryzyka naruszenia praw i wolności osób fizycznych.
>
> Infekcja oprogramowaniem typu ransomware (złośliwym oprogramowaniem, które szyfruje dane administratora do czasu zapłaty okupu) może prowadzić tylko do tymczasowej utraty dostępu do danych, jeżeli można je odzyskać z kopii zapasowej. Mimo wszystko doszło jednak do włamania, w związku z czym może być wymagane zgłoszenie zdarzenia, jeśli kwalifikuje się ono jako naruszenie poufności (tj. atakujący uzyskał dostęp do danych osobowych), co stanowi ryzyko dla praw i wolności osób fizycznych.

Art. 33(1) przewiduje, że:

> W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 55, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia. (art. 33(1)).

„*Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi*”. (art. 33(2)). Grupa Robocza Art. 29 zaleca, by podmiot przetwarzający:

> **bezzwłocznie** zawiadamiał administratora i następnie etapami, wraz z dostępnością dodatkowych szczegółów, przekazywał dalsze informacje o naruszeniu. Pomoże to administratorowi w spełnieniu wymogu poinformowania organu nadzorczego w ciągu 72 godzin. (Wytyczne Grupy Roboczej Art. 29, str. 14)

Przyjmuje się, że administrator danych „**stwierdza**” naruszenie, gdy podmiot przetwarzający go o tym poinformuje[412]; następnie administrator musi powiadomić organ ochrony danych, chyba że zastosowanie ma zastrzeżenie przewidujące, że naruszenie ochrony danych najprawdopodobniej nie zagraża prawom i swobodom osób fizycznych.

W niektórych przypadkach podmiot przetwarzający może świadczyć usługi dla kilku, a nawet dużej liczby różnych administratorów, jak ma to miejsce w przypadku dostawcy usług przechowywania danych w chmurze. W takich sytuacjach Grupa Robocza Art. 29 radzi, by:

> Jeżeli podmiot przetwarzający świadczy usługi na rzecz wielu administratorów, którzy ucierpieli na skutek tego samego incydentu, wówczas musi powiadomić o szczegółach zdarzenia wszystkich administratorów.
>
> Podmiot przetwarzający może dokonać zgłoszenia w imieniu administratora, jeżeli administrator nadał mu odpowiednie upoważnienie i sytuację taką przewidują ustalenia umowne między administratorem a podmiotem przetwarzającym. Zgłoszenia należy wówczas dokonać zgodnie z przepisami art. 33 i 34. Niemniej warto zauważyć, że odpowiedzialność prawna w związku ze zgłoszeniem leży po stronie administratora. (str. 11)

Zgłoszenie naruszenia ochrony danych odpowiedniemu („właściwemu”) organowi ochrony danych[413]„powinno co najmniej”:

[412] Wytyczne Grupy Roboczej 29, str. 14.

[413] Wskazówki dotyczące zgłaszania transgranicznych naruszeń i naruszeń mających miejsce w podmiotach spoza UE - patrz część C Wytycznych Grupy Roboczej Art. 29 (str. 14 – 16).

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".

(art. 33(3)).

W tym względzie Grupa Robocza Art. 29 stwierdza, że administrator może[414]:

> w razie potrzeby przekazać dodatkowe szczegóły. Różne rodzaje naruszeń (poufności, integralności lub dostępności) mogą wymagać przekazania dalszych informacji w celu pełnego wyjaśnienia okoliczności poszczególnych spraw.

Przykład

W ramach powiadomienia organu nadzorczego administrator może uznać za przydatne podanie nazwy podmiotu przetwarzającego dane, jeżeli to on jest pierwotną przyczyną naruszenia, zwłaszcza jeśli doprowadził do zdarzenia, które wpłynęło na wpisy danych osobowych wielu innych administratorów korzystających z usług tego samego podmiotu przetwarzającego.

> Organ nadzoru może w każdym przypadku zażądać dalszych informacji w ramach dochodzenia w sprawie naruszenia.

Ponadto:

> Jeżeli – i w zakresie, w jakim – informacji nie da się udzielić w tym samym czasie, można ich udzielać sukcesywnie bez zbędnej zwłoki. (art. 33(4))[415]

Przykład

W ciągu 72 godzin od wykrycia naruszenia administrator powiadamia organ nadzoru o utracie pamięci USB zawierającej kopię danych osobowych części jego klientów. Później niewłaściwie oznaczona pamięć USB zostaje odnaleziona w lokalu administratora, a jej zawartość odzyskana. Administrator przekazuje organowi nadzorczemu aktualne informacje i prosi o zmianę powiadomienia.

Termin zgłoszenia:

Wytyczne Grupy Roboczej Art. 29 wyjaśniają, kiedy można uznać, że administrator (lub podmiot przetwarzający) „**stwierdza**" naruszenie ochrony danych, a także podkreślają, że podmioty te są zobowiązane przewidywać takie zdarzenia oraz się do nich przygotować[416]:

> Zgodnie z tym, co opisano powyżej, w przypadku naruszenia RODO wymaga od administratora niezwłocznego zgłoszenia takiego naruszenia, jeżeli to możliwe – w ciągu 72 godzin od jego stwierdzenia. Tutaj może pojawić się pytanie, kiedy uznaje się, że administrator „stwierdził" naruszenie. Według GR29 należy uznać, że administrator „stwierdził" naruszenie, kiedy ma wystarczający stopień pewności co do tego, że miało miejsce zdarzenie zagrażające bezpieczeństwu, prowadzące do naruszenia bezpieczeństwa danych osobowych.
>
> Jak jednak wspomniano wcześniej, w RODO ustanowiono wymóg zobowiązujący administratora do wdrożenia wszelkich odpowiednich technicznych środków ochrony i wszelkich odpowiednich środków organizacyjnych, by od razu stwierdzić naruszenie ochrony danych osobowych i szybko poinformować organ nadzorczy i osoby, których dane dotyczą. W RODO stwierdzono również, że to, czy zawiadomienia dokonano bez zbędnej zwłoki, należy ustalić z uwzględnieniem w szczególności charakteru i wagi naruszenia ochrony danych osobowych, jego konsekwencji oraz niekorzystnych skutków dla osoby, której dane dotyczą. Wiąże się to z nałożeniem na

[414] Wytyczne Grupy Roboczej Art. 29, str. 12.
[415] Szczegóły i dodatkowe wytyczne w tej kwestii – zob. Wytyczne Grupy Roboczej Art. 29, str. 13-14.
[416] Wytyczne Grupy Roboczej Art. 29, str. 11-12.

administratora obowiązku utrzymania zdolności do terminowego „stwierdzania" wystąpienia wszelkich naruszeń, aby zapewnić możliwość podjęcia stosownych działań.

To, kiedy dokładnie można uznać, że administrator „stwierdził" wystąpienie określonego naruszenia, będzie zależało od okoliczności, w jakich doszło do tego naruszenia. W niektórych przypadkach wystąpienie naruszenia można stosunkowo łatwo stwierdzić już na początku, natomiast w innych ustalenie, czy doszło do ujawnienia danych osobowych, może wymagać czasu. W tym kontekście powinno się jednak położyć nacisk na szybkie zbadanie danego incydentu w celu ustalenia, czy faktycznie doszło do naruszenia ochrony danych osobowych, a jeżeli tak – podjąć działania zaradcze i, w razie konieczności, zgłosić naruszenie.

Przykłady

1. W przypadku utraty pamięci USB zawierającej niezaszyfrowane dane osobowe ustalenie, czy nieuprawnione osoby uzyskały dostęp do tych danych okazuje się często niemożliwe. Niemniej jednak, mimo że administrator może nie być w stanie ustalić, czy w danym przypadku doszło do naruszenia dotyczącego poufności danych, taki przypadek musi zostać zgłoszony, ponieważ można z wystarczającą dozą pewności stwierdzić, że doszło do naruszenia dotyczącego dostępności danych; w tym kontekście przyjmuje się, że administrator „stwierdził" wystąpienie naruszenia w momencie, w którym zdał sobie sprawę z utraty pamięci USB.

2. Osoba trzecia informuje administratora, że przypadkowo otrzymała dane osobowe jednego z jego klientów, i przedstawia dowody potwierdzające, że doszło do nieuprawnionego ujawnienia tych danych. Ponieważ administrator otrzymał dowody jednoznacznie świadczące o wystąpieniu naruszenia dotyczącego poufności danych, nie można mieć żadnych wątpliwości co do tego, że „stwierdził" wystąpienie takiego naruszenia.

3. Administrator wykrywa potencjalne włamanie do swojej sieci. Administrator sprawdza systemy w celu ustalenia, czy bezpieczeństwo danych osobowych przechowywanych w tym systemie zostało narażone na szwank, po czym potwierdza, że faktycznie tak się stało. Ponieważ administrator uzyskał dowody jednoznacznie świadczące o wystąpieniu naruszenia, nie można mieć żadnych wątpliwości co do tego, że stwierdził wystąpienie takiego naruszenia.

4. Cyberprzestępca kontaktuje się z administratorem po włamaniu się do jego systemu, aby zażądać okupu. W takim przypadku – po sprawdzeniu swojego systemu i potwierdzeniu, że faktycznie został on zaatakowany – administrator dysponuje dowodem jednoznacznie świadczącym o wystąpieniu naruszenia, dlatego też nie można mieć żadnych wątpliwości co do tego, że stwierdził wystąpienie takiego naruszenia.

5. Osoba fizyczna informuje administratora, że otrzymała wiadomość e-mail, której nadawca podszywa się pod administratora i która zawiera dane osobowe dotyczące (faktycznego) korzystania z usług administratora przez tę osobę, i sugeruje, że doszło do złamania środków bezpieczeństwa stosowanych przez administratora. Administrator przeprowadza krótkie postępowanie, w toku którego uzyskuje potwierdzenie, że doszło do włamania do jego sieci, i gromadzi dowody świadczące o nieuprawnionym dostępie do danych osobowych. Od tego momentu przyjmuje się, że administrator „stwierdził" wystąpienie naruszenia, a zgłoszenie naruszenia organowi nadzorczemu staje się obowiązkowe, chyba że prawdopodobieństwo, że będzie wiązało się ono z ryzykiem naruszenia praw i wolności osób fizycznych, jest niewielkie. Administrator będzie musiał podjąć odpowiednie działania zaradcze, aby zaradzić naruszeniu.

Dokumentowanie i ocena naruszenia:

RODO przewiduje także, że:

> Administrator dokumentuje **wszelkie** naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu na weryfikowanie przestrzegania niniejszego artykułu. (art. 33(5), pogrubienie dodano)

Należy zauważyć, że ten ostatni wymóg ma zastosowanie do „**wszelkich**" przypadków (tj. każdego) naruszenia ochrony danych osobowych, a nie ogranicza się do naruszenia danych podlegającego obowiązkowemu zgłoszeniu do organu ochrony danych. Oznacza to, że do rejestru należy wpisywać także naruszenie ochrony danych, w przypadku których (zdaniem administratora)

„prawdopodobieństwo, że będzie wiązało się ono z ryzykiem naruszenia praw i wolności osób fizycznych, jest niewielkie".

W praktyce inspektor ochrony danych powinien zostać mocno zaangażowany we wszystkie tego typu sprawy. Często podejrzenie naruszenia należy w pierwszej kolejności zgłosić inspektorowi w ramach własnej organizacji (i/lub dyrektorowi ds. technologicznych albo inspektorowi ds. bezpieczeństwa), a ten z kolei jest zobowiązany (w stosownym przypadku wraz z pozostałymi dyrektorami/inspektorami) dokonać pierwszej natychmiastowej oceny co najmniej następujących kwestii:

- czy faktycznie doszło do naruszenia ochrony danych zgodnie z definicją zawartą w RODO (patrz wyżej cytowana definicja w art. 4(12)) -

  i jeżeli ustalono, że doszło do naruszenia lub że istnieje prawdopodobieństwo wystąpienia naruszenia:

- jakie osoby (kategorie osób, których dane dotyczą), zostały lub mogły zostać dotknięte naruszeniem oraz jakie dane osobowe (jakie kategorie danych osobowych) mogły zostać utracone lub w inny sposób dotknięte naruszeniem -

  Uwaga: Grupa Robocza Art. 29 zaleca, by tego typu kategorie także zgłaszać organowi ochrony danych w każdym powiadomieniu o naruszeniu oraz by [417]:

  rodzaje osób, których dane dotyczą, lub rodzaje danych osobowych wskazujących na istnienie ryzyka wyrządzenia określonych szkód w rezultacie naruszenia (np. kradzież tożsamości, oszustwo, strata finansowa, ryzyko naruszenia poufności danych chronionych tajemnicą zawodową), wskazać w odpowiedniej kategorii w zgłoszeniu. W ten sposób powiązane jest to z wymogiem opisania prawdopodobnych konsekwencji naruszenia.

  oraz biorąc pod uwagę poniższe kwestie:

- czy jest lub nie jest prawdopodobne, aby naruszenie bezpieczeństwa danych osobowych skutkowało ryzykiem naruszania praw i wolności osób fizycznych -

  Grupa Robocza Art. 29 bardziej szczegółowo omawia sytuacje, w których zgłoszenie nie jest wymagane[418] i przedstawia następujący przykład:

> **Przykład**
>
> Przykładem naruszenia, które nie wymagałoby zgłoszenia organowi nadzorczemu, byłaby utrata bezpiecznie zaszyfrowanego urządzenia mobilnego, z którego korzystają administrator i jego pracownicy. Zakładając, że klucz kryptograficzny jest bezpiecznie przechowywany przez administratora i nie jest to jedyna kopia danych osobowych, dane osobowe będą niedostępne dla atakującego. Oznacza to, że przedmiotowe naruszenie najprawdopodobniej nie będzie wiązało się z ryzykiem naruszenia praw i wolności osób, których te dane dotyczą. Jeżeli później okaże się, że klucz kryptograficzny został złamany, oprogramowanie lub algorytm szyfrujący ma słabe punkty, poziom ryzyka naruszenia praw i wolności osób fizycznych zmieni się i wówczas zgłoszenie może stać się konieczne.

  przy czym jeżeli ocena wykaże istnienie prawdopodobieństwa wystąpienia takiego potencjalnego ryzyka:

- czy ryzyko stanowi „wysokie ryzyko naruszenia praw lub wolności osób fizycznych" (ponieważ wymagałoby nie tylko przekazania uzasadnienia naruszenia do organu ochrony danych, ale także poinformowania osób, których dane dotyczą, jak zauważono w następnym punkcie)[419].

[417] Wytyczne Grupy Roboczej Art. 29, str. 16.
[418] Wytyczne Grupy Roboczej Art. 29, str. 22-23. Zob. także przykładowa lista przykładów w załączniku (Załącznik B) do Wytycznych, który odtworzono poniżej w kolejnym punkcie.
[419] Zob. w szczególności punkt zatytułowany „*Ocena ryzyka i wysokiego ryzyka*".

Jak wskazuje Grupa Robocza Art. 29, znaczenie zdolności do określenia, czy w danym przypadku doszło do naruszenia, ocenienia ryzyka dla osób fizycznych oraz późniejszego zgłoszenia naruszenia w przypadkach, w których będzie to konieczne, podkreślono w motywie 87 RODO:

> Należy się upewnić, czy wdrożono wszelkie odpowiednie techniczne środki ochrony i wszelkie odpowiednie środki organizacyjne, by od razu stwierdzić naruszenie ochrony danych osobowych i szybko poinformować organ nadzorczy i osobę, której dane dotyczą. To, czy zawiadomienia dokonano bez zbędnej zwłoki, należy ustalić z uwzględnieniem w szczególności charakteru i wagi naruszenia ochrony danych osobowych, jego konsekwencji oraz niekorzystnych skutków dla osoby, której dane dotyczą. Takie zawiadomienie może skutkować interwencją organu nadzorczego, zgodnie z jego zadaniami i uprawnieniami określonymi w niniejszym rozporządzeniu.

I oczywiście, jeżeli ocena wskaże na wystąpienie naruszenia oraz zagrożenia dla interesów osób fizycznych, należy pilnie ustalić **działania łagodzące.**

Kwestie takie należy także **bezzwłocznie, najszybciej jak to możliwe,** przekazać kierownictwu najwyższego szczebla. Jakiekolwiek wewnętrzne dyskusje na ten temat nie powinny opóźniać poinformowania kierownictwa tak szybko, jak to możliwe, po ustaleniu naruszenia.

Fakt, że oceny takie przeprowadzono w sumienny sposób, należy **starannie odnotować**[420]. Uwzględnić przy tym wyniki odpowiednich ocen oraz ich przyczyn, rozpatrywane środki łagodzące oraz fakt, że o ocenie i proponowanych środkach łagodzących poinformowano kierownictwo najwyższego szczebla, a także podjęto konkretne środki zatwierdzone przez to kierownictwo oraz to, czy i kiedy zostaną one podjęte. Przy ocenie należy także uwzględnić fakt, że naruszenie (jeżeli wymaga zgłoszenia) zostało zgłoszone odpowiedniemu organowi ochrony danych oraz kiedy (dokładna data), wraz z kopią zgłoszenia, a także, tam, gdzie to wymagane, uwzględnienie faktu, że osoby, których dane dotyczą, zostały poinformowane o naruszeniu oraz w jaki sposób, wraz z kopią odpowiedniego zgłoszenia i odpowiedniej notatki prasowej, itp. (w sposób omówiony w kolejnym punkcie). Ponadto, jak stwierdzono w Wytycznych Grupy Roboczej Art. 29:

> Informacje na temat naruszenia powinny być dokumentowane w miarę rozwoju sytuacji (str. 14).

W organizacjach, które wyznaczyły inspektora ochrony danych, powinien on odgrywać istotną rolę w tym zakresie, co podkreśla Grupa Robocza Art. 29[421]:

> Administrator lub podmiot przetwarzający może wyznaczyć inspektora ochrony danych – zgodnie z wymogami art. 37 albo dobrowolnie w ramach dobrej praktyki. W art. 39 RODO określono szereg zadań wchodzących w zakres obowiązków inspektora ochrony danych, co jednak nie uniemożliwia przydzielenia mu – w stosownych przypadkach – dodatkowych zadań przez podmiot przetwarzający.
>
> Do zadań wchodzących w zakres obowiązków inspektora ochrony danych, które są szczególnie istotne z punktu widzenia zgłaszania naruszenia – obok innych obowiązków – należą przekazywanie administratorowi lub podmiotowi przetwarzającemu zaleceń oraz informacji dotyczących ochrony danych, monitorowanie przestrzegania przepisów RODO oraz przekazywanie zaleceń w zakresie ocen skutków dla ochrony danych. Inspektor ochrony danych musi również współpracować z organem nadzorczym i służyć jako punkt kontaktowy dla organu nadzorczego i osób, których dane dotyczą. Należy również podkreślić, że zgodnie z art. 33 ust. 3 lit. b) podczas zgłaszania naruszenia organowi nadzorczemu administrator musi przekazać imię i nazwisko oraz dane kontaktowe swojego inspektora ochrony danych lub innego punktu kontaktowego.
>
> W kwestii dokumentowania naruszeń administrator lub podmiot przetwarzający mogą rozważyć zasięgnięcie opinii swojego inspektora ochrony danych na temat struktury i przygotowania dokumentacji oraz zarządzania nią. Inspektor ochrony danych może również otrzymać dodatkowe zadanie polegające na prowadzeniu takich rejestrów.
>
> Z powyższych czynników wynika, że inspektor ochrony danych powinien odgrywać kluczową rolę we wspieraniu zapobiegania naruszeniom lub przygotowaniu na wypadek ich wystąpienia poprzez wydawanie zaleceń i monitorowanie przestrzegania przepisów, jak również w sytuacji naruszenia

[420] Grupa Robocza Art. 29 sugeruje, aby dokonać tego *„w sporządzonych przez administratora planach reagowania na incydenty lub w przyjętych przez niego zasadach zarządzania"* (str. 12). Warunki te omówiono szczegółowo w części V Wytycznych Grupy Roboczej Art. 29, *„Rozliczalność i prowadzenie dokumentacji"*.
[421] Wytyczne Grupy Roboczej Art. 29, pkt V.B str. 32-33.

> (tj. podczas zgłaszania naruszenia organowi nadzorczemu) oraz podczas wszelkich dalszych postępowań prowadzonych przez organ nadzorczy. W tym kontekście Grupa Robocza Art. 29 zaleca niezwłoczne informowanie inspektora ochrony danych o wystąpieniu naruszenia oraz angażowanie go na wszystkich etapach procesu zarządzania w sytuacji wystąpienia naruszenia oraz procesu zgłaszania naruszenia.

Wytyczne Grupy Roboczej Art. 29 wyjaśniają, że organizacje nie powinny w tym zakresie przyjmować jedynie reaktywnej postawy. Powinny raczej wprowadzić **politykę bezpieczeństwa**, która ***z góry*** pozwala uniknąć naruszenia ochrony danych oraz zawiera plany zapobiegania, łagodzenia i rozwiązywania tego typu incydentów. W odniesieniu do czynności przetwarzania danych osobowych, które mogą powodować wysokie ryzyko związane z interesem osób fizycznych, opracowanie tego typu strategii może stanowić część odpowiedniej oceny skutków dla ochrony danych (patrz Zadanie 4 powyżej)[422].

Informowanie osób, których dane dotyczą:

Grupa Robocza Art. 29 wyjaśnia wymogi informowania osób, których dane dotyczą, o naruszeniu ochrony danych w następujący sposób:

> W niektórych przypadkach administrator musi nie tylko zgłosić naruszenie organowi nadzorczemu, ale również powiadomić o nim osoby fizyczne, na które to naruszenie wywiera wpływ.
>
> Art. 34 ust. 1 stanowi, że:
>
> > Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.
>
> Administratorzy powinni pamiętać, że zgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu jest obowiązkowe, chyba że jest mało prawdopodobne, by skutkowało ono ryzykiem naruszenia praw i wolności osób fizycznych. Ponadto jeżeli istnieje prawdopodobieństwo, że naruszenie ochrony danych osobowych spowoduje wysokie ryzyko naruszenia praw i wolności osób fizycznych, należy poinformować o nim również osoby fizyczne. A zatem poziom zagrożenia skutkujący powstaniem obowiązku przekazania osobom fizycznym informacji o naruszeniu jest wyższy niż w przypadku zgłaszania naruszenia organom nadzorczym, dzięki czemu nie ma obowiązku zgłaszania osobom fizycznym wszystkich naruszeń, co pozwala ochronić je przed nadmiarem niepotrzebnych powiadomień.
>
> RODO stanowi, że osoby fizyczne należy poinformować o naruszeniu „bez zbędnej zwłoki", tj. najszybciej jak to możliwe. Zawiadomienie osób fizycznych ma na celu przede wszystkim dostarczenie im szczegółowych informacji na temat działań zapobiegawczych, które powinny podjąć. Jak wspomniano powyżej, w zależności od charakteru naruszenia i powstałego ryzyka, szybkie zawiadomienie pozwoli osobom fizycznym podjąć działania, aby uchronić się przed wszelkimi negatywnymi skutkami naruszenia.

W Załączniku B do Wytycznych Grupy Roboczej Art. 29 przedstawiono przykładowy wykaz 10 sytuacji naruszenia ochrony danych osobowych z informacją, kogo należy zawiadomić.

Wytyczne Grupy Roboczej Art. 29 dodają[423]:

> **Informacje, których należy udzielić**
>
> W odniesieniu do zawiadamiania osób fizycznych art. 34(2) stanowi, że:
>
> > Zawiadomienie, o którym mowa w ust. 1 niniejszego artykułu, jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki, o których mowa w art. 33 ust. 3 lit. b), c) i d).
>
> Zgodnie z tym przepisem administrator musi udzielić co najmniej następujących informacji:
>
> - opis charakteru naruszenia;
> - imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego;

[422] Wytyczne Grupy Roboczej Art. 29, str. 8.
[423] Część III.B, str. 22. Tekst po edycji, wyłącznie dla celów prezentacji.

- opis możliwych konsekwencji naruszenia oraz
- opis środków zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

Przykład:

Jednym z przykładów środków zastosowanych w celu zaradzenia naruszeniu i zminimalizowania jego ewentualnych negatywnych skutków może być deklaracja administratora, że po zgłoszeniu naruszenia właściwemu organowi nadzorczemu administrator uzyskał zalecenie dotyczące zarządzania naruszeniem i ograniczenia jego wpływu. Administrator powinien również – w stosownych przypadkach – przekazać osobom fizycznym szczegółowe zalecenia na temat sposobów ochrony przed potencjalnymi niekorzystnymi skutkami naruszenia – takich jak zmiana haseł – jeżeli ich dane uwierzytelniające zostały ujawnione. Również w tym wypadku administrator może podjąć decyzję o przekazaniu większej ilości informacji, niż jest to wymagane.

Wytyczne wyjaśniają również, że[424]:

> Co do zasady osoby, których dane dotyczą, należy zawiadomić o naruszeniu bezpośrednio, chyba że takie działanie wymagałoby niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób (art. 34(3)(c)).

Osoby, których dane dotyczą, należy poinformować „tak szybko, jak jest to rozsądnie możliwe, w ścisłej współpracy z organem nadzorczym" (motyw 86). Wytyczne podkreślają ponadto, że[425]:

> Kontakt i konsultacje z organem nadzorczym pozwolą administratorom uzyskać nie tylko zalecenia na temat powiadamiania osób, których dane dotyczą, o naruszeniu zgodnie z art. 34, ale również na temat stosownych wiadomości, które należy wysłać do osób fizycznych oraz najwłaściwszego sposobu skontaktowania się z nimi.
>
> Kwestii tej dotyczy zalecenie zawarte w motywie 88, które stanowi, że w zawiadomieniu o naruszeniu „należy [...] uwzględnić prawnie uzasadnione interesy organów ścigania, jeżeli przedwczesne ujawnienie mogłoby niepotrzebnie utrudnić badanie okoliczności naruszenia ochrony danych osobowych". Może to oznaczać, że w pewnych okolicznościach, gdy jest to uzasadnione, oraz zgodnie z zaleceniami organów ścigania, administrator może opóźnić wysłanie zawiadomienia o naruszeniu do osób fizycznych, na które wywiera ono wpływ, do momentu, w którym takie zawiadomienie nie zaszkodzi takim postępowaniom. Osoby, których dane dotyczą, należy jednak wciąż natychmiast poinformować po upływie tego okresu.
>
> Jeżeli administrator nie jest w stanie zawiadomić danej osoby fizycznej o naruszeniu, ponieważ przechowywane dane są niewystarczające do skontaktowania się z tą osobą, w takim szczególnym przypadku administrator powinien ją poinformować tak szybko, jak jest to rozsądnie wykonalne (np. jeżeli osoba fizyczna skorzysta z przewidzianego w art. 15 prawa do uzyskania dostępu do swoich danych osobowych i dostarczy administratorowi dodatkowe informacje wymagane do skontaktowania się z nią).

Wyjątki

Jak zauważono w Wytycznych Grupy Roboczej Art. 29[426]:

> W art. 34(3) określono trzy sytuacje, w których nie ma konieczności zawiadomienia osób fizycznych w przypadku wystąpienia naruszenia. Sytuacje te są następujące:
>
> - administrator zastosował przed wystąpieniem naruszenia odpowiednie techniczne i organizacyjne środki w celu ochrony danych osobowych, w szczególności środki uniemożliwiające odczyt danych osobom, które nie są uprawnione do dostępu do tych danych. Może to na przykład obejmować zabezpieczenie danych osobowych za pomocą najnowocześniejszego szyfrowania lub tokenizacji;

[424] Część III.C, str. 21; zob. dalsze wskazówki dotyczące innych sposobów informowania odpowiednich osób, których dane dotyczą, o naruszeniu danych.
[425] *Idem*, str. 23 – 25.
[426] Część III.D, p. 24.

- natychmiast po wystąpieniu naruszenia administrator podjął działania w celu wyeliminowania prawdopodobieństwa powstania wysokiego ryzyka naruszenia praw lub wolności osoby fizycznej. Na przykład w niektórych sytuacjach administrator mógł natychmiast zidentyfikować osobę fizyczną, która uzyskała dostęp do danych osobowych, i podjąć wobec niej działania, zanim mogła ona w jakikolwiek sposób wykorzystać te dane. Mimo to należy odpowiednio uwzględnić możliwe skutki każdego naruszenia poufności, również w tym wypadku biorąc pod uwagę charakter przedmiotowych danych;
- skontaktowanie się z danymi osobami fizycznymi wymagałoby niewspółmiernie dużego wysiłku, na przykład ponieważ w wyniku naruszenia utracono ich dane kontaktowe albo dane te nigdy nie były znane. Na przykład archiwum urzędu statystycznego uległo zalaniu, a dokumenty zawierające dane osobowe przechowywano tylko w formie papierowej. W takim przypadku administrator musi wydać publiczny komunikat lub zastosować podobny środek, za pomocą którego osoby fizyczne zostaną poinformowane w równie skuteczny sposób. Jeżeli wykonanie tego działania wymagałoby niewspółmiernie dużego wysiłku, można również przewidzieć uzgodnienia techniczne, dzięki którym informacje na temat naruszenia będą dostępne na żądanie, co może okazać się przydatne dla osób, na które naruszenie mogło wywrzeć wpływ, lecz z którymi administrator nie mógł się w inny sposób skontaktować.

Zgodnie z zasadą rozliczalności administratorzy powinni być w stanie wykazać przed organem nadzorczym, że spełniają co najmniej jeden z tych warunków. Warto pamiętać, że choć początkowo zgłoszenie może nie być wymagane ze względu na fakt, że prawdopodobieństwo wystąpienia ryzyka naruszenia praw i wolności osób fizycznych jest niskie, z czasem sytuacja może się zmienić i może wystąpić konieczność przeprowadzenia kolejnej oceny ryzyka.

Jeżeli administrator zdecyduje się nie zawiadamiać osoby fizycznej o naruszeniu, w art. 34(4) wyjaśniono, że organ nadzorczy może od niego tego zażądać, jeżeli jego zdaniem naruszenie może powodować wysokie ryzyko dla osób fizycznych. Ewentualnie może stwierdzić, że spełnione zostały warunki, o których mowa w art. 34(3), i w takim przypadku zawiadomienie osób fizycznych nie jest konieczne. Jeżeli organ nadzorczy stwierdzi, że decyzja o niezawiadamianiu osób, których dane dotyczą, nie jest odpowiednio uzasadniona, może rozważyć wykorzystanie swoich uprawnień i nałożenie sankcji.

Ocena ryzyka i wysokiego ryzyka:

Ponownie, wystarczy zacytować Wytyczne Grupy Roboczej Art. 29[427]:

Mimo że w RODO wprowadzono obowiązek zgłaszania naruszenia, nie jest ono wymagane we wszystkich sytuacjach:

- zgłoszenie naruszenia właściwemu organowi nadzorczemu jest obowiązkowe, chyba że dane naruszenie najprawdopodobniej nie będzie wiązało się z ryzykiem naruszenia praw i wolności osób fizycznych;
- osobę fizyczną zawiadamia się o naruszeniu jedynie wówczas, gdy naruszenie może powodować wysokie ryzyko naruszenia praw i wolności tych osób.

Oznacza to, że natychmiast po stwierdzeniu naruszenia administrator musi nie tylko dążyć do ograniczenia negatywnych skutków incydentu, lecz również ocenić ryzyko, które może powstać w wyniku tego naruszenia. Wynika to z dwóch ważnych przyczyn: po pierwsze, znajomość prawdopodobieństwa i potencjalnej dotkliwości wpływu na osoby fizyczne pomoże administratorowi w podjęciu skutecznych działań pozwalających zapanować nad skutkami naruszenia i je zminimalizować; po drugie, pomoże administratorowi stwierdzić, czy zgłoszenie naruszenia organowi nadzorczemu oraz – w stosownych przypadkach – osobom, których dotyczy naruszenie, jest konieczne.

Jak wyjaśniono powyżej, zgłoszenie naruszenia jest obowiązkowe, chyba że jest mało prawdopodobne, by skutkowało ono ryzykiem naruszenia praw i wolności osób fizycznych, a to, czy o naruszeniu należy zawiadomić osoby, których dane dotyczą, zależy przede wszystkim od tego, czy naruszenie może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych. Ryzyko to istnieje w przypadku, gdy naruszenie może prowadzić do uszczerbku fizycznego lub szkód majątkowych lub niemajątkowych dla osób, których dane zostały naruszone.

[427] Część IV.A i B, str. 26, przypisy pominięto; z uwzględnieniem edycji dla celów prezentacji.

Przykłady:

Przykłady takich szkód obejmują dyskryminację, kradzież lub sfałszowanie tożsamości, straty finansowe i naruszenie dobrego imienia. Jeżeli naruszenie obejmuje dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, wyznanie lub przekonania światopoglądowe, lub przynależność do związków zawodowych oraz jeżeli przetwarzane są dane genetyczne, dane dotyczące zdrowia lub seksualności lub dane dotyczące wyroków skazujących i naruszeń prawa lub związanych z tym środków bezpieczeństwa – należy uznać, że taka szkoda prawdopodobnie nastąpi.

Czynniki, które należy uwzględnić podczas oceny ryzyka

Zgodnie z zaleceniami zawartymi w motywach 75 i 76 RODO podczas oceny ryzyka zasadniczo należy wziąć pod uwagę zarówno prawdopodobieństwo, jak i powagę ryzyka naruszenia praw lub wolności osób, których dane dotyczą. Stwierdzono również, że ryzyko naruszenia należy oszacować na podstawie obiektywnej oceny.

Należy podkreślić, że podczas oceny ryzyka naruszenia praw i wolności osób fizycznych powstałego w wyniku wystąpienia naruszenia kładzie się nacisk na inne kwestie, niż kwestie dotyczące ryzyka uwzględniane w ocenie skutków dla ochrony danych. W ocenie skutków dla ochrony danych bierze się pod uwagę zarówno ryzyko dla planowego przetwarzania danych, jak i ryzyko powstałe w przypadku wystąpienia naruszenia. Badając możliwe naruszenie, rozpatruje się w ujęciu ogólnym prawdopodobieństwo jego wystąpienia oraz szkody dla osób, których dane dotyczą, jakie mogą z niego wyniknąć; innymi słowy, jest to ocena wydarzenia hipotetycznego. W przypadku faktycznego naruszenia wydarzenie już nastąpiło, więc nacisk kładzie się w całości na powstałe ryzyko, że naruszenie będzie skutkowało wpływem na osoby fizyczne.

Przykład:

Z oceny skutków dla ochrony danych wynika, że rozważane wykorzystanie określonego oprogramowania zabezpieczającego do ochrony danych osobowych stanowi właściwy środek służący zapewnieniu stopnia bezpieczeństwa, który jest odpowiedni względem ryzyka dla osób fizycznych, jakie w innym przypadku wynikałoby z przetwarzania danych. Gdyby jednak w późniejszym czasie wykryto lukę w zabezpieczeniach, sytuacja ta wpłynęłaby na przydatność oprogramowania do ograniczenia ryzyka dla chronionych danych osobowych, a zatem oprogramowanie należałoby poddać ponownej ocenie w ramach trwającej oceny skutków dla ochrony danych.

Luka w oprogramowaniu zostaje później wykorzystana i następuje naruszenie. Administrator powinien przeprowadzić ocenę konkretnych okoliczności naruszenia, sprawdzić, których danych dotyczy naruszenie, a także oszacować potencjalny poziom wpływu na osoby fizyczne i prawdopodobieństwo wystąpienia tego ryzyka.

Oceniając ryzyko dla osób fizycznych będące wynikiem naruszenia, administrator powinien uwzględnić zatem konkretne okoliczności naruszenia, w tym wagę potencjalnego wpływu i prawdopodobieństwo jego wystąpienia. Grupa Robocza Art. 29 zaleca zatem, aby w trakcie oceny brano pod uwagę następujące kryteria[428]:

Rodzaj naruszenia

Rodzaj stwierdzonego naruszenia może wpłynąć na poziom ryzyka dla osób fizycznych.

Przykład:

Konsekwencje dla osoby fizycznej w przypadku naruszenia dotyczącego poufności danych, którego istotą jest ujawnienie informacji medycznych osobom nieupoważnionym, mogą być inne niż konsekwencje naruszenia polegającego na utracie informacji medycznych danej osoby, do których nie ma już dostępu.

[428] Art. 3.2 Rozporządzenia 611/2013 zawiera wytyczne dotyczące czynników, jakie należy wziąć pod uwagę w związku ze zgłoszeniem naruszenia w sektorze usług łączności elektronicznej, które mogą być przydatne w kontekście zgłaszania naruszenia na mocy RODO. Zob. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:pl:PDF [oryginalny przypis].

Charakter, wrażliwość i ilość danych osobowych

Kluczowym czynnikiem podczas oceniania ryzyka jest oczywiście rodzaj i wrażliwość danych osobowych, które zostały ujawnione w wyniku naruszenia. Zazwyczaj ryzyko powstania szkody dla osób, których dotyczy naruszenie, wzrasta wraz z wrażliwością danych, lecz należy wziąć pod uwagę również inne dane osobowe dotyczące tych osób, które mogą już być dostępne. Na przykład ujawnienie imienia i nazwiska oraz adresu danej osoby prawdopodobnie nie wyrządzi jej szkody w normalnej sytuacji. Jednak jeżeli imię i nazwisko oraz adres rodzica adopcyjnego zostaną ujawnione rodzicowi biologicznemu, może mieć to bardzo poważne konsekwencje zarówno dla rodzica adopcyjnego, jak i dla dziecka.

Naruszenia powiązane z danymi dotyczącymi zdrowia, dokumentami tożsamości lub danymi finansowymi, takimi jak dane kart kredytowych mogą spowodować szkody, jeżeli występują pojedynczo, lecz jeżeli wystąpią łącznie, mogą zostać wykorzystane do kradzieży tożsamości. Zbiór różnych danych osobowych ma zazwyczaj bardziej wrażliwy charakter niż pojedynczy element danych osobowych.

Niektóre rodzaje danych osobowych mogą się na pierwszy rzut oka wydawać nieszkodliwe, ale należy dokładnie rozważyć, jakie informacje takie dane mogą ujawnić na temat osoby fizycznej, na którą naruszenie wywiera wpływ. Wykaz klientów regularnie odbierających dostawy może nie stanowić szczególnie wrażliwych danych, ale takie same dane na temat klientów, którzy poprosili o wstrzymanie dostaw na czas urlopu, byłyby dla przestępców przydatne.

Ponadto niewielka ilość bardzo wrażliwych danych osobowych może mieć znaczny wpływ na daną osobę fizyczną, a wiele różnych szczegółów może się ujawnić szerszy zakres informacji na temat tej osoby. Podobnie naruszenie, które ma wpływ na duże ilości danych osobowych dotyczące wielu osób, może wywołać skutki dla odpowiednio dużej liczby osób fizycznych.

Łatwość identyfikacji osób fizycznych

Istotnym czynnikiem, który należy wziąć pod uwagę, jest łatwość, z jaką strona, która ma dostęp do ujawnionych danych osobowych, będzie w stanie zidentyfikować konkretne osoby fizyczne lub dopasować dane do innych informacji służących identyfikacji osób fizycznych. W zależności od okoliczności identyfikacja może być możliwa bezpośrednio w oparciu o dane osobowe, których dotyczy naruszenie, bez potrzeby gromadzenia dodatkowych informacji pozwalających określić tożsamość danej osoby lub dopasowanie danych osobowych do konkretnej osoby może być bardzo trudne, lecz wciąż wykonalne pod pewnymi warunkami. Identyfikacja może być pośrednio lub bezpośrednio możliwa w oparciu o ujawnione dane, ale może również zależeć od konkretnego kontekstu naruszenia i publicznej dostępności powiązanych danych osobowych. Może to mieć większe znaczenie w przypadku naruszeń dotyczących poufności i dostępności danych.

Jak stwierdzono powyżej, dane osobowe chronione za pomocą odpowiedniego poziomu szyfrowania będą nieczytelne dla osób nieupoważnionych, które nie posiadają klucza deszyfrującego. Ponadto odpowiednio wdrożona pseudonimizacja (zdefiniowana w art. 4(5) jako „przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej") również może zmniejszyć prawdopodobieństwo zidentyfikowania osób fizycznych w przypadku naruszenia. Jednak aby dane były nieczytelne, nie można polegać jedynie na technikach pseudonimizacji.

Waga konsekwencji dla osób fizycznych

W zależności od charakteru danych osobowych, których dotyczy naruszenie – na przykład szczególnych kategorii danych osobowych – możliwe szkody, których mogą doznać osoby fizyczne, mogą być szczególnie poważne, zwłaszcza w przypadku, gdy w wyniku naruszenia nastąpi kradzież lub sfałszowanie tożsamości, uszkodzenie ciała, cierpienie psychiczne, upokorzenie lub naruszenie dobrego imienia. Jeżeli naruszenie jest związane z danymi osobowymi dotyczącym osób szczególnie narażonych, może to dla nich stwarzać większe ryzyko szkody.

To, czy administrator wie, że dane osobowe znajdują się w rękach osób, których zamiary są nieznane lub które mogą mieć złe intencje, może mieć znaczenie dla poziomu potencjalnego ryzyka. Może nastąpić naruszenie dotyczące poufności danych polegające na omyłkowym

ujawnieniu danych osobowych stronie trzeciej, zgodnie z definicją w art. 4(10), lub innemu odbiorcy. Może to nastąpić na przykład w sytuacji, gdy dane osobowe zostaną przypadkowo wysłane do niewłaściwego działu organizacji lub do organizacji dostawców, z której usług powszechnie się korzysta. Administrator może wezwać odbiorcę do zwrotu albo bezpiecznego zniszczenia otrzymanych danych. W obu przypadkach – z uwagi na fakt, że administrator pozostaje z tymi podmiotami w stałych stosunkach i może znać stosowane przez nie procedury, ich historię i inne istotne szczegóły ich dotyczące – odbiorcę można uznać za „zaufanego". Innymi słowy, administrator może ufać odbiorcy na tyle, aby móc racjonalnie oczekiwać, że strona ta nie odczyta omyłkowo wysłanych danych lub nie uzyska do nich wglądu oraz że wypełni polecenie ich odesłania. Nawet jeżeli do danych uzyskano wgląd, administrator nadal może mieć zaufanie do odbiorcy, że nie podejmie on żadnych dalszych działań w kwestii tych danych oraz że niezwłocznie zwróci dane do administratora i będzie współpracować przy ich odzyskaniu. W takich przypadkach administrator może uwzględnić tę kwestię w ocenie ryzyka przeprowadzanej w następstwie naruszenia – fakt, że odbiorca jest zaufany może spowodować, że skutki naruszenia nie będą poważne, ale nie znaczy to, że naruszenie nie miało miejsca. To z kolei może jednak wyeliminować prawdopodobieństwo wystąpienia ryzyka dla osób fizycznych, w wyniku czego nie będzie już potrzeby powiadomienia organu nadzorczego lub osób fizycznych, na które to naruszenie wywiera wpływ. Również w tym wypadku wszystko będzie zależało od konkretnej sytuacji. Administrator wciąż jednak musi przechowywać informacje dotyczące naruszenia w ramach ogólnego obowiązku prowadzenia dokumentacji na temat naruszeń (...).

Należy również zwrócić uwagę na to, jak trwałe są konsekwencje wobec osób fizycznych, gdyż wpływ może być postrzegany jako poważniejszy, jeżeli dotyczy długiego okresu.

Cechy szczególne danej osoby fizycznej

Naruszenie może mieć wpływ na dane osobowe dotyczące dzieci lub innych osób szczególnie narażonych, w przypadku których w takiej sytuacji może występować większe ryzyko, że znajdą się w niebezpieczeństwie. Z daną osobą fizyczną mogą wiązać się również inne czynniki wpływające na wagę konsekwencji naruszenia, jakie mogą dla niej wyniknąć.

Cechy szczególne administratora danych

Charakter i rola administratora oraz prowadzone przez niego działania mogą mieć wpływ na poziom ryzyka dla osób fizycznych wynikającego z naruszenia. Przykładowo w organizacji medycznej przetwarzane są szczególne kategorie danych osobowych, co oznacza, że w przypadku naruszenia tych danych osobowych osoby fizyczne są narażone na większe zagrożenie niż w przypadku, gdy naruszenie dotyczy listy adresowej czasopisma.

Liczba osób fizycznych, na które naruszenie wywiera wpływ

Naruszenie może dotyczyć tylko jednej osoby, kilku osób lub kilku tysięcy osób – albo dużo większej ich liczby. Zazwyczaj potencjalny wpływ naruszenia wzrasta wraz z liczbą osób, których ono dotyczy. Jednak w zależności od charakteru danych osobowych oraz kontekstu, w którym zostały one ujawnione, naruszenie może mieć poważne konsekwencje nawet dla jednej osoby. Również w tym wypadku najważniejsze jest przeanalizowanie prawdopodobieństwa wystąpienia konsekwencji dla osób, na które naruszenie na wpływ, oraz tego, jak poważne będą te konsekwencje.

Uwagi ogólne

W związku z tym podczas oceny ryzyka, które może powstać w wyniku naruszenia, administrator powinien łącznie uwzględnić wagę potencjalnego wpływu na prawa i wolności osób fizycznych i prawdopodobieństwo jego wystąpienia. Oczywiście ryzyko wzrasta, gdy konsekwencje naruszenia są poważniejsze, jak również wtedy, gdy wzrasta prawdopodobieństwo ich wystąpienia. W przypadku jakichkolwiek wątpliwości administrator powinien zgłosić naruszenie, nawet jeśli taka ostrożność mogłaby się okazać nadmierna. W załączniku B przedstawiono użyteczne przykłady różnych rodzajów naruszeń skutkujących ryzykiem lub wysokim ryzykiem dla osób fizycznych.

Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA) opracowała zalecenia dotyczące metod oceny wagi naruszenia, które mogą się przydać administratorom i podmiotom

przetwarzającym podczas opracowywania planów działania i zarządzania w sytuacji wystąpienia naruszenia[429].

- o – O – o -

Załącznik:

Przykłady naruszeń ochrony danych osobowych i podmiotów, które należy poinformować (z Wytycznych Grupy Roboczej Art. 29)

Przykład	**Czy należy zgłosić naruszenie organowi nadzorczemu?**	**Czy należy zgłosić naruszenie osobie, której dane dotyczą?**	**Uwagi/zalecenia**
i. Administrator przechowywał zaszyfrowaną kopię bezpieczeństwa archiwum danych osobowych na pamięci USB. Pamięć ukradziono podczas włamania.	Nie.	Nie.	Jeżeli dane zostały zaszyfrowane za pomocą najnowocześniejszego algorytmu, utworzono kopie bezpieczeństwa danych, unikalny klucz nie został złamany, a dane można przywrócić w odpowiednim czasie – być może naruszenie to nie podlega zgłoszeniu. Jeżeli jednak w późniejszym czasie klucz zostanie złamany, sytuacja ta będzie wymagała zgłoszenia.
ii. Administrator prowadzi usługę internetową. W wyniku cyberataku na tę usługę nastąpił wyciek danych osób fizycznych. Klienci administratora znajdują się w jednym państwie członkowskim.	Tak, naruszenie należy zgłosić organowi nadzorczemu, jeżeli możliwe są konsekwencje dla osób fizycznych.	Tak, naruszenie należy zgłosić osobom fizycznym w zależności od charakteru danych osobowych, których dotyczy naruszenie, oraz gdy możliwe konsekwencje dla osób fizycznych są poważne.	
iii. Krótkotrwała, kilkuminutowa awaria systemu zasilania w centrum obsługi telefonicznej administratora, w wyniku której klienci nie mogą skontaktować się z administratorem i uzyskać dostępu do swoich danych.	Nie.	Nie.	Naruszenie to nie podlega zgłoszeniu, lecz mimo to należy ten incydent zarejestrować na podstawie art. 33(5). Administrator musi prowadzić odpowiednie rejestry.
iv. Administrator pada ofiarą ataku za pomocą oprogramowania typu	Tak, naruszenie należy zgłosić organowi nadzorczemu, jeżeli	Tak, naruszenie należy zgłosić osobom fizycznym w zależności	Jeżeli istniałaby kopia bezpieczeństwa i możliwe byłoby przywrócenie

[429] ENISA, Zalecenia dotyczące metod oceny wagi naruszeń ochrony danych osobowych: https://www.enisa.europa.eu/publications/dbn-severity [przypis oryginalny]

ransomware, w wyniku którego wszystkie dane zostały zaszyfrowane. Nie są dostępne żadne kopie bezpieczeństwa, a danych nie można przywrócić. W trakcie postępowania okazuje się, że oprogramowanie typu ransomware wykorzystano jedynie do zaszyfrowania danych, a w systemie nie stwierdzono obecności żadnego innego złośliwego oprogramowania.	możliwe są konsekwencje dla osób fizycznych, ponieważ sytuacja ta jest równoznaczna z utratą dostępności.	od charakteru danych osobowych, których dotyczy naruszenie, potencjalnych skutków braku dostępności danych oraz innych możliwych konsekwencji.	danych w odpowiednim czasie, zgłaszanie naruszenia organowi nadzorczemu lub osobom fizycznym nie byłoby konieczne, ponieważ nie miałyby miejsca trwała utrata dostępności lub naruszenie poufności danych. Jeżeli jednak organ nadzorczy dowiedziałby się o tym incydencie z innych źródeł, mógłby rozważyć wszczęcie postępowania do celów oceny zgodności z szerszymi wymogami dotyczącymi bezpieczeństwa określonymi w art. 32.
v. Pewna osoba dzwoni do centrum obsługi telefonicznej banku, by zgłosić naruszenie ochrony danych. Osoba ta otrzymała miesięczny wyciąg bankowy przeznaczony dla kogoś innego. Administrator przeprowadza krótkie postępowanie (tj. trwające do 24 godzin) i ustala z uzasadnioną pewnością, że miało miejsce naruszenie ochrony danych osobowych, i stwierdza, czy w jego systemie występuje wada, która może oznaczać, że naruszenie wpłynęło lub mogło wpłynąć na inne osoby fizyczne.	Tak.	Naruszenie zgłasza się wyłącznie osobom fizycznym, na które naruszenie wywarło wpływ, jeżeli istnieje wysokie ryzyko i jest jasne, że naruszenie nie dotyczy nikogo innego.	Jeżeli w wyniku dalszego postępowania stwierdzono, że naruszenie ma wpływ na większą liczbę osób fizycznych, należy przekazać organowi nadzorczemu aktualne informacje, a administrator wykonuje dodatkową czynność polegającą na zawiadomieniu o naruszeniu innych osób fizycznych, jeżeli sytuacja ta może powodować dla nich wysokie ryzyko.
vi. Administrator prowadzi internetową platformę handlową, a jego klienci znajdują się w wielu państwach członkowskich. Platforma pada ofiarą cyberataku i atakujący publikuje w internecie identyfikatory użytkownika, hasła i historię zakupów.	Tak, naruszenie należy zgłosić wiodącemu organowi nadzorczemu, jeżeli ma miejsce transgraniczne przetwarzanie.	Tak, ponieważ może to doprowadzić do powstania wysokiego ryzyka.	Administrator powinien zareagować, np. wymusić zmianę haseł do kont, których dotyczy naruszenie, jak również poczynić inne kroki w celu zminimalizowania ryzyka. Administrator powinien również wziąć pod uwagę wszelkie inne wymogi zgłaszania naruszeń, np. wynikające z dyrektywy dotyczącej cyberbezpieczeństwa, które

			mają do niego zastosowanie z uwagi na fakt, że jest dostawcą usług cyfrowych.
vii. Przedsiębiorstwo zajmujące się web hostingiem, które pełni rolę podmiotu przetwarzającego, znajduje błąd w kodzie, który kontroluje autoryzację użytkowników. W wyniku tej wady każdy użytkownik może uzyskać wgląd w szczegółowe informacje na temat konta dowolnego innego użytkownika.	Jako podmiot przetwarzający przedsiębiorstwo zajmujące się web hostingiem musi niezwłocznie zgłosić naruszenie swoim klientom, na których wywarło ono wpływ (administratorom). Zakładając, że przedsiębiorstwo zajmujące się web hostingiem przeprowadziło swoje własne postępowanie, administratorzy, na których naruszenie wywarło wpływ, powinni mieć wystarczającą pewność co do tego, czy padli ofiarą naruszenia, a tym samym tego, czy można uznać, że „stwierdzili naruszenie" po zgłoszeniu naruszenia przez przedsiębiorstwo zajmujące się web hostingiem (podmiot przetwarzający). Administrator musi następnie zgłosić naruszenie organowi nadzorczemu.	Jeżeli prawdopodobieństwo istnienia wysokiego ryzyka dla osób fizycznych jest niewielkie, nie ma potrzeby ich powiadomienia.	Przedsiębiorstwo zajmujące się web hostingiem (podmiot przetwarzający) musi również uwzględnić wszelkie inne obowiązki zgłaszania naruszeń (np. wynikające z dyrektywy dotyczącej cyberbezpieczeństwa – z uwagi na fakt, że jest dostawcą usług cyfrowych). Jeżeli nic nie wskazuje na to, że tę lukę w zabezpieczeniach wykorzystano przeciwko jakiemukolwiek administratorowi, naruszenie mogło nie podlegać zgłoszeniu, lecz prawdopodobnie należy je udokumentować lub jest związane z nieprzestrzeganiem art. 32.
viii. Szpitalna dokumentacja medyczna jest niedostępna przez 30 godzin w wyniku cyberataku.	Tak, szpital ma obowiązek zgłoszenia naruszenia, ponieważ może powstać wysokie ryzyko dla dobrostanu i prywatności pacjentów.	Tak, naruszenie należy zgłosić osobom fizycznym, na które wywiera ono wpływ.	
ix. Dane osobowe znacznej liczby studentów omyłkowo wysłano do niewłaściwej listy adresowej, na której znajduje się ponad 1000 odbiorców.	Tak, naruszenie należy zgłosić organowi nadzorczemu.	Tak, naruszenie należy zgłosić osobom fizycznym w zależności od zakresu i rodzaju ujawnionych danych osobowych i wagi możliwych konsekwencji.	
x. Wiadomość e-mail w ramach marketingu bezpośredniego wysłano do odbiorców	Tak, zgłoszenie naruszenia organowi nadzorczemu może być obowiązkowe, jeżeli	Tak, naruszenie należy zgłosić osobom fizycznym w zależności od zakresu i rodzaju	Zgłoszenie może nie być konieczne, jeżeli nie ujawniono żadnych danych wrażliwych i jeżeli

w polach „do:” lub „dw:”, tym samym umożliwiając każdemu odbiorcy wgląd w adresy e-mail innych odbiorców.	naruszenie dotyczy dużej liczby osób, jeżeli ujawniono dane wrażliwe (takie jak np. lista adresowa psychoterapeuty) lub jeżeli inne czynniki stwarzają wysokie ryzyko (np. wiadomość e-mail zawiera hasła startowe).	ujawnionych danych osobowych i wagi możliwych konsekwencji.	ujawniono tylko niewielką liczbę adresów e-mail.

- o – O – o -

ZADANIE 7: Zadanie dochodzeniowe (z uwzględnieniem obsługi skarg wewnętrznych i zewnętrznych)

Uwaga: Zadanie to jest niezależne i odmienne od obsługi składanych przez osoby, których dane dotyczą, wniosków o udzielenie dostępu, skorygowanie, itp., o których mowa w Zadaniu 8.

Dochodzenie

Chociaż nie zostało to wyraźnie wspomniane w RODO, z szerokiego opisu ogólnego stanowiska i ogólnych zadań inspektora ochrony danych oraz w szczególności ze spoczywającego na nim zadania „monitorowania przestrzegania" RODO: art. 39(1)(b) – wynika, że inspektor ochrony danych może z własnej inicjatywy lub na wniosek kierownictwa albo na przykład organu przedstawicielskiego pracowników lub związków zawodowych lub jakiejkolwiek osoby (z organizacją lub spoza niej lub nawet osoby informującej o nieprawidłowościach, która powinna być w danym kraju chroniona) **badać** sprawy i okoliczności bezpośrednio związane z jego zadaniami oraz **zgłaszać** je osobie lub organowi, któremu zlecono lub nakazano dochodzenie, i/lub najwyższemu kierownictwu. Jak ujmuje to Europejski Inspektor Ochrony Danych w swoim stanowisku na temat inspektorów ochrony danych[430]:

> **Monitorowanie przestrzegania** (...): inspektor ochrony danych ma zapewnić stosowanie Rozporządzenia w ramach instytucji. Inspektor ochrony danych może z własnej inicjatywy lub na wniosek instytucji albo organu, administratora, komitetu pracowniczego lub jakiejkolwiek osoby zbadać sprawy i okoliczności bezpośrednio związane z jego zadaniami oraz zgłaszać je osobie, której dochodzenie dotyczy, lub administratorowi.

RODO wyjaśnia - aczkolwiek w mniej wyraźnych słowach niż uczyniono to w załączniku do rozporządzenia o ochronie danych w instytucjach UE - że inspektorzy ochrony danych muszą otrzymać **wszelkie odpowiednie zasoby oraz dostęp do wszystkich danych osobowych i biur, urządzeń przetwarzających dane i nośników danych** (wraz z odpowiednimi i koniecznymi uprawnieniami do ***uwierzytelniania, dostępu do rejestru i zatrzymania danych***), jakie są niezbędne do realizacji powierzonych im zadań (zob. art. 38(2)), tj. także w związku z tego typu dochodzeniem[431]. Podobnie, chociaż zostało to ponownie wyraźniej stwierdzone w odniesieniu do inspektorów ochrony danych w instytucjach UE niż inspektorów ochrony danych wyznaczonych na podstawie RODO, **wszyscy odpowiedni pracownicy administratora oraz w rzeczywistości wszyscy pracownicy agencji zewnętrznych, z uwzględnieniem w szczególności podmiotów przetwarzających (w tym dostawców usług w chmurze dla administratora), powinni udzielić inspektorowi w ramach tego typu dochodzenia pełnego wsparcia** oraz ***pełnych odpowiedzi i informacji*** w odpowiedzi na zapytania lub wnioski inspektora[432]. **Administratorzy powinni jasno to wyjaśnić w wewnętrznych wytycznych dla pracowników oraz uwzględnić w tym zakresie jasne klauzule w swoich umowach z zewnętrznymi dostawcami i podmiotami przetwarzającymi.**

Egzekwowanie

Pomimo kompetencji do monitorowania przestrzegania RODO, obsługi skarg i badania ewentualnych naruszeń rozporządzenia, **inspektor ochrony danych ma ograniczone uprawnienia do egzekwowania.** Z zasady, jak zauważono powyżej, jeżeli inspektor ochrony danych uzna, że RODO zostało w pewnym względzie naruszone przez jego organizację albo przez zewnętrznego dostawcę lub podmiot przetwarzający, inspektor powinien zgłosić ten fakt najwyższemu kierownictwu, i to najwyższe kierownictwo jest odpowiedzialne za podjęcie działań korygujących, z uwzględnieniem w stosownym przypadku sankcji wobec pracowników, agentów lub podmiotów przetwarzających, które nie wypełniły swoich obowiązków, np. poprzez wydanie ostrzeżenia lub nałożenie innych kar albo w wyjątkowych okolicznościach zwolnienie lub rozwiązanie umowy. Na przykład, jeżeli za gromadzenie danych odpowiada zewnętrzny usługodawca (np. poprzez obsługiwane przez niego zautomatyzowane systemy)

---

[430] EDPS, Position paper on the role of Data Protection Officers in ensuring effective compliance with Regulation (EC) 45/2001, (przypis 243 powyżej), str. 6-7 (pogrubienie zgodnie z oryginałem).

[431] Załącznik do Rozporządzenia (UE) 45/2001 przewiduje, że inspektorzy ochrony danych w instytucjach UE: „*nieustanny dostęp do danych będących przedmiotem operacji przetwarzania, a także wszystkich biur, urządzeń przetwarzających dane i nośników danych*" (*załącznik*, art. 4, drugie zdanie).

[432] Załącznik do Rozporządzenia (UE) 45/2001 przewiduje, że: „*Każdy właściwy administrator ma wspomagać inspektora ochrony danych w wykonywaniu jego obowiązków i udzielić informacji w odpowiedzi na pytania*." (*Załącznik*, art. 4, pierwsze zdanie).

i taki usługodawca nie przestrzega RODO, np. jeżeli chodzi o powiadomienia lub, co gorsza, wykorzystywanie zgromadzonych danych ukradkiem w innych (niezadeklarowanych) celach, inspektor ochrony danych powinien zaproponować, by administrator skorzystał z usług innego podmiotu, oraz jednocześnie powiadomić organ ochrony danych.

Niepodjęcie tego typu działań będzie działało na niekorzyść inspektora (organizacji) w przypadku wszczęcia przez krajowy organ ochrony danych postępowania egzekucyjnego zmierzającego do ustalenia możliwej do nałożenia „administracyjnej kary pieniężnej" (zob. art. 83).

Ponadto jednym z zadań inspektora ochrony danych jest skonsultowanie się z właściwym organem ochrony danych „w stosownym przypadkach" w każdej ewentualnej sprawie (art. 39(1)(e). W przypadku poważnej różnicy poglądów pomiędzy inspektorem ochrony danych a najwyższym kierownictwem jego organizacji, gdy zdaniem inspektora danych konkretna operacja przetwarzania narusza lub (poważnie) naruszy RODO i/lub stosowne przepisy krajowe, a kierownictwo chce taką operację wykonać lub nie zamierza podjąć wobec niej żadnych sankcji, oczywiście odpowiednim rozwiązaniem dla inspektora ochrony danych wydawałoby się skorzystanie z takiego uprawnienia i (skuteczne) przekazanie sprawy do organu ochrony danych. To organ ochrony danych zdecyduje o skorzystaniu z przysługujących mu silnych uprawnień dochodzeniowych i egzekucyjnych, z uwzględnieniem możliwości nakazania niewdrażania lub zaprzestania operacji, w zależności od tego, co uzna za stosowne (zob. art. 58(2)(d) i (f) w szczególności).

Zob. poniżej: punkty zatytułowane „*Współpraca i konsultacje z organem ochrony danych"* i „*Obsługa zapytań i skarg*".

- o – O – o -

Zadania doradcze

ZADANIE 8: Zadanie doradcze - informacje ogólne

Inspektor ochrony danych musi zapewnić przestrzeganie Rozporządzenia oraz doradzać, by inspektorzy wypełniali swoje obowiązki. Inspektor ochrony danych może więc **informować,** udzielać **porad** lub wydawać **rekomendacje** dla celów ***praktycznych usprawnień*** w ochronie danych przez organizację i/lub spraw dotyczących stosowania przepisów o ochronie danych (tj. RODO i innych unijnych przepisów w tym zakresie, takich jak na chwilę obecna Dyrektywa o e-prywatności z 2002 roku i w przyszłości ewentualne Rozporządzenie o e-prywatności oraz przepisy krajowe oparte na „określonych klauzulach" RODO lub mające zastosowanie na innej podstawie), a także dla celów ***zmiany i aktualizacji polityk i praktyk organizacji dotyczących ochrony danych*** w świetle nowych instrumentów prawnych, decyzji, rozwiązań lub wytycznych (zob. art. 39(1)(a)).

W tym celu inspektor ochrony danych powinien być w stanie **dokładnie monitorować zmiany legislacyjne i regulacyjne w obszarze ochrony danych, bezpieczeństwa danych, itp.**, by alarmować kierownictwo wyższego i odpowiedniego niższego szczebla o nadchodzących ***nowych instrumentach UE*** (takich jak wyżej wspomniane Rozporządzenie o e-prywatności) lub nowych ***decyzjach wykonawczych i sądowych podjętych na szczeblu UE*** (takich jak odpowiednie nowe decyzje stwierdzające odpowiedni poziom ochrony, podjęte przez Komisję Europejską i dotyczące krajów trzecich, do których organizacja inspektora przekazuje dane, albo odpowiednie wyroki Trybunału Sprawiedliwości UE), ***nowych wytycznych przyjętych na szczeblu UE*** (w szczególności opiniach lub rekomendacjach, itp. wydanych przez ***Europejską Radę Ochrony Danych***) oraz **o *podobnych instrumentach, decyzjach, rozwiązaniach lub wytycznych wydanych w kraju inspektora ochrony danych*** (lub krajach) siedziby. RODO faktycznie **wymaga,** by każdy administrator wspólnie z inspektorem ochrony danych zapewnili „[***wszelkie] zasoby niezbędne*** *do wykonania tych zadań ... oraz* ***utrzymania jego wiedzy fachowej***" (art. 38(2)). Inspektor ochrony danych powinien więc mieć możliwość uczestniczenia (oraz należy go zachęcać do uczestnictwa) w odpowiednich seminariach, konferencjach i spotkaniach, w szczególności organizowanych przez krajowy lub regionalny państwowy organ (lub organy) ochrony danych.

Z inspektorem ochrony danych **konsultować mogą się także** (a właściwie z zasady w odpowiednich sprawach **muszą się konsultować**) przedstawiciele kierownictwa, organ przedstawicielski pracowników lub związki zawodowe albo każdy pracownik, z uwzględnieniem oczywiście i w szczególności „właścicieli"/osób w ramach organizacji, na których spoczywa szczególna odpowiedzialność za konkretną operację przetwarzania, za każdym razem, gdy dana osoba wnioskuje o poradę (zob. także Zadanie 7 poniżej).

Jak ujmuje to Grupa Robocza Art. 29 w swoich Wytycznych dotyczących inspektorów ochrony danych (formalnie zatwierdzonych przez Europejską Radę Ochrony Danych)[433]:

> W związku z tym organizacja powinna zapewnić między innymi:
>
> - udział inspektora ochrony danych w spotkaniach przedstawicieli wyższego i średniego szczebla organizacji;
> - uczestnictwo inspektora ochrony danych przy podejmowaniu decyzji dotyczących przetwarzania danych osobowych. Niezbędne informacje powinny zostać udostępnione inspektorowi odpowiednio wcześniej, umożliwiając mu zajęcie stanowiska;
> - stanowisko inspektora ochrony danych powinno być zawsze brane pod uwagę. W razie braku porozumienia Grupa Robocza Art. 29 zaleca, w ramach dobrych praktyk, dokumentowanie przypadków i powodów postępowania niezgodnego z zaleceniem inspektora;
> - w przypadku stwierdzenia naruszenia albo innego zdarzenia związanego z danymi osobowymi należy natychmiast skonsultować się z inspektorem ochrony danych.
>
> W określonych przypadkach administrator lub podmiot przetwarzający powinni stworzyć wytyczne ochrony danych osobowych, które wskazywałyby przypadki wymagające konsultacji z inspektorem ochrony danych.

[433] Wytyczne Grupy Roboczej Art. 29 dotyczące oceny skutków dla ochrony danych (przypis 242 powyżej), str. 13-14.

ZADANIE 9: Wspieranie i promowanie „Ochrony danych w fazie projektowania oraz jako opcji domyślnej"

Jak zauważono w dyskusji w ramach Zadania 6, z inspektorem ochrony danych należy z zasady konsultować wszelkie sprawy dotyczące ochrony danych w ramach organizacji, z uwzględnieniem opracowania ogólnych wytycznych, itp.

Jednak jest jedna sprawa o szczególnym znaczeniu. To nowy jednoznaczny wymóg RODO (nie uwzględniony jeszcze w Dyrektywie o ochronie danych z 1995 roku, chociaż można było go już tam wyczytać)[434], aby administratorzy uwzględnili zasadę „**ochrony danych w fazie projektowania i jako opcji domyślnej**" (co obejmuje zasadę „***bezpieczeństwa na etapie projektowania [i jako opcji domyślnej]***")[435] we wszystkich swoich operacjach. Jak ujęto to w art. 25:

> Artykuł 25
>
> **Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych**
>
> 1. 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 niniejszego rozporządzenia oraz chronić prawa osób, których dane dotyczą.
> 2. 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.
> 3. … [436]

Tutaj możemy jedynie w skrócie omówić tą zasadę. Europejski Inspektor Ochrony Danych podsumowuje **ogólną koncepcję i jej podstawy** następująco[437]:

> Zwrot „prywatność w fazie projektowania" został pierwotnie przyjęty przez Ann Cavoukian, gdy została ona Komisarzem ds. Informacji i Prywatności w Ontario w Kanadzie. Zgodnie z jej koncepcją prywatność w fazie projektowania można podzielić na „**7 fundamentalnych zasad**"[438], podkreślających potrzebę **aktywności** przy rozpatrywaniu wymogów [lub zgodnie z przepisami UE - ochrony danych] prywatności, począwszy od fazy projektowania przez cały cykl życia danych, które należy *„uwzględnić w projekcie i architekturze systemów informatycznych oraz praktyk biznesowych ... bez uszczerbku dla funkcjonalności ..."*, z uwzględnieniem prywatności jako podstawowego ustawienia, kompleksowego bezpieczeństwa, w tym bezpiecznego niszczenia

[434] Zob. np. powtórzone odwołanie do tej zasady w Opinii Grupy Roboczej Art. 29 nr 8/2014 w sprawie ostatnich postępów w dziedzinie internetu rzeczy (Opinion 8/2014 on the on Recent Developments on the Internet of Things) (WP223), przyjętej 16 września 2014 r. http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

[435] Zob. WP223 (poprzedni przypis), str. 22, przedostatni podpunkt.

[436] Trzeci paragraf przewiduje, że *„Wywiązywanie się z obowiązków, o których mowa w ust. 1 i 2 niniejszego artykułu, można wykazać między innymi poprzez wprowadzenie zatwierdzonego mechanizmu certyfikacji określonego w art. 42."* Zostało to przedyskutowane w związku z Zadaniem 9.

[437] Europejski Inspektor Ochrony Danych (EDPS), Wstępna opinia na temat prywatności w fazie projektowania (Preliminary Opinion on privacy by design) (Opinia 5/2018), wydana 31 maja 2018 r. str. 4, par. 17 (oryginalny zapis pochyłą czcionką), https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf (dodano podkreślenie). Należy zauważyć, że Europejski Inspektor Ochrony Danych wyróżnia szerszą zasadę „prywatności w fazie projektowania", która ma „wymiar wizjonerski i etyczny", od bardziej konkretnych wymogów prawnych „ochrona danych w fazie projektowania" i „domyślna ochrona danych", przewidzianych w art. 25 RODO (pkt 1.4) .

[438] Zob. https://www.ipc.on.ca/wp-content/uploads/2018/01/pbd.pdf. Zobacz „siedem fundamentalnych zasad": 1. Działanie proaktywne zamiast reakcyjnego i prewencyjne zamiast naprawczego; 2. Prywatność jako ustawienie domyślne; prywatność wbudowana w projekt; 4. Pełna funkcjonalność - Suma dodatnia, brak sumy zerowej; 5. Bezpieczeństwo od początku do końca - Ochrona w całym cyklu przetwarzania; 6 Widoczność i przejrzystość - Jawność; 7. Poszanowanie prywatności użytkownika - Użytkownik w centrum zainteresowań. [przypis oryginalny] http://www.ipc.on.ca/wp-content/uploads/2018/01/pbd.pdf.

> danych oraz silnej przejrzystości będącej przedmiotem niezależnej weryfikacji. Zasada domyślnej prywatności została wymieniona jako druga z fundamentalnych zasad przy założeniu że domyślna prywatność obejmuje *„zapewnienie automatycznej ochrony danych osobowych w każdym systemie informatycznym i każdej praktyce biznesowej. Jeżeli jednostka nie podejmuje żadnych działań, jej prywatność w dalszym ciągu pozostaje nietknięta. Jednostka nie musi podejmować żadnych działań, by chronić swoją prywatność - **jest to domyślnie wbudowane w system**".* Stwierdzenie to stanowi mocną definicję operacyjną zasady domyślnej prywatności, gdy jednostka nie ponosi ciężaru dążenia do ochrony w trakcie korzystania z usługi lub produktu, ale „automatycznie" korzysta (bez potrzeby aktywnego działania) z fundamentalnego prawa do prywatności i ochrony danych osobowych.

Zdaniem Europejskiego Inspektora Ochrony Danych „ochrona danych w fazie projektowania" **ma kilka wymiarów**, parafrazując[439]:

- **pierwszy wymiar -** operacje przetwarzania danych osobowych powinny być zawsze ***wynikiem projektu*** obejmującego ***cały cykl życia projektu,*** w ramach którego należy jasno ustalić ryzyko naruszenia oraz wymogi dotyczące ochrony danych;
- **drugi wymiar -** projekt powinien być oparty na ***zarządzaniu ryzykiem,*** w ramach którego aktywami, które należy chronić, są ***jednostki, których dane mają być przetwarzane, oraz w szczególności ich podstawowe prawa i wolności;***
- **trzeci wymiar** - środki, jakie należy podjąć, by chronić takie jednostki oraz prawa i wolności, muszą być ***odpowiednie i skuteczne*** w odniesieniu do ustalonego ryzyka w świetle zasad ochrony danych określonych w art. 5 RODO, które mogą być postrzegane jako ***cele do osiągnięcia***;
- **czwarty wymiar** - obowiązek ***zintegrowania ustalonych [niezbędnych, stosownych i skutecznych] zabezpieczeń z przetwarzaniem.***

Dodaje on także, że[440]:

> **Wszystkie cztery wymiary są jednakowo ważne i stają się integralną częścią zasady rozliczalności** oraz - tam, gdzie to stosowne - podlegają nadzorowi ze strony właściwych organów nadzorczych.

Europejski Inspektor Ochrony Danych podkreśla znaczenie ochrony danych w fazie projektowania oraz domyślnej ochrony danych w odniesieniu do różnych uczestników procesu: administratorów i podmiotów przetwarzających w ogóle[441], twórców produktów i technologii (wrażliwych na kwestie prywatności)[442], usługi łączności elektronicznej[443], usługi tożsamości elektronicznej[444], dostawców „inteligentnych" liczników i sieci[445]. W odniesieniu do **administracji publicznych** Europejski Inspektor Ochrony Danych podkreśla, że[446]:

> Artykuł 25 ma zastosowanie do wszystkich rodzajów organizacji działających jako administratorzy, z uwzględnieniem **administracji publicznych**, które, biorąc pod uwagę ich rolę służenia dobru publicznemu, **powinny dawać przykład w procesie ochrony podstawowych praw i wolności jednostek.** W motywie 78 RODO podkreśla rolę ochrony danych w fazie projektowania oraz domyślnej ochrony danych, gdy administracje publiczne muszą ustalić swoich dostawców produktów i usług, stwierdzając, że *„**Zasadę uwzględniania ochrony danych w fazie projektowania i zasadę domyślnej ochrony danych należy też brać pod uwagę w przetargach publicznych**"*. **Administracja publiczna znajduje się na pierwszej linii, jeżeli chodzi o stosowanie tych zasad w odpowiedzialny sposób, z możliwością** w razie potrzeby **wykazania ich wdrożenia** właściwemu organowi nadzorczemu.

---

[439] Szczegóły dotyczące tych wymiarów zdaniem EDPS - patrz: Opinia wstępna 5/2018 (przypis 437 powyżej), str. 6 – 7 (par. 27 – 32).
[440] *Idem*, str. 7, par. 32, pogrubiona czcionka dodana przez autorów Podręcznika.
[441] *Idem*, str. 7. par. 35 – 36.
[442] *Idem*, str. 7. par. 37.
[443] *Idem*, str. 8 – 9, par. 42 – 44 (z odwołaniem do Dyrektywy o e-prywatności oraz proponowanego Rozporządzenia o e-prywatności).
[444] *Idem*, str. 9. par. 45 (z odwołaniem do Rozporządzenia eIDAS).
[445] *Idem*, str. 9 – 10, par. 46 – 50 (z odwołaniem do Rekomendacji o szablonie oceny skutków dla ochrony danych).
[446] *Idem*, str. 8, par. 38, pochyła czcionka zgodnie z oryginałem, pogrubiona czcionka dodana przez autorów Podręcznika.

Odwołanie do **przetargów publicznych** jest szczególnie istotne. Inspektorzy ochrony danych powinni ***doradzać*** swoim organizacjom, że otwierając tego typu przetargi, administracje publiczne powinny wyraźnie wezwać do składania ofert przez oferentów, którzy mogą „wykazać", że ich produkty lub usługi są w pełni zgodne z RODO (oraz innymi właściwymi unijnymi i krajowymi przepisami o ochronie danych)[447] oraz że wprowadzili „ochronę danych w fazie projektowania i domyślną ochronę danych" w odpowiednich produktach lub usługach. Faktycznie tacy oferenci powinni uzyskać ***przewagę konkurencyjną*** nad oferentami, których produkty lub usługi nie potwierdzają spełnienia powyższych wymogów[448].

Europejski Inspektor Ochrony Danych omawia dość obszernie różne **metodologie**, jakie opracowano w celu wdrożenia ochrony danych w fazie projektowania oraz domyślnej ochrony danych[449]. Nie możemy ich tutaj opisać w całości lub nawet sparafrazować, ale inspektorzy ochrony danych powinni zapoznać się z nimi wszystkimi (nawet bardziej szczegółowo, niż przewiduje to dokument EDPS). Wystarczy zauważyć, że **Europejski Inspektor Ochrony Danych poprawnie łączy prywatność w fazie projektowania i domyślną prywatność z oceną skutków dla ochrony danych**, co zostało omówione w Zadaniu 7 [450] oraz wyraźnie podkreśla, że[451]:

> **Rola prywatności i inspektorów ochrony danych ma centralne znaczenie, zaś ich zaangażowanie stanowi podstawę podejścia do prywatności w fazie projektowania.** Na pierwszych etapach, gdy organizacje planują swoje systemy przetwarzania danych, inspektorzy muszą być na bieżąco, aby mogli w razie potrzeby wspierać kierowników, właścicieli oraz departamenty informatyczne i technologiczne. Ich umiejętności powinny spełniać tego typu wymagania.

Umiejętności takie obejmują **pełne wykształcenie i przeszkolenie w zakresie odpowiednich metodologii** i technologii (w razie potrzeby w ramach dodatkowego szkolenia stanowiskowego) oraz **głębokie zaangażowanie w projektowanie, opracowanie, testowanie i dostosowywania wszystkich produktów, usług i działań organizacji, które są wrażliwe z punktu widzenia prywatności** (z uwzględnieniem przetargów) na każdym z etapów procesu.

- o – O – o -

[447] Zob. dyskusja na temat zasady „rozliczalności" w części drugiej, pkt 2.4.
[448] Podejście takie zostało wyraźnie przyjęte w ustawie o ochronie danych Schleswig-Holstein.
[449] Europejski Inspektor Ochrony Danych, Wstępna opinia 5/2018 (przypis 437 powyżej), str. 13 – 15, par. 63 – 72. Zob. także odpowiednie odwołania do amerykańskiego programu „NIST privacy engineering program" oraz raportu NIST „Report on privacy engineering and risk management for U.S. federal systems" (str. 11, par. 56, przypisy 76 i 74) i „EU ENISA 2014 analysis of the (then) state of the art" (str. 12 par. 59, przypis 82).
[450] *Idem*, str. 8. par. 39 – 40.
[451] *Idem*, str. 15, par. 76, pogrubiona czcionka dodana przez autorów Podręcznika.

ZADANIE 10: Doradzanie w sprawie zgodności oraz monitorowanie zgodności z politykami ochrony danych, postanowieniami umów pomiędzy współadministratorem a podmiotem przetwarzającym, dwoma administratorami a podmiotem przetwarzającym i administratorem a podmiotem przetwarzającym, Wiążącymi regułami korporacyjnymi i klauzulami o przekazywaniu danych

Aby przestrzegać postanowień RODO, a w szczególności, by to „wykazać", administratorzy mogą i powinni przyjąć lub podpisać szereg środków i instrumentów. Jak zauważono w pkt. 2.2.2, środki takie obejmują:

- sporządzanie i formalne przyjmowanie wewnętrznych **polityk ochrony danych** (zob: art. 24(2)) w celu uregulowania takich spraw, jak:
  - ✓ stosowane przez organizację **papierowe formularze, formularze internetowe** oraz **oświadczenia o ochronie danych/prywatności na stronach internetowych,** korzystanie z **cookies** i innych plików śledzących;
  - ✓ **dostęp i zmiana rejestrów,** itp. w odpowiednim oprogramowaniu i sprzęcie;
  - ✓ wydawanie **„łat"** dla swojego własnego oprogramowania;
  - ✓ itp.
- zawieranie **umów administracyjnych** („**uzgodnień**") pomiędzy organami lub podmiotami publicznymi, w szczególności jeżeli pełnią one funkcję „**współadministratorów**" w stosunku do określonych operacji przetwarzania;
- sporządzanie i uzgadnianie odpowiednich **umów z innymi administratorami i podmiotami przetwarzającymi** oraz
- **podpisywanie** lub sporządzanie **standardowych lub indywidualnie zatwierdzanych umów o przekazie danych.**

Głównym punktem, który należy tutaj podkreślić, jest to, że wszystkie wymienione funkcje to zadania (środki umożliwiające „wykazanie przestrzegania") administratora a nie inspektora ochrony danych (patrz punkt zatytułowany *„Brak odpowiedzialności inspektora ochrony danych za przestrzeganie RODO"* w części drugiej, pkt 2.5.4).

Jednak w praktyce inspektor ochrony danych powinien zostać mocno zaangażowany we wszystkie tego typu sprawy. A przynajmniej nowy inspektor ochrony danych, w szczególności inspektor mianowany dla organizacji, w której poprzednio takiego stanowiska nie było, powinien **dokonać przeglądu** wszystkich tego rodzaju istniejących dokumentów i instrumentów, by sprawdzić, czy w dalszym ciągu w pełni spełniają one wszystkie wymogi prawne dotyczące ochrony danych.

Na podstawie takiego przeglądu inspektor powinien **zalecić zmiany w istniejących dokumentach, itp.**, w szczególności jeżeli sporządzono i przyjęto je przed przyjęciem i wejściem w życie RODO oraz powinien **zalecić sporządzenie i przyjęcie takich dokumentów**, jeżeli (jego zdaniem) powinny one zostać przyjęte, ale do tej pory tego nie uczyniono.

Inspektor ochrony danych jest formalnie odpowiedzialny za **monitorowanie** przestrzegania polityk, ustaleń i umów przyjętych lub zawartych przez administratora w związku z przetwarzaniem danych osobowych (art. 39(1)(b)).

ZADANIE 11: Udział w tworzeniu kodeksów postępowania i w procesie certyfikacji

W części drugiej, w pkt. 2.2.2, zauważyliśmy, że przestrzeganie i zapewnienie pełnej zgodności z zatwierdzonym **kodeksem postępowania** lub **zatwierdzonym certyfikatem ochrony danych** może także stanowić istotny element lub środek umożliwiający wykazanie zgodności z RODO w związku ze sprawami uwzględnionymi w takim kodeksie lub certyfikacie (bez tego stanowiący prawny dowód zgodności).

To od administratora, a nie od inspektora ochrony danych, zależy decyzja o przystąpieniu do odpowiedniego kodeksu dla sektora, w którym organizacja działa, lub uzyskaniu certyfikatu ochrony

danych w formie przewidzianej w Rozporządzeniu (art. 40 – 43). Jednak inspektor ochrony danych ma w pełni prawo **zarekomendować** takie działania.

W rzeczywistości inspektorzy ochrony danych w organizacjach działających w określonym sektorze powinni wręcz uczestniczyć w **opracowaniu kodeksu postępowania** dla sektora, chociaż w proces ten należy także zaangażować radcę prawnego i pracowników organizacji sektorowych, pod których nadzorem kodeks jest opracowywany (z uwzględnieniem w szczególności pracowników działów teleinformatycznych, jeżeli kodeks porusza kwestie techniczne, takie jak bezpieczeństwo teleinformatyczne, szyfrowanie, itp.).

Inspektor ochrony danych może także **wspierać proces uzyskania certyfikatu** przez jego organizację poprzez pomaganie w zgromadzeniu lub zapewnieniu organowi certyfikacyjnemu „wszelkich informacji i wszelkiego dostępu do swoich czynności przetwarzania, które to informacje i dostęp są niezbędne do przeprowadzenia procedury certyfikacji" (art. 42(6)). Jednak, jeżeli program certyfikacji jest oparty na **ocenie** operacji przetwarzania danych osobowych administratora przez jednego lub więcej ***niezależnych ekspertów*** akredytowanych przez właściwy organ certyfikujący (jak ma to miejsce w przypadku głównego programu w UE, *European Privacy Seal [EuroPriSe]*)[452], inspektor ochrony danych nie może pełnić takiej roli, gdyż prowadziłoby to do konfliktu interesów.

Uwaga: W pewnym zakresie szczegółowy rejestr oceny skutków dla ochrony danych, który omówiono w Zadaniu 4 i ciągłe monitorowanie operacji, przedyskutowane w Zadaniu 5 (oraz rejestry tego ciągłego monitorowania), spełniają podobną funkcję do certyfikatów, ponieważ rejestry potwierdzają, że administrator i jego pracownicy starannie przyjrzeli się wszystkim implikacjom odpowiednich operacji przetwarzania danych osobowych dla ochrony danych, ustalili i obliczyli ryzyko naruszenia podstawowych praw jednostek oraz przyjęli odpowiednie środki łagodzące. Przewaga certyfikatów nad taką oceną polega na tym, że za certyfikację odpowiadają niezależni eksperci zewnętrzni. Jednak w znacznej mierze będzie to zależeć od jakości akredytowanych programów certyfikacyjnych i tego, w jaki sposób będą one powiązane z egzekwowaniem przez organy ochrony danych.

- o – O – o -

[452] Zob. https://www.european-privacy-seal.eu/EPS-en/fact-sheet.

Współpraca i konsultacje z organem ochrony danych

ZADANIE 12: Współpraca z organem ochrony danych

Inspektor ochrony danych ma za zadanie odpowiadać na wnioski organu ochrony danych oraz w ramach swoich kompetencji współpracować z nim na jego wniosek lub z własnej inicjatywy (art. 39(1)(d)).

W tym względzie Grupa Robocza Art. 29 stwierdza, że[453]:

> Zadania te odnoszą się do pomocniczej roli inspektora ochrony danych, wspomnianej we wstępie do tych Wytycznych. Inspektor ochrony danych ma pełnić funkcję punktu kontaktowego, aby umożliwić organowi nadzorczemu dostęp do dokumentów i informacji w celu realizacji zadań, o których mowa w art. 57, jak również wykonywania uprawnień w zakresie prowadzonych postępowań, uprawnień naprawczych, uprawnień w zakresie wydawania zezwoleń oraz uprawnień doradczych, zgodnie z art. 58. Jak już wspomniano, inspektor ochrony danych związany jest tajemnicą i poufnością dotyczącą wykonywania zadań inspektora, zgodnie z prawem Unii lub prawem państwa członkowskiego (art. 38(5)). Zakaz ten nie wyłącza możliwości kontaktowania się inspektora ochrony danych w celu uzyskania porady ze strony organu nadzorczego. Artykuł 39(1)(e) stanowi, że inspektor ochrony danych może konsultować się z organem nadzorczym we wszystkich sprawach, w stosownych przypadkach.

Europejski Inspektor Ochrony Danych dodatkowo w przydatny sposób uzupełnił zadania inspektorów ochrony danych w instytucjach UE w ich relacjach z EDPS, co zostało określone w poniższych cytatach, z uwzględnieniem zmian w tekście, by móc zastosować słowa EDPS *mutatis mutandis* do relacji pomiędzy organami ochrony danych państw członkowskich (i EDPB) a wyznaczonymi na mocy RODO inspektorami ochrony danych. Europejski Inspektor Ochrony Danych zauważa po pierwsze, że[454]:

> Inspektor ochrony danych ma za zadanie odpowiadać na wnioski [odpowiedniego organu ochrony danych] oraz w ramach swoich kompetencji współpracować z nim na jego wniosek lub z własnej inicjatywy. Zadanie to podkreśla fakt, że inspektor ochrony danych ułatwia współpracę pomiędzy [organem ochrony danych] a instytucją w szczególności w ramach postępowania dochodzeniowego, rozpatrywania skarg lub wstępnych kontroli. Inspektor ochrony danych nie tylko zna instytucję od wewnątrz, ale także prawdopodobnie wie, kto jest najlepszą osobą do kontaktu w tej instytucji. Inspektor ochrony danych może także znać ostatnie zmiany mogące mieć wpływ na ochronę danych osobowych oraz należycie o nich poinformować [organ ochrony danych].

Europejski Inspektor Ochrony Danych następnie rozwija to w odniesieniu do różnych wspomnianych spraw, które mają w znacznej mierze zastosowanie także do kwestii wynikających z RODO[455]:

> **IV. Relacja pomiędzy inspektorem ochrony danych a [organem ochrony danych]**
>
> Na zapewnienie zgodności z Rozporządzeniem wpływać będzie relacja robocza pomiędzy inspektorem ochrony danych a [odpowiednim organem ochrony danych]. Nie wolno postrzegać inspektora ochrony danych jako agenta organu ochrony danych, gdyż jest on członkiem instytucji/podmiotu, z którym współpracuje. Jak już wspomniano, tego typu bliskość stawia go w doskonałej sytuacji umożliwiającej mu zapewnienie zgodności z przepisami z wnętrza organizacji oraz doradzanie lub ingerowanie na wczesnym etapie, by uniknąć ewentualnej interwencji ze strony organu nadzorczego. Jednocześnie [organ ochrony danych] może zaoferować inspektorom cenne wsparcie w realizacji spoczywających na nich funkcji[456].
>
> W związku z powyższym [od organów ochrony danych można oczekiwać][457] wsparcia dla idei rozwoju możliwej synergii pomiędzy inspektorami ochrony danych oraz [organami ochrony

[453] Wytyczne Grupy Roboczej Art. 29 dotyczące inspektorów ochrony danych (przypis 242 powyżej), str. 18.
[454] EDPS, Position paper on DPOs (przypis 243 powyżej), str. 6. Zmiany w tekście podano w nawiasach kwadratowych.
[455] *Idem*, Część IV (str. 10 – 11).
[456] Na przykład **francuski** organ ochrony danych, CNIL, zapewnia przydatny specjalny „**extranet**" dla zarejestrowanych inspektorów ochrony danych, dostępny tylko dla nich na podstawie nazwy użytkownika i hasła, w którym prezentowane są teksty prawne (ustawy, dekrety, itp.) oraz szkolenia i informacje, z uwzględnieniem informacji na temat nowych sprawozdań lub wytycznych wydanych przez CNIL, a także innych prawnych i praktycznych zmian oraz umożliwia im wymianę poglądów i prowadzenie dyskusji. Zobacz sekcję 2.3.5. zatytułowaną „Trening formalny i certyfikacja" oraz przypis 274 powyżej.
[457] W oryginalnym zdaniu napisano, że EDPS „wspiera" ta ideę. Można oczekiwać, że organy ochrony danych (i Europejska Rada Ochrony Danych) przyjmą takie samo stanowisko.

danych], która przyczyniłaby się do osiągnięcia ogólnego celu skutecznej ochrony danych osobowych w ramach instytucji ...

IV. 1. Zapewnienie przestrzegania przepisów

Zapewnienie przestrzegania przepisów rozpoczyna się w szczególności od podnoszenia świadomości. Jak wspomniano powyżej, inspektorzy ochrony danych odgrywają istotną rolę w procesie rozwoju wiedzy na temat kwestii związanych z ochroną danych w ramach instytucji/podmiotu. [Można oczekiwać, że organy ochrony][458] potraktują zarówno to, jak i konsekwencje takiego postępowania z zadowoleniem, jako przejaw stymulowania skutecznego podejścia prewencyjnego, a nie stosowania represyjnego nadzoru nad ochroną danych.

Inspektor ochrony danych doradza instytucji/podmiotowi w ramach praktycznych rekomendacji poprawy systemu ochrony danych w takiej instytucji/takim podmiocie lub w zakresie interpretacji albo stosowania [RODO][459]. Taką funkcję doradczą sprawują także [organy ochrony danych], które doradzają wszystkim [krajowym] instytucjom/podmiotom w sprawach dotyczących przetwarzania danych osobowych ([art. 57(1)(c) RODO])). W tym obszarze [krajowi inspektorzy ochrony danych już w przeszłości] byli często wzywani, by udzielić porady inspektorom ochrony danych w konkretnych kwestiach związanych z ochroną danych (indywidualne podejście). [Można oczekiwać, że organy ochrony danych oraz Europejska Rada Ochrony Danych] opracują stanowisko w sprawie pewnych tematów, aby udzielić instytucjom/podmiotom wskazówki dotyczące pewnych ogólniejszych kwestii[460].

IV.2 Wstępne kontrole

Opinie przekazane [przez organ ochrony danych] w ramach [uprzednich konsultacji na mocy art. 36 RODO] oraz [poglądy wyrażone przez organy ochrony danych w procesie wydawania uprzedniej zgody zgodnie z art. 36(5) RODO] stanowią dla [organu ochrony danych] okazję do monitorowania i zapewnienie zgodności z postanowieniami [RODO].... [461]

… Przed ostatecznym przyjęciem opinii z wstępnej kontroli [organ ochrony danych może][462] wysłać wstępny projekt do inspektora ochrony danych z informacją o planowanych rekomendacjach, otwierając tym samym pole do dyskusji na temat skuteczności i konsekwencji planowanych rekomendacji. [Można oczekiwać, że organy ochrony danych], by opracować wykonalne rekomendacje, będą wyczulone na obawy instytucji wyrażane przez inspektora ochrony danych.

IV. 3. Egzekwowanie

W obszarze wdrożenia konkretnych środków ochrony danych pojawia się potencjalna synergia pomiędzy inspektorami ochrony danych a [organami ochrony danych], jeżeli chodzi o stosowanie sankcji oraz rozpatrywanie skarg i zapytań.

Jak już wspomniano, inspektorzy ochrony danych mają ograniczone uprawnienia do egzekwowania. [Organ ochrony danych] będzie uczestniczyć w zapewnieniu zgodności z [RODO] poprzez podejmowanie skutecznych kroków w obszarze uprzednich [konsultacji lub zgód], a także

[458] W oryginalnym zdaniu stwierdza się, że Europejski Inspektor Ochrony Danych „potraktuje" takie podejście z zadowoleniem, ale (także w świetle przeszłych praktyk) ponownie można oczekiwać, że organy ochrony danych (i Europejska Rada Ochrony Danych) przyjmą takie samo stanowisko.

[459] Odwołanie w dokumencie Europejskiego Inspektora Ochrony Danych dotyczy rozporządzenia określającego zasady ochrony danych dla samych instytucji UE (Rozporządzenie (WE) 45/2001) (przypis 148 powyżej), ale, jeżeli chodzi o inspektorów ochrony danych wyznaczonych na mocy RODO, dotyczy to oczywiście także RODO. Podobne zmiany uczyniliśmy również w innych miejscach cytatu.

[460] W oryginalnym zdaniu napisano, że EDPS „zamierza opracować" stanowiska i wskazówki. Ponownie można oczekiwać, że organy ochrony danych i Europejska Rada Ochrony Danych przyjmą takie samo stanowisko w odniesieniu do RODO. Zdanie to brzmi: „W odniesieniu do inspektorów ochrony danych wyznaczonych zgodnie z RODO krajowe organy ochrony danych, a w szczególności nowa Europejska Rada Ochrony Danych, niewątpliwie wydadzą podobne wskazówki".

[461] Pozostała część tego paragrafu oraz pominięte zdanie na początku kolejnego paragrafu wspominają, że luka czasowa pomiędzy wejściem w życie Rozporządzenia a wyznaczeniem Europejskiego Inspektora Ochrony Danych stworzyła duże zaległości w sprawach, które podlegają „kontroli wstępnej" *ex post.* Nie jest jednak jasne, czy podobne problemy wynikają także z RODO. Jeżeli tak jest, w kontekście tym należy rozważyć wystosowanie przez Europejskiego Inspektora Ochrony Danych wezwania do inspektorów ochrony danych oraz organu nadzorującego, by pełnili funkcję „strategicznych partnerów" w procesie rozstrzygnięcia tej sprawy.

[462] Praktyka wysyłania „wstępnego projektu zaleceń" do administratora w kontekście „uprzedniej konsultacji"/"uprzedniego zatwierdzenia" nie została opisana w RODO (ani w Rozporządzeniu 45/2001). Jednak sam fakt, że RODO nawiązuje do „uprzednich konsultacji", wyraźnie sugeruje że organy ochrony danych będą na mocy takiego instrumentu stosować podobne podejście, co znalazło odzwierciedlenie w dodanym dwukrotnie zwrocie w nawiasie kwadratowym.

skarg i innych zapytań. Kroki takie są skuteczne, jeżeli zostaną dobrze ukierunkowane i są wykonalne - w procesie ustalania dobrze ukierunkowanego stosowania danego środka, inspektor ochrony danych może być także postrzegany jako partner strategiczny.

Należy zachęcać do rozpatrywania skarg i zapytań przez inspektora ochrony danych na poziomie lokalnym[463], przynajmniej jeżeli chodzi o pierwszy etap dochodzenia i rozstrzygnięcia. [Można więc oczekiwać, że organy ochrony danych przyjmą stanowisko][464], że inspektorzy ochrony danych powinni spróbować zbadać i rozstrzygnąć skargę na poziomie lokalnym przed jej przekazaniem do [organu ochrony danych]. Inspektor ochrony danych powinien także ... skonsultować się z [organem ochrony danych] za każdym razem, gdy ma wątpliwości co do procedury lub treści skargi. Nie zabrania to jednak osobie, której dane dotyczą, bezpośredniego skierowania sprawy we własnym zakresie do [organu ochrony danych] na mocy [art. 77(1) RODO]. Przysługujące inspektorowi ochrony danych ograniczone uprawnienia egzekwowania oznaczają, że w niektórych przypadkach skargę lub zapytanie należy przekazać [organowi ochrony danych]. Dlatego też [organ ochrony danych] zapewnia cenne wsparcie w obszarze egzekwowania. Z kolei inspektor ochrony danych musi przekazywać [organowi ochrony danych] informacje oraz zapewnić monitorowanie przyjętych środków.

IV.4. Pomiar efektywności[465]

Jeżeli chodzi o pomiar efektywności wdrożenia wymogów ochrony danych, inspektora ochrony danych należy postrzegać jako przydatnego partnera w procesie oceny postępów w tym obszarze. Na przykład, gdy mierzone są wyniki nadzoru wewnętrznego nad ochroną danych, [można oczekiwać, że organy ochrony danych] będą zachęcać[] inspektorów ochrony danych do opracowania swoich własnych kryteriów dobrego nadzoru (standardów zawodowych, konkretnych planów dla instytucji, rocznych programów prac ...). Kryteria te z kolei umożliwiają [organowi ochrony danych], jeżeli zostanie o to poproszony, ocenę pracy inspektora ochrony danych, ale będą także służyć mu do pomiaru stanu wdrożenia postanowień [RODO] w ramach danej instytucji/danego podmiotu.

Jest również prawdopodobne, że inspektorzy ochrony danych w sektorze publicznym zostaną wezwani przez organy nadzorcze do udziału w konsultacjach prowadzonych przez organy nadzorcze oraz do dostarczenia informacji, gdy organ nadzorczy przygotowuje formalny projekt opinii lub projekty przepisów w dziedzinie ochrony danych, które dotyczą obszarów, w których działa inspektor ochrony danych.

W końcu należy zauważyć, że **inspektor ochrony danych odgrywa istotną rolę w procesie wspierania organu ochrony danych w realizacji kontroli na miejscu**, konsultacjach inspektora z administratorami w konkretnych sektorach, itp. Na przykład organy ochrony danych rzadko przeprowadzają inspekcje bez uprzedzenia - odbywa się to z jedynie w przypadku podejrzanych jednostek, które mogłyby ukrywać dane lub inne dowody, gdyby zostały o takiej inspekcji uprzedzone. W praktyce organy ochrony danych normalnie z wyprzedzeniem organizują inspekcje przy pomocy administratora i w szczególności jego inspektora ochrony danych, który będzie w stanie zapewnić dyspozycyjność odpowiednich osób oraz możliwość sprawdzenia właściwych systemów. Często ma to zasadnicze znaczenie, w szczególności w odniesieniu do złożonych systemów przetwarzania, w których dla właściwego przeglądu konieczna jest dogłębna znajomość architektury teleinformatycznej i procesów wewnętrznych. A gdy organ ochrony danych chce szczegółowo zbadać przetwarzanie danych osobowych w konkretnym kontekście lub sektorze, jak ma to z reguły miejsce w ramach rocznego planu i doboru priorytetów, zwróci się do

[463] Należy zauważyć, że rozpatrywanie zapytań i skarg ze strony osób, których dane dotyczą, omówiono bardziej szczegółowo w Zadaniu 11.

[464] Pierwsze dwa zdania w tym paragrafie ponownie dotyczą praktyki promowanej przez Europejskiego Inspektora Ochrony Danych, ale i tutaj (także biorąc pod uwagę przeszłe praktyki) należy oczekiwać, że krajowe organy ochrony danych przyjmą takie samo podejście (jak to wskazane w nawiasach kwadratowych).

[465] Nie istnieją konkretne wymagania, ani w Rozporządzeniu 45/2001 (w odniesieniu do instytucji UE), ani w RODO (w odniesieniu do podmiotów objętych tym instrumentem), dotyczące „pomiaru efektywności" przyjętych przez administratorów środków przez odpowiedni organ nadzorujący (odpowiednio Europejskiego Inspektora Ochrony Danych lub krajowe organy ochrony danych) w celu zapewnienia zgodności z odpowiednim instrumentem. W ramach instytucji UE, Europejski Inspektor Ochrony Danych (prawidłowo) jednak postrzega to jako naturalny element swojej pracy. Należy oczekiwać, że organy ochrony danych państw członkowskich (oraz Europejska Rada Ochrony Danych) także będą „zachęcać" inspektorów ochrony danych do udziału w procesie zapewnienia wysokiego poziomu zgodności poprzez przyjmowanie lub przestrzeganie „standardów zawodowych, konkretnych planów dla instytucji, rocznych programów prac", itp., co odzwierciedlono w nawiasach kwadratowych.

inspektorów ochrony danych administratorów działających w danym kontekście lub sektorze w celu uzyskania realnego wglądu, zorganizowania z nimi spotkań oraz uzyskania odpowiedzi na konsultacje. Stanowi to także część tego, co Europejski Inspektor Ochrony Danych nazywa „strategicznym partnerstwem" pomiędzy inspektorami ochrony danych a organami ochrony danych.

- o – O – o -

Obsługa wniosków osób, których dane dotyczą

ZADANIE 13: Obsługa wniosków i skarg osób, których dane dotyczą

RODO przewiduje, że:

> Osoby, których dane dotyczą, mogą kontaktować się z inspektorem ochrony danych we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy niniejszego Rozporządzenia.
>
> (art. 38(4))

Osoby, których dane dotyczą i które zechcą skorzystać z któregokolwiek z przysługujących im **praw** - prawa dostępu, sprostowania i usunięcia („prawa do bycia zapomnianym"), ograniczenia przetwarzania, przenoszalności danych, prawa do sprzeciwu ogólnie i w odniesieniu do zautomatyzowanego podejmowania decyzji i profilowania - w odniesieniu do organizacji lub które mają **ogólne pytania** lub **skargi** dotyczące ochrony danych przez organizację, powinny normalnie zwracać się w pierwszej kolejności do inspektora ochrony danych takiej organizacji (jeżeli go wyznaczono).

Ułatwia to wymóg RODO zakładający, że organizacja jest zobowiązana opublikować dane inspektora ochrony danych (art. 37(7)) oraz że administrator musi zapewnić *„by inspektor ochrony danych był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych [w odniesieniu do organizacji]"* (art. 38(1)). (Dlatego też, jeżeli osoba, której dane dotyczą, miałaby się sama skierować do kogoś w organizacji, takiego jak radca prawny lub dyrektor generalny, powinni oni przekazać jej wniosek do inspektora ochrony danych).

Ponadto niezależny status inspektora ochrony danych (art. 38(3)) powinien gwarantować, że wnioski, zapytania lub skargi zostaną obsłużone przez inspektora ochrony danych lub przez odpowiedzialnego pracownika pod jego nadzorem w **odpowiedni sposób, bez uprzedzeń na rzecz organizacji lub przeciwko osobie, której dane dotyczą.** W każdym przypadku inspektor ochrony danych powinien sam napisać lub przejrzeć odpowiedź udzielaną osobie, której dane dotyczą. Odpowiedź taka powinna uwzględniać poradę, że - jeżeli osoba, której dane dotyczą, nie jest zadowolona z odpowiedzi - ma prawo przekazać sprawę do organu ochrony danych.

Wynika to z faktu, że w każdej sytuacji przysługujące osobom, których dane dotyczą, prawo do składania wniosków, zapytań i skarg wobec organizacji (tj. jej inspektora ochrony danych), co pozostaje **bez uszczerbku dla ich praw do wniesienia skargi do organu ochrony danych.** A konkretnie, każdy organ ochrony danych jest zobowiązany i uprawniony na swoim terytorium do:

> rozpatrywania skarg wniesionych przez osobę, której dane dotyczą, oraz prowadzenie w odpowiednim zakresie postępowania w przedmiocie tych skarg i informowanie o postępach i wynikach tych postępowań ...
>
> (art. 57(1)(f))

W ramach skarg do organu ochrony danych osoby, których dane dotyczą, mogą być reprezentowane przez odpowiednią organizację, która nie ma zarobkowego charakteru (art. 80), a powyższy obowiązek i uprawnienie organu ochrony danych do rozpatrywania skarg obejmuje także wniesione tą drogą sprawy (patrz: w art. 57(1)(f) zwroty pominięte w powyższym cytacie).

W tym świetle inspektorzy ochrony danych powinni także chcieć podjąć się wniosków i **skarg ze strony tego typu organizacji przedstawicielskich**, a nie tylko ze strony osób, których dane dotyczą.

Jak już wspomniano w odniesieniu do Zadania 10 (*Współpraca z organem ochrony danych*), należy oczekiwać (także w świetle przeszłych praktyk), że krajowe organy ochrony danych (podobnie jak Europejski Inspektor Ochrony Danych w stosunku do inspektorów ochrony danych w instytucjach UE) będą zachęcać osoby, których dane dotyczą, (i takie organizacje) by zawsze najpierw przekazywać wszelkie kwestie administratorowi, a konkretnie jego inspektorowi ochrony danych, by sprawdzić, czy dana sprawa nie może zostać w zadowalający sposób zbadana i rozwiązana w ramach takich kontaktów i bez udziału organu ochrony danych, z zastrzeżeniem że w razie wystąpienia wątpliwości co do ogólnej interpretacji i stosowania RODO inspektor ochrony danych powinien skonsultować się z organem ochrony danych. Nigdy nie należy jednak zniechęcać osób, których dane dotyczą, (lub organizacji

przedstawicielskich), od przekazywania spraw i oczywiście w szczególności pryncypalnych kwestii do organu ochrony danych.

Jak ujmuje to Europejski Inspektor Ochrony Danych, organ nadzorujący i inspektorzy ochrony danych tworzą „strategiczne partnerstwo" - organy ochrony danych mogą zachęcać osoby, których dane dotyczą, by w pierwszej kolejności rozstrzygały wszelkie kwestie bezpośrednio z inspektorami ochrony danych, zaś inspektorzy ochrony danych mogą być w stanie - oraz mogą być zobowiązani - współpracować z organem nadzorującym, by mieć pewność, że odpowiedzi udzielane na pytania i skargi zostaną właściwie obsłużone i w razie potrzeby doprowadzą do zmian w odpowiednich praktykach stosowanych przez administratora. Organy ochrony danych muszą być w stanie polegać na inspektorach ochrony danych, by prawdziwie wspierać osoby, których dane dotyczą, w procesie rozpatrywania skarg, a inspektorzy ochrony danych muszą być w stanie polegać na organach ochrony danych, by zapewnić faktyczne wykonanie rekomendacji dotyczących zmian.

Wzmacnia to delikatny charakter stanowiska inspektora ochrony danych, które zostało omówione w części drugiej, pkt 2.5 - inspektorzy ochrony danych tworzą pomost pomiędzy administratorem a organem nadzorującym i (w pewnym zakresie mieszając metafory, chyba że ktoś odczytuje pomost jako trap) nie powinni mieć możliwość upadku pomiędzy statek a nabrzeże.

- o – O – o -

Informowanie i podnoszenie świadomości

ZADANIE 14: Wewnętrzne i zewnętrzne zadania informowania i podnoszenia świadomości

RODO przewiduje, że zadania inspektora ochrony danych obejmują „co najmniej":

> informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie
>
> (art. 39(1)(a))

Wewnętrznie (w ramach organizacji, w której pracuje inspektor ochrony danych) oznacza to z jednej strony **informowanie** pracowników o ich prawach oraz z drugiej strony **instruowanie** administratorów i organizacji oraz pracowników, z uwzględnieniem „właścicieli"/osób odpowiedzialnych za konkretną operację, w ramach ich obowiązków oraz zakresu odpowiedzialności, a także **szkolenie** ich, jak to zrealizować.

Jak ujmuje to Europejski Inspektor Ochrony Danych we wcześniej cytowanym fragmencie[466]:

> Zapewnienie przestrzegania przepisów rozpoczyna się w szczególności od podnoszenia świadomości ... Inspektorzy ochrony danych odgrywają istotną rolę w procesie rozwoju wiedzy na temat kwestii związanych z ochroną danych w ramach instytucji/podmiotu.

Podnoszenie świadomości „[stymuluje] skuteczne podejście prewencyjne, a nie stosowanie represyjnego nadzoru nad ochroną danych"[467].

Środki przyjęte przez inspektora ochrony danych w odniesieniu do takich celów mogą obejmować wydawanie **not informacyjnych dla pracowników**, organizowanie wewnętrznych **sesji szkoleniowych** poświęconych ochronie danych, co powinno mieć na celu zaszczepienie pracownikom świadomości i wrażliwości wobec ochrony danych i praw osób, których dane dotyczą, („refleks w ochronie danych") w ramach wszystkich ról pełnionych przez nie w społeczeństwie, tj. roli zwykłego obywatela, pracownika, lidera zespołu lub członka kadry zarządzającej.

Dotyczy to także stworzenia wewnętrznej **strony internetowej** informującej i przekazującej wiedzę na temat ochrony danych, a także sporządzenie i wydanie **oświadczeń o prywatności** na stronach internetowych pracowników[468].

Zewnętrznie, poza zapewnieniem, by osobom, których dane dotyczą, przekazano odpowiednią informację, gdy ich dane są gromadzone po raz pierwszy (zgodnie z art. 12-14 RODO), np. w formie jasnej informacji na stronie internetowej, inspektor ochrony danych powinien także współpracować z pracownikami ds. Public Relations, by zapewnić **pełną przejrzystość operacji przetwarzania danych osobowych w organizacji**, celów, dla jakich organizacja gromadzi i przetwarza dane osobowe, kategorii osób, których dane dotyczą, i kategorii danych, odbiorców danych, informacji, czy dane są przekazywane do krajów trzecich poza UE/EOG, itp.

RODO nie wymaga od administratorów upubliczniania całego rejestru operacji przetwarzania danych osobowych[469]**.** Jednak RODO oczywiście także tego nie zabrania.

Europejski Inspektor Ochrony Danych zdecydowanie opowiada się za publikacją w przypadku instytucji UE, w szczególności w świetle faktu, że (podobnie jak Dyrektywa o ochronie danych z 1995 roku) wcześniejsze rozporządzenie nie wymagało publikacji „funkcjonalnie równorzędnych" danych powiadomienia[470]:

> Rejestry stanowią istotne narzędzie sprawdzenia i dokumentowania, że organizacja ma swoje czynności przetwarzania pod kontrolą. ...

---

[466] EDPS, Position paper on DPOs (przypis 243 powyżej), str. 10.
[467] *Idem*.
[468] *Idem*, str. 5.
[469] Dyrektywa o ochronie danych z 1995 roku wymagała od organów ochrony danych upublicznienia szczegółów operacji przetwarzania (art. 21).
[470] EDPS, Accountability on the ground (przypis 353 powyżej), str. 8, podkreślenie zgodne z oryginałem.

Europejski Inspektor Ochrony Danych zdecydowanie zaleca, aby [instytucje UE] podawały rejestry do publicznej wiadomości, najlepiej poprzez ich publikację w internecie ...

Istnieje wiele powodów, dla których należy upublicznić rejestr:

- przyczynia się to do przejrzystości instytucji UE 12;
- pomaga wzmocnić zaufanie publiczne;
- ułatwia dzielenie się informacjami pomiędzy instytucjami UE;
- niepublikowanie stanowiłoby krok wstecz w stronę starych [reguł].

Prawie to samo można powiedzieć o rejestrze operacji przetwarzania prowadzonym na mocy RODO przez administratorów, przynajmniej jeżeli chodzi o organy publiczne. Niektóre państwa członkowskie mogą w swoim prawie krajowym nałożyć obowiązek publikowania szczegółów rejestru, ale organy publiczne w krajach, w których nie jest to obowiązkowe, w dalszym ciągu powinny to rozważyć w świetle obserwacji poczynionych przez Europejskiego Inspektora Ochrony Danych.

Oczywiście administratorzy i podmioty przetwarzające nie powinni czuć się zobowiązani do publikacji informacji na temat swoich ustaleń dotyczących bezpieczeństwa, które mogłyby zostać wykorzystane w celu naruszenia ich bezpieczeństwa (zostało to już uwzględnione w postanowieniach Dyrektywy o ochronie danych z 1995 roku dotyczących publikacji szczegółów czynności przetwarzania, które wcześniej zgłoszono organom ochrony danych)[471].

Podstawowe informacje na temat operacji przetwarzania danych osobowych przez organizację powinny być w każdym przypadku łatwo dostępne na jej **stronie internetowej** oraz przedstawione w **ulotkach** i **formularzach** (z uwzględnieniem wersji dostępnych dla osób niepełnosprawnych).

Strona internetowa i tego typu formularze powinny także w jasny sposób prezentować informacje na temat **sposobów, w jaki osoby, których dane dotyczą, mogą korzystać ze swoich praw** (z uwzględnieniem jasnej publicznej informacji z **danymi kontaktowymi inspektora ochrony danych**, chociaż niekoniecznie z nazwiskiem), **kodeksów postępowania**, do jakich organizacja przystąpiła oraz **certyfikatów**, jakie uzyskała (sprawy te można zaprezentować poprzez uznane **logo** lub **pieczęcie**), itp.

Każda strona internetowa powinna oczywiście spełniać wymagania unijnego prawa o ochronie danych oraz odpowiednich dodatkowych przepisów krajowych w takich sprawach, jak pliki **cookies i inne pliki śledzące,** itp.

ZADANIE 15: Planowanie i przegląd działań inspektora ochrony danych

Wreszcie, biorąc pod uwagę ogromną liczbę i zakres zadań inspektora ochrony danych, powinien on przygotować roczny plan swoich działań, biorąc pod uwagę przewidywany czas potrzebny na wykonanie każdego z nich oraz czas potrzebny na wprowadzenie przewidywalnych nowych zmian, jednocześnie biorą pod uwagę czas potrzebny na reakcję na nieprzewidziane zdarzenia; oraz dokonywać regularnego przeglądu i aktualizacji tego planu.

- o – O – o -

Douwe Korff i Marie Georges
Cambridge/Paryż, grudzień 2018 r.

[471] Zob. ponownie art. 21 Dyrektywy o ochronie danych z 1995 roku, który wyklucza informacje wymienione w art. 19(1)(f), tj. ogólny opis zabezpieczeń administratora, z informacji, jakie należy udostępnić opinii publicznej. Należy jednak zauważyć, że wiara w „bezpieczeństwo poprzez niezrozumiałość" (security through obscurity) została już dawno zdyskredytowana; zob. https://pl.wikipedia.org/wiki/Security_through_obscurity.