Rada
Unii Europejskiej

Bruksela, 12 stycznia 2017 r.
(OR. en)

5034/17

Międzyinstytucjonalny numer referencyjny:
2017/0002 (COD)

DATAPROTECT 2
JAI 2
DAPIX 2
FREMP 1
DIGIT 2
CODEC 4

WNIOSEK

Od:	Sekretarz Generalny Komisji Europejskiej, podpisał dyrektor Jordi AYET PUIGARNAU
Data otrzymania:	12 stycznia 2017 r.
Do:	Jeppe TRANHOLM-MIKKELSEN, Sekretarz Generalny Rady Unii Europejskiej
Nr dok. Kom.:	COM(2017) 8 final
Dotyczy:	Wniosek w sprawie ROZPORZĄDZENIA PARLAMENTU EUROPEJSKIEGO I RADY dotyczącego ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez unijne instytucje, organy i jednostki organizacyjne oraz swobodnego przepływu takich danych i uchylający rozporządzenie (WE) nr 45/2001 i decyzję nr 1247/2002/WE

Delegacje otrzymują w załączeniu dokument COM(2017) 8 final.

Zał.: COM(2017) 8 final

KOMISJA
EUROPEJSKA

Bruksela, dnia 10.1.2017 r.
COM(2017) 8 final

2017/0002 (COD)

Wniosek

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY

dotyczący ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez unijne instytucje, organy i jednostki organizacyjne oraz swobodnego przepływu takich danych i uchylający rozporządzenie (WE) nr 45/2001 i decyzję nr 1247/2002/WE

UZASADNIENIE

1. KONTEKST WNIOSKU

• Przyczyny i cele wniosku

W art. 16 ust. 1 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE) wprowadzonym Traktatem z Lizbony ustanawia się zasadę, zgodnie z którą każda osoba ma prawo do ochrony danych osobowych, które jej dotyczą. Ponadto w art. 16 ust. 2 TFUE Traktatem z Lizbony wprowadzono szczególną podstawę prawną przyjęcia zasad dotyczących ochrony danych osobowych. W art. 8 Karty praw podstawowych Unii Europejskiej zapisano ochronę danych osobowych jako jedno z praw podstawowych.

Prawo do ochrony danych osobowych ma również zastosowanie do przetwarzania danych osobowych przez instytucje, organy i jednostki organizacyjne UE. Rozporządzenie (WE) nr 45/2001[1] – podstawowy dokument ustanawiający obowiązujące unijne przepisy o ochronie danych osobowych – zostało przyjęte w 2001 r. z myślą o realizacji dwóch celów: ochrony prawa podstawowego do ochrony danych oraz zagwarantowania swobodnego przepływu danych osobowych na całym terytorium Unii. Rozporządzenie zostało uzupełnione decyzją nr 1247/2002/WE[2].

W dniu 27 kwietnia 2016 r. Parlament Europejski i Rada przyjęły ogólne rozporządzenie o ochronie danych (rozporządzenie (UE) 2016/679), które zacznie obowiązywać w dniu 25 maja 2018 r. W niniejszym rozporządzeniu wezwano do dostosowania rozporządzenia (WE) nr 45/2001 do zasad i przepisów ustanowionych w rozporządzeniu (UE) 2016/679, aby zapewnić solidne i spójne ramy ochrony danych w Unii i umożliwić stosowanie obu instrumentów równocześnie[3].

Dostosowanie, na ile to możliwe, przepisów o ochronie danych skierowanych do instytucji, organów i jednostek organizacyjnych UE do przepisów o ochronie danych przyjętych w odniesieniu do państw członkowskich jest zgodne ze spójnym podejściem do ochrony danych osobowych w całej Unii. W każdym przypadku, w którym przepisy niniejszego wniosku opierają się na tej samej koncepcji co przepisy rozporządzenia (UE) 2016/679, oba przepisy należy interpretować tak samo, w szczególności ze względu na fakt, że systematyka wniosku powinna być rozumiana jako równoważna systematyce rozporządzenia (UE) 2016/679[4].

W przeglądzie rozporządzenia (WE) nr 45/2001 uwzględnia się również wyniki zapytań i konsultacji z zainteresowanymi stronami, a także badanie oceniające stosowanie rozporządzenia na przestrzeni ostatnich 15 lat.

Nie jest to inicjatywa w ramach programu sprawności i wydajności regulacyjnej (REFIT).

---

[1] Rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych, Dz.U. L 8 z 12.1.2001.

[2] Decyzja nr 1247/2002/WE Parlamentu Europejskiego, Rady i Komisji z dnia 1 lipca 2002 r. w sprawie regulaminu i ogólnych warunków regulujących wykonywanie obowiązków przez Europejskiego Pełnomocnika ds. Ochrony Danych, Dz.U. L 183 z 12.7.2002, s. 1.

[3] Zob. art. 98 i motyw 17 rozporządzenia (UE) 2016/679.

[4] Zob. wyrok TSUE z dnia 9 marca 2010 r., Komisja/Niemcy, C-518/07, ECLI:EU:C:2010:125, pkt 26 i 28.

- **Spójność z przepisami obowiązującymi w tej dziedzinie polityki**

Celem wniosku jest dostosowanie przepisów rozporządzenia (WE) nr 45/2001 do zasad i przepisów ustanowionych w rozporządzeniu (UE) 2016/679, aby zapewnić solidne i spójne ramy ochrony danych w Unii. Do wniosku włączono również odpowiednie zasady ustanowione w rozporządzeniu (WE) XXXX/XX [rozporządzenie o prywatności elektronicznej] w odniesieniu do ochrony końcowych urządzeń telekomunikacyjnych użytkowników końcowych.

- **Spójność z pozostałymi obszarami polityki Unii**

Nie dotyczy

2. PODSTAWA PRAWNA, ZASADA POMOCNICZOŚCI I ZASADA PROPORCJONALNOŚCI

- **Podstawa prawna**

Ochrona osób fizycznych w związku z przetwarzania ich danych osobowych jest jednym z praw podstawowych określonym w art. 8 ust. 1 Karty praw podstawowych Unii Europejskiej.

Niniejszy wniosek oparty jest na art. 16 TFUE będącym podstawą prawną przyjmowania przepisów o ochronie danych. Artykuł ten umożliwia przyjmowanie przepisów dotyczących ochrony osób fizycznych w związku z przetwarzania danych osobowych przez instytucje, organy i jednostki organizacyjne Unii w wykonywaniu działań wchodzących w zakres zastosowania prawa Unii. Umożliwia on także przyjmowanie przepisów dotyczących swobodnego przepływu danych osobowych, w tym danych osobowych przetwarzanych przez tego rodzaju instytucje, organy i jednostki organizacyjne.

- **Pomocniczość (w przypadku kompetencji niewyłącznych)**

Przedmiot niniejszego rozporządzenia stanowi kompetencję wyłączną Unii, ponieważ tylko Unia może przyjmować przepisy regulujące przetwarzanie danych osobowych przez instytucje unijne.

- **Proporcjonalność**

Zgodnie z zasadą proporcjonalności do osiągnięcia podstawowego celu polegającego na zapewnieniu jednakowego stopnia ochrony osób fizycznych w związku z przetwarzaniem danych osobowych oraz swobodnego przepływu danych osobowych w całej Unii niezbędne i właściwe jest ustanowienie przepisów dotyczących przetwarzania danych osobowych przez unijne instytucje, organy i jednostki organizacyjne. Niniejsze rozporządzenie nie wykracza poza to, co jest konieczne do osiągnięcia przedmiotowych celów zgodnie z art. 5 ust. 4 Traktatu o Unii Europejskiej.

- **Wybór instrumentu**

Rozporządzenie uznaje się za odpowiedni instrument prawny do celów określenia ram dotyczących ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez unijne instytucje, organy i jednostki organizacyjne oraz swobodnego przepływu takich danych. W rozporządzeniu zapewnia się osobom fizycznym prawa możliwe do wyegzekwowania na drodze prawnej i określa się obowiązki administratorów w zakresie

przetwarzania danych w unijnych instytucjach, organach i jednostkach organizacyjnych. W rozporządzeniu przewiduje się również obowiązek niezależnego organu nadzorczego, jakim jest Europejski Inspektor Ochrony Danych, polegający na monitorowaniu przetwarzania danych osobowych przez unijne instytucje, organy i jednostki organizacyjne.

3. WYNIKI OCEN *EX POST*, KONSULTACJI Z ZAINTERESOWANYMI STRONAMI I OCEN SKUTKÓW

Komisja przeprowadziła konsultacje z zainteresowanymi stronami w latach 2010 i 2011 oraz sporządziła ocenę skutków w związku z pracami nad pakietem dotyczącym reformy ochrony danych, zawierającym informacje na temat proponowanych zmian w rozporządzeniu (WE) nr 45/2001. W tym kontekście Komisja przeprowadziła również badanie wśród koordynatorów ds. ochrony danych działających w ramach Komisji[5].

Jeżeli chodzi o praktyczne stosowanie rozporządzenia (WE) nr 45/2001 przez unijne instytucje, organy i jednostki organizacyjne, zgromadzone informacje pochodziły od Europejskiego Inspektora Ochrony Danych (EIOD), innych unijnych instytucji, organów i jednostek organizacyjnych, innych dyrekcji generalnych Komisji i jednego wykonawcy zewnętrznego. Kwestionariusz przesłano do sieci inspektorów ochrony danych[6].

Inspektorzy ochrony danych z szeregu unijnych instytucji, organów i jednostek organizacyjnych przeprowadzili warsztaty poświęcone reformie rozporządzenia nr 45/2001, które odbyły się w dniach 9 lipca 2015 r., 22 października 2015 r., 19 stycznia 2016 r. i 15 marca 2016 r.

W 2013 r. Komisja podjęła decyzję o przeprowadzeniu badania oceniającego dotychczasowe stosowanie rozporządzenia (WE) nr 45/2001, które zleciła zewnętrznemu wykonawcy. W dniu 8 czerwca 2015 r. Komisja otrzymała końcowe wyniki badania oceniającego (sprawozdanie końcowe, pięć studiów przypadków i analizę poszczególnych artykułów)[7].

Ocena wykazała skuteczność systemu zarządzania, w którego centrum znajdują się inspektorzy ochrony danych i EIOD. W wyniku oceny ustalono, że podział uprawnień między inspektorów ochrony danych a EIOD jest przejrzysty i odpowiednio wyważony, a oba organy dysponują odpowiednim zakresem uprawnień. Mogą jednak pojawić się trudności wynikające z braku uprawnień ze względu na niewystarczające wsparcie inspektorów ochrony danych ze strony ich kierownictwa.

W badaniu oceniającym wskazano, że rozporządzenie (WE) nr 45/2001 można by lepiej egzekwować dzięki stosowaniu sankcji przez EIOD. Lepsze wdrażanie przepisów o ochronie danych można by osiągnąć dzięki większemu wykorzystaniu uprawnień organu nadzorczego nadanych EIOD. Ustalono również, że, aby lepiej wdrażać wymogi dotyczące zatrzymywania

---

5 Zob. pod adresem http://ec.europa.eu/justice/data-protection/reform/index_en.htm.

6 Zob. ogólne sprawozdanie Europejskiego Inspektora Ochrony Danych „Measuring compliance with Regulation (EC) 45/2001 in EU institutions (»Survey 2013«)" oraz „Opinion 3/2015 »Europe's big opportunity: EDPS recommendations on the EU's options for data protection reform«".

7 JUST/2013/FRAC/FW/0157/A4 w kontekście wielokrotnej umowy ramowej JUST/2011/EVAL/01 (RS 2013/05) – sprawozdanie „Evaluation Study on Regulation (EC) 45/2001", Ernst and Young, dostępne pod adresem http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=51087.

danych i ich bezpieczeństwa, administratorzy danych powinni przyjąć zasady zarządzania ryzykiem i przeprowadzać oceny ryzyka przed przystąpieniem do operacji przetwarzania.

Z badania wynika również, że obowiązujące przepisy zawarte w rozdziale IV rozporządzenia (WE) nr 45/2001, dotyczące sektora telekomunikacyjnego, są nieaktualne i konieczne jest dostosowanie tego rozdziału do dyrektywy o prywatności elektronicznej. Zgodnie z badaniem oceniającym istnieje również potrzeba doprecyzowania niektórych kluczowych definicji zawartych w rozporządzeniu (WE) nr 45/2001. Dotyczy to identyfikacji administratorów danych w unijnych instytucjach, organach i jednostkach organizacyjnych, definicji odbiorcy i objęcia obowiązkiem zachowania poufności również zewnętrzne podmioty przetwarzające.

W badaniu oceniającym zwrócono również uwagę na potrzebę uproszczenia systemu zgłoszeń i kontroli wstępnych w celu zwiększenia efektywności i ograniczenia obciążenia administracyjnego.

Podmiot oceniający przeprowadził ankietę internetową w 64 unijnych instytucjach, organach i jednostkach organizacyjnych. Na pytania zadane w ankiecie odpowiedzi udzieliło 422 odpowiedzialnych urzędników z podmiotów działających jako administratorzy danych, 73 inspektorów ochrony danych, 118 koordynatorów ds. ochrony danych i 109 respondentów z sektora informatycznego. Podmiot oceniający przeprowadził również szereg wywiadów z zainteresowanymi stronami. W dniu 26 marca 2015 r. podmiot oceniający wraz z Komisją zorganizowały końcowe warsztaty, w których udział wzięło wielu administratorów danych, inspektorów ochrony danych, koordynatorów ds. ochrony danych, respondentów z sektora informatycznego i przedstawicieli EIOD.

- **Gromadzenie i wykorzystanie wiedzy specjalistycznej**

Zob. odniesienie do badania oceniającego w poprzednim punkcie.

- **Ocena skutków**

Skutki niniejszego wniosku odczują głównie unijne instytucje, organy i jednostki organizacyjne. Zostało to potwierdzone na podstawie zgromadzonych informacji pochodzących od EIOD, innych unijnych instytucji, organów i jednostek organizacyjnych, dyrekcji generalnych Komisji i wykonawcy zewnętrznego. Ponadto skutki nowych obowiązków wynikających z rozporządzenia (UE) 2016/679, do którego mają zostać dostosowane przepisy niniejszego rozporządzenia, poddano ocenie w kontekście prac przygotowawczych nad niniejszym rozporządzeniem. Tym samym nie ma potrzeby przeprowadzenia szczególnej oceny skutków niniejszego rozporządzenia.

- **Sprawność regulacyjna i uproszczenie**

Nie dotyczy

- **Prawa podstawowe**

Prawo do ochrony danych osobowych określono w art. 8 Karty praw podstawowych Unii Europejskiej (karta), w art. 16 TFUE i art. 8 europejskiej konwencji praw człowieka. Jak

podkreślił Trybunał Sprawiedliwości Unii Europejskiej[8], prawo do ochrony danych osobowych nie jest prawem absolutnym i powinno być oceniane w świetle jego funkcji społecznej[9]. Ochrona danych jest ściśle powiązana z poszanowaniem życia prywatnego i rodzinnego chronionego na podstawie art. 7 karty.

W niniejszym wniosku określa się przepisy dotyczące ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez unijne instytucje, organy i jednostki organizacyjne oraz swobodnego przepływu takich danych.

Inne prawa podstawowe zapisane w karcie, na które wniosek może potencjalnie mieć wpływ, to: wolność wypowiedzi (art. 11); prawo własności, a w szczególności ochrona praw własności intelektualnej (art. 17 ust. 2); zakaz dyskryminacji innych osób ze względu na takie czynniki jak: rasa, pochodzenie etniczne, cechy genetyczne, religię lub przekonania, poglądy polityczne lub wszelkie inne poglądy, niepełnosprawność lub orientację seksualną (art. 21); prawa dziecka (art. 24); prawo do wysokiego poziomu ochrony zdrowia ludzkiego (art. 35); prawo dostępu do dokumentów (art. 42); prawo do skutecznego środka prawnego i dostępu do bezstronnego sądu (art. 47*).*

4. WPŁYW NA BUDŻET

Zob. załączona ocena skutków finansowych.

5. INNE ELEMENTY

- **Plany wdrożenia i monitorowanie, ocena i sprawozdania**

Nie dotyczy

- **Dokumenty wyjaśniające (w przypadku dyrektyw)**

Nie dotyczy

ROZDZIAŁ I – PRZEPISY OGÓLNE

W art. 1 definiuje się zakres przedmiotowy rozporządzenia oraz, tak jak w art. 1 rozporządzenia (WE) nr 45/2001, określa się dwa cele rozporządzenia. Są to: ochrona prawa podstawowego do ochrony danych oraz zagwarantowanie swobodnego przepływu danych osobowych na terytorium Unii. W artykule tym przewiduje się również główne zadania Europejskiego Inspektora Ochrony Danych.

W art. 2 określa się zakres stosowania rozporządzenia: rozporządzenie ma zastosowanie do przetwarzania danych osobowych w sposób zautomatyzowany lub w inny sposób przez wszystkie unijne instytucje i organy, o ile takie przetwarzanie jest prowadzone podczas

[8] Zob. wyrok Trybunału Sprawiedliwości z dnia 9 listopada 2010 r., Volker und Markus Schecke i Eifert, sprawy połączone C-92/09 i C-93/09, ECLI:EU:C:2009:284, pkt 48.

[9] Zgodnie z art. 52 ust. 1 karty można ograniczyć korzystanie z prawa do ochrony danych, o ile takie ograniczenia są przewidziane prawem i respektują istotę praw i wolności, i o ile, z zastrzeżeniem zasady proporcjonalności, są one konieczne i rzeczywiście odpowiadają celom interesu ogólnego uznawanym przez Unię Europejską lub potrzebom ochrony praw i wolności innych osób.

wykonywania czynności całkowicie lub częściowo podlegających prawu Unii. Materialny zakres stosowania tego rozporządzenia jest neutralny pod względem technologicznym. Ochrona danych osobowych ma zastosowanie do zautomatyzowanego przetwarzania danych osobowych oraz do przetwarzania ręcznego, jeżeli dane osobowe znajdują się lub mają się znaleźć w zbiorze danych.

Art. 3 zawiera definicje terminów używanych w rozporządzeniu. Z wyjątkiem definicji terminów: „instytucje i organy unijne", „administrator", „użytkownik" i „spis", które są właściwe dla niniejszego rozporządzenia, terminy stosowane w tym rozporządzeniu zdefiniowano w rozporządzeniu (UE) 2016/679, rozporządzeniu (UE) 0000/00 [nowe rozporządzenie o prywatności elektronicznej], dyrektywie 00/0000/UE [dyrektywa ustanawiająca europejski kodeks łączności elektronicznej] oraz dyrektywie Komisji 2008/63/WE.

ROZDZIAŁ II – ZASADY

W art. 4 określa się zasady dotyczące przetwarzania danych osobowych, które odpowiadają zasadom wskazanym w art. 5 rozporządzenia (UE) 2016/679. W porównaniu z rozporządzeniem (WE) nr 45/2001 w rozporządzeniu dodaje się nowe zasady dotyczące przejrzystości, integralności i poufności.

Art. 5 opiera się na art. 6 rozporządzenia (UE) 2016/679 i zawiera kryteria dotyczące zgodności przetwarzania z prawem, przy czym jedyny wyjątek stanowi kryterium prawnie uzasadnionego interesu realizowanego przez administratora, które nie ma zastosowania do sektora publicznego i tym samym nie może być stosowane wobec instytucji i organów unijnych. W art. 5 zachowuje się kryteria już określone w art. 5 rozporządzenia (WE) nr 45/2001.

W art. 6 wyjaśnia się warunki przetwarzania w innym celu zgodnym z przepisami zgodnie z art. 6 ust. 4 rozporządzenia (UE) 2016/679. W porównaniu z art. 6 rozporządzenia (WE) nr 45/2001 we wspomnianym nowym przepisie zapewnia się większą elastyczność i pewność prawa w zakresie dalszego przetwarzania do celów zgodnych z przepisami.

W art. 7 wyjaśnia się – zgodnie z art. 7 rozporządzenia (UE) 2016/679 – warunki, aby zgoda stanowiła ważną podstawę prawną w odniesieniu do zgodności przetwarzania z prawem.

W art. 8 określa się – zgodnie z art. 8 rozporządzenia (UE) 2016/679 – dalsze warunki zgodności z prawem przetwarzania danych osobowych dzieci w odniesieniu do usług społeczeństwa informacyjnego oferowanych im bezpośrednio. W artykule określa się, że, aby zgoda była ważna, dziecko musi mieć ukończone co najmniej 13 lat.

W art. 9 określa się – zgodnie z art. 8 rozporządzenia (WE) nr 45/2001 – zasady ustanawiające specjalny stopień ochrony w odniesieniu do przekazywania danych osobowych odbiorcom innym niż instytucje i organy unijne posiadającym jednostkę organizacyjną w Unii i podlegającym rozporządzeniu (UE) 2016/679 lub dyrektywie (UE) 2016/680. W artykule wyjaśnia się, że jeżeli przekazywanie danych odbywa się z inicjatywy administratora, musi on wykazać, że jest to działanie konieczne i proporcjonalne.

W art. 10 określono ogólny zakaz przetwarzania szczególnych kategorii danych osobowych oraz wyjątki od tej zasady ogólnej na podstawie art. 9 rozporządzenia (UE) 2016/679 i rozwinięcia art. 10 rozporządzenia (WE) nr 45/2001.

W art. 11 określa się – zgodnie z art. 10 rozporządzenia (UE) 2016/679 i art. 10 ust. 5 rozporządzenia (WE) nr 45/2001 – warunki przetwarzania danych osobowych dotyczących wyroków skazujących i naruszeń prawa.

Art. 12 zawiera wyjaśnienie obowiązków informacyjnych administratora wobec osoby, której dane dotyczą – zgodnie z art. 11 rozporządzenia (UE) 2016/679 – i stanowi, że jeżeli dane osobowe przetwarzane przez administratora nie pozwalają mu zidentyfikować osoby fizycznej, nie powinien on mieć obowiązku uzyskania dodatkowych informacji w celu zidentyfikowania osoby, której dane dotyczą, wyłącznie po to, by zastosować się do przepisów niniejszego rozporządzenia. Administrator nie powinien jednak odmawiać przyjęcia dodatkowych informacji od osoby, której dane dotyczą, by ułatwić jej wykonywanie jej praw.

W art. 13 określa się – na podstawie art. 89 ust. 1 rozporządzenia (UE) 2016/679 – zasady dotyczące zabezpieczeń mających zastosowanie do przetwarzania do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych.

ROZDZIAŁ III – PRAWA OSOBY, KTÓREJ DANE DOTYCZĄ

Sekcja 1 – Przejrzystość oraz tryby korzystania z praw

W art. 14 wprowadza się – na podstawie art. 12 rozporządzenia (UE) 2016/679 – obowiązek administratora polegający na zapewnieniu przejrzystych, łatwo dostępnych i zrozumiałych informacji, procedur i mechanizmów ułatwiających osobie, której dane dotyczą, wykonywanie przysługujących jej praw, co w stosownych przypadkach obejmuje zapewnienie sposobów umożliwiających składanie wniosków drogą elektroniczną, wymóg udzielenia odpowiedzi na wniosek osoby, której dane dotyczą, w określonym terminie oraz przedstawienia uzasadnienia odmowy udzielenia odpowiedzi. Ponieważ od instytucji i organów unijnych w żadnych okolicznościach nie oczekuje się pobierania opłat w związku z kosztami administracyjnymi ponoszonymi z tytułu udzielania informacji, w niniejszym akcie nie uwzględniono tej możliwości, przewidzianej w rozporządzeniu (UE) 2016/679.

Sekcja 2 – Informacje i dostęp do danych

W art. 15 określa się obowiązki informacyjne administratora wobec osoby, której dane dotyczą, w przypadku zbierania danych osobowych od tej osoby – na podstawie art. 13 rozporządzenia (UE) 2016/679 i rozwinięcia art. 11 rozporządzenia (WE) nr 45/2001 – polegające na udzielaniu informacji takiej osobie, w tym informacji na temat okresu przechowywania i prawa do wniesienia skargi oraz w odniesieniu do międzynarodowego przekazywania danych.

W art. 16 doprecyzowuje się – na podstawie art. 14 rozporządzenia (UE) 2016/679 i rozwinięcia art. 12 rozporządzenia (WE) nr 45/2001 – obowiązki informacyjne administratora wobec osoby, której dane dotyczą, w sytuacji, w której dane osobowe jej dotyczące uzyskano z innego źródła, polegające na udzielaniu informacji na temat źródła pochodzenia danych. W artykule tym utrzymuje się ponadto możliwe odstępstwa przewidziane w rozporządzeniu (UE) 2016/679, np. obowiązek taki nie wystąpi, jeżeli osoba, której dane dotyczą, dysponuje już tymi informacjami, udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku ze strony administratora, dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianym w prawie Unii lub też utrwalenie lub ujawnienie danych są wyraźnie przewidziane prawem. Mogłoby to

na przykład dotyczyć postępowań prowadzonych przez służby odpowiedzialne za sprawy zabezpieczenia społecznego lub zdrowia publicznego.

W art. 17 przewiduje się – zgodnie z art. 15 rozporządzenia (UE) 2016/679 i dalszym uzupełnieniem art. 13 rozporządzenia (WE) nr 45/2001 – prawo dostępu osoby, której dane dotyczą, do jej danych osobowych i dodaje się nowe elementy, takie jak obowiązek informowania osób, których dane dotyczą, o okresie przechowywania, prawach do sprostowania i usuwania danych oraz wniesienia skargi.

Sekcja 3 – Sprostowanie i usuwanie

W art. 18 określa się prawo osoby, której dane dotyczą, do poprawiania danych na podstawie art. 16 rozporządzenia (UE) 2016/679 i dalszego rozwinięcia art. 14 rozporządzenia (WE) nr 45/2001.

W art. 19 określa się prawo osoby, której dane dotyczą, do bycia zapomnianym i do usunięcia danych zgodnie z art. 17 rozporządzenia (UE) 2016/679 i rozwinięciem art. 16 rozporządzenia (WE) nr 45/2001. W artykule określa się warunki wykonywania prawa do bycia zapomnianym, w tym obowiązek administratora, który podał dane osobowe do wiadomości publicznej, polegający na poinformowaniu osób trzecich, że osoba, której dane dotyczą, żąda, usunięcia wszelkich łączy do tych danych osobowych, ich kopii lub replikacji.

W art. 20 wprowadza się prawo do ograniczenia przetwarzania w niektórych przypadkach, unikając w ten sposób niejednoznacznego terminu „blokowanie” zastosowanego w rozporządzeniu (WE) nr 45/2001 i zapewniając spójność z nową terminologią użytą w art. 18 rozporządzenia (UE) 2016/679.

W art. 21 przewiduje się – zgodnie z art. 19 rozporządzenia (UE) 2016/679 i rozwinięciem art. 17 rozporządzenia (WE) nr 45/2001 – obowiązek administratora polegający na poinformowaniu odbiorców, którym ujawniono dane osobowe, o każdym przypadku sprostowania lub usunięcia danych osobowych lub o ograniczeniu przetwarzania, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Ponadto administrator informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.

W art. 22 wprowadza się – zgodnie z art. 20 rozporządzenia (UE) 2016/679 – prawo osoby, której dane dotyczą, do przenoszenia danych, tj. prawo do uzyskania dotyczących jej danych osobowych, które podała administratorowi, lub do tego, aby tego rodzaju dane zostały przekazane bezpośrednio innemu administratorowi, jeżeli jest to możliwe z technicznego punktu widzenia. W artykule tym przewidziano jako warunek konieczny, a także w celu dalszej poprawy dostępu osób fizycznych do ich danych osobowych, prawo do uzyskania od administratora tych danych w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego. Prawo to ma zastosowanie jedynie wówczas, gdy przetwarzanie opiera się na zgodzie osoby, której dane dotyczą, lub na zawartej przez tę osobę umowie.

Sekcja 4 – Prawo sprzeciwu oraz podejmowanie zautomatyzowanej decyzji indywidualnej

W art. 23 przewidziano prawo sprzeciwu przysługujące osobie, której dane dotyczą, na podstawie art. 21 rozporządzenia (UE) 2016/679 i rozwinięcia art. 18 rozporządzenia (WE) nr 45/2001.

Artykuł 24 dotyczy prawa osoby, której dane dotyczą, do tego, by nie podlegała ona środkowi, który opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu zgodnie z art. 22 rozporządzenia (UE) 2016/679 i rozwinięciem art. 19 rozporządzenia (WE) nr 45/2001.

Sekcja 5 – Ograniczenia

W art. 25 dopuszcza się ograniczenia praw osoby, której dane dotyczą, określonych w art. 14–22 i w art. 34 i 38 oraz zasad określonych w art. 4 (o ile jego przepisy odpowiadają prawom i obowiązkom przewidzianym w art. 14–22). Tego rodzaju ograniczenia należy określać w aktach prawnych przyjmowanych na podstawie Traktatów lub wewnętrznych przepisów instytucji i organów unijnych. Jeżeli w aktach prawnych przyjętych na podstawie Traktatów lub wewnętrznych przepisów instytucji i organów unijnych nie przewidziano możliwości tego rodzaju ograniczenia, instytucje i organy unijne mogą narzucić ograniczenie doraźne, jeżeli nie narusza ono istoty podstawowych praw i wolności w odniesieniu do danej operacji przetwarzania i stanowi w demokratycznym społeczeństwie niezbędny i proporcjonalny środek, który zapewnia osiągnięcie co najmniej jednego celu dopuszczającego ograniczenie praw osoby, której dane dotyczą. Podejście to jest zgodne z art. 23 rozporządzenia (UE) 2016/679. W przeciwieństwie jednak do art. 23 rozporządzenia (UE) 2016/679 oraz zgodnie z art. 20 rozporządzenia (WE) nr 45/2001 w przepisie tym nie przewiduje się możliwości ograniczenia prawa do sprzeciwu ani prawa do niepodlegania decyzjom opartym wyłącznie na zautomatyzowanym przetwarzaniu. Wymogi dotyczące ograniczeń są dostosowane do Karty praw podstawowych Unii Europejskiej i europejskiej konwencji praw człowieka, w myśl wykładni odpowiednio Trybunału Sprawiedliwości Unii Europejskiej i Europejskiego Trybunału Praw Człowieka.

ROZDZIAŁ IV – ADMINISTRATOR I PODMIOT PRZETWARZAJĄCY

Sekcja 1 – Obowiązki ogólne

W art. 26 oparto się na art. 24 rozporządzenia (UE) 2016/679 i wprowadzono „zasadę rozliczalności”, opisując obowiązek przestrzegania przez administratora przepisów niniejszego rozporządzenia oraz wykazywania takiej zgodności, w tym w drodze przyjmowania odpowiednich środków technicznych i organizacyjnych oraz, w stosownych przypadkach, wewnętrznych polityk i mechanizmów. W przepisie tym nie zachowano przepisu art. 24 ust. 3 rozporządzenia (UE) 2016/679, ponieważ instytucje i organy unijne nie powinny stosować się do kodeksów postępowania czy mechanizmów certyfikacji.

W art. 27 określa się – zgodnie z art. 25 rozporządzenia (UE) 2016/679 – obowiązki administratora wynikające z zasady uwzględniania ochrony danych w fazie projektowania oraz zasady domyślnej ochrony danych.

Artykuł 28 dotyczący współadministratorów opiera się na art. 26 rozporządzenia (UE) 2016/679, co ma na celu wyjaśnienie obowiązków współadministratorów – niezależnie, czy są to instytucje lub organy unijnych czy też nie – jeżeli chodzi o ich stosunki wewnętrzne oraz wobec osoby, której dane dotyczą. Przepis ten reguluje sytuację, w której wszyscy współadministratorzy podlegają temu samemu systemowi prawnemu (niniejszemu rozporządzeniu), oraz sytuację, w której niektórzy z nich podlegają niniejszemu rozporządzeniu a niektórzy – innemu instrumentowi prawnemu (rozporządzeniu (UE) 2016/679, dyrektywie (UE) 2016/680, dyrektywie (UE) 2016/681 i innym szczególnym systemom ochrony danych dotyczącym instytucji lub organów unijnych).

Art. 29 opiera się na art. 28 rozporządzenia (UE) 2016/679 i zawiera rozwinięcie art. 23 rozporządzenia (WE) nr 45/2001 w celu wyjaśnienia pozycji i obowiązków podmiotów przetwarzających, w tym zawiera stwierdzenie, że podmiot przetwarzający, który narusza postanowienia niniejszego rozporządzenia przy określaniu celów i sposobów przetwarzania, uznaje się za administratora w odniesieniu do tego przetwarzania.

W art. 30 dotyczącym przetwarzania z upoważnienia administratora lub podmiotu przetwarzającego, który opiera się na art. 29 rozporządzenia (UE) 2016/679, ustanawia się zakaz przetwarzania takich danych w stosunku do podmiotu przetwarzającego i każdej osoby działającej z upoważnienia administratora lub podmiotu przetwarzającego i mającej dostęp do danych osobowych z wyjątkiem sytuacji, w których tego rodzaju podmiot lub osoba przetwarzają je wyłącznie na polecenie administratora, chyba że wymaga tego prawo Unii lub prawo państwa członkowskiego.

W art. 31, opierającym się na art. 30 rozporządzenia (UE) 2016/679, wprowadza się obowiązek administratorów i podmiotów przetwarzających polegający na prowadzeniu dokumentacji dotyczącej operacji przetwarzania, za które odpowiadają, zamiast wcześniejszego powiadamiania Europejskiego Inspektora Ochrony Danych zgodnie z wymogami art. 25 rozporządzenia (WE) nr 45/2001 oraz rejestru prowadzonego przez inspektorów ochrony danych. W przeciwieństwie do rozporządzenia (UE) 2016/679 przepis ten nie zawiera odniesienia do przedstawicieli, ponieważ instytucje unijne nie będą miały przedstawicieli, a zawsze będą miały inspektorów ochrony danych. Nie zachowano odniesień do przekazywania danych na podstawie wyjątków mających zastosowanie w szczególnych sytuacjach, jak to przewidziano w rozporządzeniu (UE) 2016/679, ponieważ w niniejszym rozporządzeniu nie przewiduje się tego rodzaju przekazywania danych. Obowiązek prowadzenia rejestru czynności przetwarzania może mieć charakter scentralizowany na szczeblu instytucji unijnej lub organu unijnego. W takim przypadku instytucje i organy unijne mogą prowadzić swoje rejestry czynności przetwarzania w formie publicznie dostępnego rejestru.

W art. 32 wyjaśnia się na podstawie art. 31 rozporządzenia (UE) 2016/679 obowiązki instytucji i organów unijnych dotyczące współpracy z EIOD.

Sekcja 2 – Bezpieczeństwo danych osobowych i poufność łączności elektronicznej

W art. 33 zobowiązuje się administratora – zgodnie z art. 32 rozporządzenia (UE) 2016/679 i rozwinięciem art. 22 rozporządzenia (WE) nr 45/2001 – do wprowadzenia odpowiednich środków mających na celu zapewnienie bezpieczeństwa przetwarzania, rozszerzając ten obowiązek na podmioty przetwarzające, niezależnie od warunków umowy zawartej z administratorem.

W art. 34, który opiera się na art. 36 rozporządzenia (WE) nr 45/2001, zapewnia się poufność łączności elektronicznej w obrębie instytucji i organów unijnych.

Artykuł 35 opiera się na obowiązującej praktyce instytucji i organów unijnych i obejmuje ochroną informacje mające związek z końcowymi urządzeniami telekomunikacyjnymi użytkowników końcowych, którzy łączą się z dostępnymi publicznie stronami internetowymi i aplikacjami mobilnymi udostępnianymi przez instytucje i organy unijne zgodnie z rozporządzeniem (UE) XXXX/XX [nowe rozporządzenie o prywatności elektronicznej], a w szczególności z jego art. 8.

W art. 36, który opiera się na art. 38 rozporządzenia (WE) nr 45/2001, przewidziano ochronę danych osobowych zawartych w publicznych i prywatnych spisach prowadzonych przez instytucje i organy unijne.

W art. 37 i 38 wprowadza się obowiązek zgłaszania naruszenia ochrony danych osobowych zgodnie z art. 33 i 34 rozporządzenia (UE) 2016/679.

Sekcja 3 – Ocena skutków dla ochrony danych i uprzednie konsultacje

W art. 39, który opiera się na art. 35 rozporządzenia (UE) 2016/679, wprowadza się obowiązek sporządzania przez administratorów i podmioty przetwarzające oceny skutków w zakresie ochrony danych przed podjęciem operacji przetwarzania, z którymi wedle wszelkiego prawdopodobieństwa wiąże się wysokie ryzyko naruszenia praw i wolności osób fizycznych. Obowiązek ten będzie miał zastosowanie w szczególności w przypadku systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, przetwarzaniu na dużą skalę szczególnych kategorii danych lub systematycznym monitorowaniu na dużą skalę miejsc dostępnych publicznie.

Artykuł 40 opiera się na art. 36 rozporządzenia (UE) 2016/679 i dotyczy przypadków, w których zezwolenie EIOD oraz konsultacje z nim są obowiązkowe przed przystąpieniem do przetwarzania. W art. 40 ust. 1 przytacza się jednak motyw 94 rozporządzenia (UE) 2016/679 w celu wyjaśnienie zakresu stosowania obowiązku przeprowadzenia konsultacji.

Sekcja 4 – Informacje i dostęp do danych

W art. 41 nałożono na instytucje i organy unijne obowiązek informowania EIOD o wdrażanych przez nie środkach administracyjnych i wewnętrznych przepisach odnoszących się do przetwarzania danych osobowych.

Artykuł 42 stanowi, że Komisja ma obowiązek konsultować się z EIOD po przyjęciu wniosków w sprawie aktów ustawodawczych oraz zaleceń lub wniosków przedłożonych Radzie zgodnie z art. 218 TFUE oraz podczas opracowywania aktów delegowanych lub aktów wykonawczych, które mają wpływ na ochronę praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych. Jeżeli tego rodzaju akty mają szczególne znaczenie dla ochrony praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych, Komisja może również skonsultować się z Europejską Radą Ochrony Danych. W takich przypadkach oba organy powinny koordynować swoje prace w celu wydania wspólnej opinii. Na wydanie zalecenia w wyżej wymienionych przypadkach ustanawia się termin 8 tygodni, od którego możliwe są odstępstwa w sprawach pilnych, a jeżeli sprawa nie ma charakteru pilnego – w stosownych przypadkach, na przykład, gdy Komisja opracowuje akty delegowane i wykonawcze.

Sekcja 5 – Obowiązek reagowania na zarzuty

W art. 43 nałożono na administratorów i podmiot przetwarzający obowiązek reagowania na zarzuty po przekazywaniu im sprawy do rozpatrzenia w wyniku decyzji EIOD.

Sekcja 6 – Inspektor ochrony danych

Na podstawie art. 37 ust. 1 lit. a) rozporządzenia (UE) 2016/679 i art. 24 rozporządzenia (WE) nr 45/2001 do art. 44 wprowadzano obowiązkowe powołanie inspektora ochrony danych w instytucjach i organach unijnych.

Na podstawie art. 38 rozporządzenia (UE) 2016/679 i art. 24 rozporządzenia (WE) nr 45/2001 w art. 45 określa się status inspektora ochrony danych.

Na podstawie art. 39 rozporządzenia (UE) 2016/679 i art. 24 rozporządzenia (WE) nr 45/2001 oraz pkt 2 i 3 załącznika do rozporządzenia (WE) nr 45/2001 w art. 46 określa się główne zadania inspektora ochrony danych.

ROZDZIAŁ V – PRZEKAZYWANIE DANYCH OSOBOWYCH DO PAŃSTW TRZECICH LUB ORGANIZACJI MIĘDZYNARODOWYCH

Ponadto na podstawie art. 9 rozporządzenia (WE) nr 45/2001 art. 47 zawiera ogólną zasadę, zgodnie z art. 44 rozporządzenia (UE) 2016/679, w myśl której przestrzeganie pozostałych przepisów niniejszego rozporządzenia i warunków określonych w rozdziale V jest warunkiem jakiegokolwiek przekazania danych osobowych do państw trzecich lub organizacji międzynarodowych, w tym dalszego przekazania danych z państwa trzeciego lub przez organizację międzynarodową do innego państwa trzeciego lub innej organizacji międzynarodowej.

Art. 48 stanowi, że przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej może nastąpić, gdy Komisja stwierdzi na podstawie art. 45 ust. 3 rozporządzenia (UE) 2016/679, że dane państwo trzecie, terytorium lub określony sektor lub określone sektory w tym państwie trzecim lub dana organizacja międzynarodowa zapewniają odpowiedni stopień ochrony, a dane osobowe są przekazywane tylko po to, aby umożliwić wykonywanie zadań wchodzących w zakres kompetencji administratora. Ust. 2 i 3 przedmiotowego artykułu zostały przejęte z art. 9 rozporządzenia (WE) nr 45/2001, ponieważ stanowią przydatne elementy monitorowania stopnia ochrony w państwach trzecich i organizacjach międzynarodowych.

W art. 49 opartym na art. 46 rozporządzenia (UE) 2016/679 wymaga się, aby w przypadku przekazywania danych do państw trzecich, gdy Komisja nie wydała decyzji stwierdzającej odpowiedni stopień ochrony, wprowadzono odpowiednie zabezpieczenia, w szczególności standardowe klauzule ochrony danych oraz klauzule umowne. Zgodnie z rozporządzeniem (UE) 2016/679 podmioty przetwarzające inne niż instytucje i organy unijne mogą stosować wiążące reguły korporacyjne, kodeksy postępowania i mechanizmy certyfikacji. Ust. 4 przedmiotowego artykułu dotyczący obowiązku instytucji i organów unijnych polegającego na informowaniu EIOD o kategoriach przypadków, w których zastosowały ten artykuł, odpowiada art. 9 ust. 8 rozporządzenia (WE) nr 45/2001 i zostaje zachowany ze względu na swoją specyfikę. Ust. 5 opiera się na zasadzie praw nabytych, obejmującej obowiązujące zezwolenia, określonej w art. 46 ust. 5 rozporządzenia (UE) 2016/679.

W art. 50 doprecyzowuje się zgodnie z art. 48 rozporządzenia (UE) 2016/679, że wyroki sądów lub decyzje organów administracyjnych państw trzecich wymagające przekazania lub ujawnienia danych osobowych mogą zostać uznane lub być wykonywane wyłącznie, gdy opierają się na umowie międzynarodowej, takiej jak umowa o wzajemnej pomocy prawnej, obowiązującej między wzywającym państwem trzecim a Unią, bez uszczerbku dla innych podstaw przekazania na podstawie niniejszego rozdziału.

W art. 51, opierającym się na art. 49 rozporządzenia (UE) 2016/679, przedstawiono i doprecyzowano odstępstwa dotyczące przekazywania danych. Dotyczy to w szczególności przekazywania danych wymaganego i niezbędnego do ochrony istotnego interesu publicznego, na przykład w sytuacji międzynarodowego przekazywania danych, w którym biorą udział organy ds. konkurencji, organy podatkowe lub organy celne, bądź też między służbami odpowiedzialnymi za zabezpieczenie społeczne lub zarządzanie rybołówstwem. Ust. 5 dotyczący obowiązku informowania EIOD o kategoriach przypadków, w których zastosowano odstępstwo w odniesieniu do przekazania danych, odpowiada obowiązującemu obecnie art. 9 ust. 8 rozporządzenia (WE) nr 45/2001.

W art. 52 bazującym na art. 50 rozporządzenia (UE) 2016/679 wyraźnie przewidziano mechanizmy współpracy międzynarodowej na rzecz ochrony danych osobowych między EIOD we współpracy z Komisją i Europejską Radą Ochrony Danych a organami nadzorczymi państw trzecich.

ROZDZIAŁ VI – EUROPEJSKI INSPEKTOR OCHRONY DANYCH

Artykuł 53 opiera się na art. 41 rozporządzenia (WE) nr 45/2001 i dotyczy ustanowienia EIOD.

W art. 54, opierającym się na art. 42 rozporządzenia (WE) nr 45/2001 i na art. 3 decyzji 1247/2002/WE, określono zasady powoływania EIOD przez Parlament Europejski i Radę. Określono w nim również długość kadencji EIOD, która będzie trwać pięć lat.

W art. 55, opierającym się na art. 43 rozporządzenia (WE) nr 45/2001 i na art. 1 decyzji 1247/2002/WE, określono regulacje i ogólne warunki dotyczące wypełnianie obowiązków przez EIOD i jego personel oraz dotyczące zasobów finansowych.

W art. 56, opierającym się na art. 52 rozporządzenia (UE) 2016/679 i art. 44 rozporządzenia (WE) nr 45/2001, doprecyzowano warunki niezależności EIOD, uwzględniając orzecznictwo Trybunału Sprawiedliwości Unii Europejskiej.

W art. 57, opierającym się na art. 45 rozporządzenia (WE) nr 45/2001, ustanowiono wobec EIOD obowiązek zachowania tajemnicy zawodowej w trakcie kadencji i po jej zakończeniu w odniesieniu do informacji poufnych, które EIOD uzyskał w toku wykonywania oficjalnych obowiązków.

W art. 58, opierającym się na art. 57 rozporządzenia (UE) 2016/679 i art. 46 rozporządzenia (WE) nr 45/2001, określono obowiązki EIOD, w tym obowiązek rozpatrywania skarg i prowadzenia postępowań dotyczących tych skarg oraz upowszechniania w społeczeństwie wiedzy o ryzyku, przepisach, zabezpieczeniach i prawach.

W art. 59, opierającym się na art. 58 rozporządzenia (UE) 2016/679 i art. 47 rozporządzenia (WE) nr 45/2001, określono uprawnienia EIOD.

W art. 60 opierającym się na art. 59 rozporządzenia (UE) 2016/679 i art. 48 rozporządzenia (WE) nr 45/2001, określono obowiązek sporządzenia przez EIOD rocznego sprawozdania z działalności.

ROZDZIAŁ VII – WSPÓŁPRACA I SPÓJNOŚĆ

W art. 61, opierającym się na art. 61 rozporządzenia (UE) 2016/679 i art. 46 lit. f) rozporządzenia (WE) nr 45/2001, wprowadza się wyraźne zasady dotyczące współpracy EIOD z krajowymi organami nadzorczymi.

W art. 62 ustanowiono obowiązki EIOD w ramach skoordynowanej współpracy z krajowymi organami nadzorczymi w sytuacjach, w których inne akty unijne odnoszą się do tego artykułu. Celem artykułu jest wdrożenie jednolitego modelu skoordynowanego nadzoru. Tego rodzaju model można by wykorzystać do celów skoordynowanego nadzoru nad dużymi systemami informatycznymi, takimi jak: Eurodac, System Informacyjny Schengen drugiej generacji (SIS II), wizowy system informacyjny, system informacji celnej lub system wymiany informacji na rynku wewnętrzny, a ponadto do celów nadzoru nad niektórymi agencjami unijnymi, takimi jak Europol, w przypadku których obowiązuje szczególny model współpracy między EIOD a organami krajowymi. Europejska Rada Ochrony Danych powinna funkcjonować jako jednolite forum na potrzeby zapewnienia skutecznego i skoordynowanego nadzoru w całej radzie.

ROZDZIAŁ VIII – ŚRODKI OCHRONY PRAWNEJ, ODPOWIEDZIALNOŚĆ I SANKCJE

W art. 63, opierającym się na art. 77 rozporządzenia (UE) 2016/679 i art. 32 rozporządzenia (WE) nr 45/2001, zapewniono prawo osoby, której dane dotyczą, do wniesienia skargi do EIOD. Artykuł ten stanowi, że EIOD ma obowiązek rozpatrzeć skargę i poinformować osobę, której dane dotyczą, o postępach i wynikach rozpatrywania skargi w terminie trzech miesięcy, po upływie którego skargę uznaje się za odrzuconą.

W art. 64 zachowuje się art. 32 ust. 1 rozporządzenia (WE) nr 45/2001 stanowiący, że Trybunał Sprawiedliwości Unii Europejskiej jest właściwy do orzekania we wszystkich sporach odnoszących się do przepisów niniejszego rozporządzenia, włącznie z roszczeniami odszkodowawczymi.

W art. 65 określa się prawo do odszkodowania zarówno w odniesieniu do szkód majątkowych, jak i szkód niemajątkowych, z zastrzeżeniem warunków, w tym warunków dotyczących odpowiedzialności, przewidzianych w Traktatach.

W art. 66, opierającym się na art. 83 rozporządzenia (UE) 2016/679, przyznano EIOD uprawnienie do nakładania administracyjnych kar pieniężnych na instytucje i organy unijne jako ostateczną karę i wyłącznie wówczas, gdy instytucja unijna lub organ unijny nie zastosuje się do nakazu wydanego przez EIOD, o którym mowa wart. 59 ust. 2 lit. a)–h) i j). W artykule tym określa się również kryteria, na podstawie których ustalona zostaje kwota administracyjnej kary pieniężnej w każdym pojedynczym przypadku, przy czym maksymalne roczne pułapy zostały przyjęte na podstawie wysokości kar stosowanych w niektórych państwach członkowskich.

W art. 67 dopuszcza się, zgodnie z art. 80 ust. 1 rozporządzenia (UE) 2016/679, możliwość wniesienia skargi w imieniu osoby, której dane dotyczą, przez określone organy, organizacje lub zrzeszenia.

W art. 68, zgodnie z art. 33 rozporządzenia (WE) nr 45/2001, określa się szczegółowe zasady, których celem jest ochrona pracowników unijnych, którzy wnoszą skargę do EIOD, dotyczącą domniemanego naruszenia przepisów niniejszego rozporządzenia, bez użycia oficjalnych dróg.

W art. 69, opierającym się na art. 49 rozporządzenia (WE) nr 45/2001, przewidziano kary stosowane w związku z niedopełnieniem obowiązków wynikających z niniejszego rozporządzenia przez urzędników lub innych funkcjonariuszy Unii Europejskiej.

ROZDZIAŁ IX – AKTY WYKONAWCZE

Artykuł 70 dotyczy procedury komitetowej niezbędnej do powierzenia Komisji uprawnień wykonawczych w przypadkach, w których zgodnie z art. 291 TFUE konieczne są jednolite warunki wykonywania prawnie wiążących aktów Unii. Zastosowanie ma procedura sprawdzająca.

ROZDZIAŁ X – PRZEPISY KOŃCOWE

W art. 71 uchyla się rozporządzenie (WE) nr 45/2001 i decyzję nr 1247/2002/WE i stanowi się, że odesłania do tych dwóch instrumentów należy traktować jako odesłania do niniejszego rozporządzenia.

W art. 72 wyjaśnia się, że niniejsze rozporządzenie nie wpływa na obecną kadencję Europejskiego Inspektora Ochrony Danych i zastępcy inspektora, a art. 54 ust. 4, 5 i 7 oraz art. 56 i 57 niniejszego rozporządzenia mają zastosowanie do obecnego zastępcy inspektora do końca jego kadencji, tj. do dnia 5 grudnia 2019 r.

W art. 73 określa się dzień 25 maja 2018 r. jako datę wejścia w życie niniejszego rozporządzenia celem zapewnienia spójności z datą rozpoczęcia stosowania rozporządzenia (UE) 2016/679.

2017/0002 (COD)

Wniosek

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY

dotyczący ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez unijne instytucje, organy i jednostki organizacyjne oraz swobodnego przepływu takich danych i uchylający rozporządzenie (WE) nr 45/2001 i decyzję nr 1247/2002/WE

PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 16 ust. 2,

uwzględniając wniosek Komisji Europejskiej,

po przekazaniu projektu aktu ustawodawczego parlamentom narodowym,

uwzględniając opinię Europejskiego Komitetu Ekonomiczno-Społecznego[10],

[10] Dz.U. C […] z […], s. […].

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą,

a także mając na uwadze, co następuje:

(1) Ochrona osób fizycznych w związku z przetwarzaniem danych osobowych jest jednym z praw podstawowych. Art. 8 ust. 1 Karty praw podstawowych Unii Europejskiej (zwanej dalej „Kartą praw podstawowych") oraz art. 16 ust. 1 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE) stanowią, że każda osoba ma prawo do ochrony danych osobowych jej dotyczących.

(2) W rozporządzeniu (WE) nr 45/2001 Parlamentu Europejskiego i Rady[11] zapewnia się osobom fizycznym prawa możliwe do wyegzekwowania na drodze prawnej, określa się zobowiązania administratorów w instytucjach i organach unijnych odnoszące się do przetwarzania danych osobowych oraz tworzy się niezależny organ nadzorczy – Europejskiego Inspektora Ochrony Danych – odpowiedzialny za monitorowanie przetwarzania danych osobowych przez instytucje i organy unijne. Rozporządzenie nie ma jednak zastosowania do przetwarzania danych osobowych w toku prowadzenia przez instytucje i organy unijne działalności nieobjętej zakresem stosowania prawa Unii.

(3) W dniu 27 kwietnia 2016 r. przyjęto rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679[12] i dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/680[13]. W powyższym rozporządzeniu określa się przepisy ogólne dotyczące ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i zapewnienia swobodnego przepływu danych osobowych w Unii, natomiast w powyższej dyrektywie określa się przepisy szczegółowe dotyczące ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i zapewnienia swobodnego przepływu danych osobowych w Unii w dziedzinach współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej.

(4) W rozporządzeniu (UE) 2016/679 podkreślono, że aby zapewnić solidne i spójne ramy ochrony danych w Unii, należy dokonać koniecznych modyfikacji rozporządzenia (WE) nr 45/2001, tak by umożliwić jego stosowanie równocześnie z rozporządzeniem (UE) 2016/679.

(5) W myśl spójnego podejścia do ochrony danych osobowych w całej Unii oraz swobodnego przepływu danych osobowych na terytorium Unii należy w miarę możliwości dostosować przepisy o ochronie danych dotyczące instytucji i organów unijnych z przepisami o ochronie danych przyjętymi w odniesieniu do sektora

---

11 Rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych (Dz.U. L 8 z 12.1.2001, s. 1).

12 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Tekst mający znaczenie dla EOG), Dz.U. L 119 z 4.5.2016, s. 1–88.

13 Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW, Dz.U. L 119 z 4.5.2016, s. 89–131.

publicznego w państwach członkowskich. W każdym przypadku, w którym przepisy niniejszego rozporządzenia opierają się na tym samym założeniu, co przepisy rozporządzenia (UE) 2016/679, oba przepisy należy interpretować tak samo, w szczególności ze względu na fakt, że systematyka niniejszego rozporządzenia powinna być uznawana za tożsamą z systematyką rozporządzenia (UE) 2016/679.

(6) Należy zapewnić ochronę wszystkim osobom, których dane osobowe są przetwarzane przez instytucje i organy unijne, niezależnie od powodu takiego przetwarzania, którym może być fakt zatrudnienia takich osób przez instytucje i organy unijne. Niniejszego rozporządzenia nie ma zastosowania do przetwarzania danych osobowych osób zmarłych. Niniejsze rozporządzenie nie dotyczy przetwarzania danych osobowych dotyczących osób prawnych, w szczególności przedsiębiorstw będących osobami prawnymi, w tym danych o firmie i formie prawnej oraz danych kontaktowych osoby prawnej.

(7) Aby zapobiec poważnemu ryzyku obchodzenia prawa, ochrona osób fizycznych powinna być neutralna pod względem technicznym i nie powinna zależeć od stosowanych technik. Ochrona osób fizycznych powinna mieć zastosowanie do zautomatyzowanego przetwarzania danych osobowych oraz do przetwarzania ręcznego, jeżeli dane osobowe znajdują się lub mają się znaleźć w zbiorze danych. Zbiory lub zestawy zbiorów oraz ich strony tytułowe, które nie są uporządkowane według określonych kryteriów, nie powinny być objęte zakresem niniejszego rozporządzenia.

(8) W deklaracji nr 21 w sprawie ochrony danych osobowych w dziedzinie współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej – załączonej do Aktu końcowego konferencji międzyrządowej, która przyjęła Traktat z Lizbony – konferencja uznała, że ze względu na szczególny charakter współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej konieczne może okazać się przyjęcie – na podstawie art. 16 TFUE – szczególnych przepisów o ochronie danych osobowych i swobodnym przepływie danych osobowych w tych dziedzinach. Niniejsze rozporządzenie powinno zatem mieć zastosowanie do agencji unijnych prowadzących działania w ramach współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej wyłącznie w zakresie, w jakim prawo Unii właściwe dla tego rodzaju agencji nie zawiera przepisów szczegółowych dotyczących przetwarzania danych osobowych.

(9) Dyrektywa (UE) 2016/680 zawiera zharmonizowane zasady ochrony i swobodnego przepływu danych osobowych przetwarzanych do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar, w tym do celów ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom. Aby zapewnić identyczny stopień ochrony osób fizycznych w Unii za pomocą praw możliwych do wyegzekwowania na drodze prawnej, oraz zapobiegać rozbieżnościom utrudniającym wymianę danych osobowych między agencjami unijnymi prowadzącymi działania w ramach współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej a właściwymi organami w państwach członkowskich, przepisy dotyczące ochrony i swobodnego przepływu operacyjnych danych osobowych przetwarzanych przez tego rodzaju agencje unijne powinny opierać się na zasadach leżących u podstaw niniejszego rozporządzenia i powinny być spójne z dyrektywą (UE) 2016/680.

(10) Jeżeli w akcie ustanawiającym agencję unijną prowadzącą działania wchodzące w zakres stosowania tytułu V rozdziały 4 i 5 Traktatu ustanawia się niezależny system ochrony danych do celów przetwarzania operacyjnych danych osobowych, niniejsze rozporządzenie nie powinno mieć wpływu na tego rodzaju systemy. Zgodnie z art. 62 dyrektywy (UE) 2016/680 Komisja powinna jednak do dnia 6 maja 2019 r. przeprowadzić przegląd aktów unijnych regulujących przetwarzanie danych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w tym do celów ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom, i w stosownych przypadkach przedstawić niezbędne wnioski dotyczące zmiany aktów w celu zapewnienia spójnego podejścia do ochrony danych osobowych w ramach współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej.

(11) Zasady ochrony danych powinny mieć zastosowanie do wszelkich informacji o zidentyfikowanych lub możliwych do zidentyfikowania osobach fizycznych. Spseudonimizowane dane osobowe, które przy użyciu dodatkowych informacji można przypisać osobie fizycznej, należy uznać za informacje o możliwej do zidentyfikowania osobie fizycznej. Aby stwierdzić, czy dana osoba fizyczna jest możliwa do zidentyfikowania, należy wziąć pod uwagę wszelkie sposoby (w tym wyodrębnienie wpisów dotyczących tej samej osoby), w stosunku do których istnieje uzasadnione prawdopodobieństwo, iż zostaną wykorzystane przez administratora lub inną osobę w celu bezpośredniego lub pośredniego zidentyfikowania osoby fizycznej. Aby stwierdzić, czy dany sposób może być z uzasadnionym prawdopodobieństwem wykorzystany do zidentyfikowania danej osoby fizycznej, należy wziąć pod uwagę wszelkie obiektywne czynniki, takie jak koszt i czas potrzebne do jej zidentyfikowania, oraz uwzględnić technologię dostępną w momencie przetwarzania danych, jak i postęp technologiczny. Zasady ochrony danych nie powinny więc mieć zastosowania do informacji anonimowych, czyli informacji, które nie wiążą się ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną, ani do danych osobowych zanonimizowanych w taki sposób, że osób, których dane dotyczą, w ogóle nie można zidentyfikować lub już nie można zidentyfikować. Niniejsze rozporządzenie nie dotyczy więc przetwarzania anonimowych informacji, w tym przetwarzania do celów statystycznych lub naukowych.

(12) Pseudonimizacja danych osobowych może ograniczyć ryzyko dla osób, których dane dotyczą, oraz pomóc administratorom i podmiotom przetwarzającym wywiązać się z obowiązku ochrony danych. Bezpośrednie wprowadzenie pojęcia „pseudonimizacja” w niniejszym rozporządzeniu nie służy wykluczeniu innych środków ochrony danych.

(13) Osobom fizycznym mogą zostać przypisane identyfikatory internetowe – takie jak adresy IP, identyfikatory plików cookie – generowane przez ich urządzenia, aplikacje, narzędzia i protokoły, czy też inne identyfikatory, generowane na przykład przez etykiety RFID. Może to skutkować zostawianiem śladów, które w szczególności w połączeniu z niepowtarzalnymi identyfikatorami i innymi informacjami uzyskiwanymi przez serwery mogą być wykorzystywane do tworzenia profili i do identyfikowania tych osób.

(14) Zgoda powinna być wyrażona w drodze jednoznacznej, potwierdzającej czynności, która wyraża odnoszące się do określonej sytuacji dobrowolne, świadome i jednoznaczne przyzwolenie osoby, której dane dotyczą, na przetwarzanie dotyczących

jej danych osobowych i która ma na przykład formę pisemnego (w tym elektronicznego) lub ustnego oświadczenia. Może to polegać na zaznaczeniu okienka wyboru podczas przeglądania strony internetowej, na wyborze ustawień technicznych do korzystania z usług społeczeństwa informacyjnego lub też na innym oświadczeniu bądź zachowaniu, które w danym kontekście jasno wskazuje, że osoba, której dane dotyczą, zaakceptowała proponowane przetwarzanie jej danych osobowych. Milczenie, okienka domyślnie zaznaczone lub niepodjęcie działania nie powinny zatem oznaczać zgody. Zgoda powinna dotyczyć wszystkich czynności przetwarzania dokonywanych w tym samym celu lub w tych samych celach. Jeżeli przetwarzanie służy różnym celom, potrzebna jest zgoda na wszystkie te cele. Jeżeli osoba, której dane dotyczą, ma wyrazić zgodę w odpowiedzi na elektroniczne zapytanie, zapytanie takie musi być jasne, zwięzłe i nie zakłócać niepotrzebnie korzystania z usługi, której dotyczy.

(15) Wszelkie przetwarzanie danych osobowych powinno być zgodne z prawem i rzetelne. Dla osób fizycznych powinno być jasne, że dotyczące ich dane osobowe są zbierane, wykorzystywane, przeglądane lub w inny sposób przetwarzane oraz w jakim stopniu te dane osobowe są lub będą przetwarzane. Zasada przejrzystości wymaga, by wszelkie informacje i wszelkie komunikaty związane z przetwarzaniem tych danych osobowych były łatwo dostępne i zrozumiałe oraz sformułowane jasnym i prostym językiem. Zasada ta dotyczy w szczególności informowania osób, których dane dotyczą, o tożsamości administratora i celach przetwarzania oraz innych informacji mających zapewnić rzetelność i przejrzystość przetwarzania w stosunku do osób fizycznych, których sprawa dotyczy, a także prawa takich osób do uzyskania potwierdzenia i informacji o przetwarzanych danych osobowych ich dotyczących. Osobom fizycznym należy uświadomić ryzyka, zasady, zabezpieczenia i prawa związane z przetwarzaniem danych osobowych oraz sposoby wykonywania praw przysługujących im w związku z takim przetwarzaniem. W szczególności konkretne cele przetwarzania danych osobowych powinny być wyraźne, uzasadnione i określone w momencie ich zbierania. Dane osobowe powinny być adekwatne, stosowne i ograniczone do tego, co niezbędne do celów, dla których są one przetwarzane. Wymaga to w szczególności zapewnienia ograniczenia okresu przechowywania danych do ścisłego minimum. Dane osobowe powinny być przetwarzane tylko w przypadkach, gdy celu przetwarzania nie można w rozsądny sposób osiągnąć innymi sposobami. Aby zapobiec przechowywaniu danych osobowych przez okres dłuższy, niż jest to niezbędne, administrator powinien ustalić termin ich usuwania lub okresowego przeglądu. Należy podjąć wszelkie rozsądne działania zapewniające sprostowanie lub usunięcie danych osobowych, które są nieprawidłowe. Dane osobowe powinny być przetwarzane w sposób zapewniający im odpowiednie bezpieczeństwo i odpowiednią poufność, w tym ochronę przed nieuprawnionym dostępem do nich i do sprzętu służącego ich przetwarzaniu lub przed nieuprawnionym korzystaniem z tych danych i z tego sprzętu.

(16) Zgodnie z zasadą rozliczalności, jeżeli instytucje i organy unijne przekazują dane osobowe w obrębie danej instytucji lub danego organu lub do innych instytucji i organów unijnych, powinny sprawdzić, czy tego rodzaju dane osobowe są niezbędne do zgodnego z prawem wykonywania zadań leżących w zakresie kompetencji odbiorcy, jeżeli odbiorca nie należy do struktur administratora. W szczególności po otrzymaniu wniosku od odbiorcy o przekazanie danych osobowych administrator powinien sprawdzić, czy istnieje odpowiednia podstawa do stwierdzenia zgodności z prawem przetwarzania przez niego danych osobowych, których dotyczy wniosek, oraz

powinien sprawdzić uprawnienia odbiorcy i dokonać wstępnej oceny konieczności przekazania danych. Jeżeli powstają wątpliwości co do tej konieczności, administrator powinien żądać dalszych informacji od odbiorcy. Odbiorca powinien zapewnić możliwość zweryfikowania konieczności przekazania danych po jego dokonaniu.

(17) Aby przetwarzanie danych osobowych było zgodne z prawem, musi ono być podyktowane koniecznością wykonania zadania realizowanego w interesie publicznym przez instytucje i organy unijne lub w ramach sprawowania przez nie władzy publicznej, koniecznością poszanowania obowiązku prawnego, któremu podlega administrator, lub inną uzasadnioną podstawą, o której mowa w niniejszym rozporządzeniu, w tym zgodą osoby, której dane dotyczą, lub koniecznością poszanowania umowy, której stroną jest osoba, której dane dotyczą, lub w celu podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy. Przetwarzanie danych osobowych w celu przeprowadzenia czynności wykonywanych w interesie ogólnym przez instytucje i organy unijne obejmuje przetwarzanie danych osobowych niezbędnych do zarządzania i funkcjonowania tych instytucji i organów. Przetwarzanie danych osobowych należy uznać za zgodne z prawem również w przypadkach, gdy jest niezbędne do ochrony interesu, który ma istotne znaczenie dla życia osoby, której dane dotyczą, lub innej osoby fizycznej. Żywotny interes innej osoby fizycznej powinien zasadniczo być podstawą przetwarzania danych osobowych wyłącznie w przypadkach, gdy ewidentnie przetwarzania tego nie da się oprzeć na innej podstawie prawnej. Niektóre rodzaje przetwarzania mogą służyć zarówno ważnemu interesowi publicznemu, jak i żywotnym interesom osoby, której dane dotyczą, na przykład gdy przetwarzanie jest niezbędne do celów humanitarnych, w tym monitorowania epidemii i ich rozprzestrzeniania się lub w nadzwyczajnych sytuacjach humanitarnych, w szczególności w przypadku klęsk żywiołowych i katastrof spowodowanych przez człowieka.

(18) Prawo Unii obejmujące wewnętrzne przepisy, o których mowa w niniejszym rozporządzeniu, powinno być jasne i precyzyjne, a jego zastosowanie przewidywalne dla osób im podlegających – jak wymaga tego orzecznictwo Trybunału Sprawiedliwości Unii Europejskiej i Europejskiego Trybunału Praw Człowieka.

(19) Przetwarzanie danych osobowych do celów innych niż cele, w których dane te zostały pierwotnie zebrane, powinno być dozwolone wyłącznie w przypadkach, gdy jest zgodne z celami, w których dane osobowe zostały pierwotnie zebrane. W takim przypadku nie jest wymagana odrębna podstawa prawna inna niż podstawa prawna, która umożliwiła zebranie danych osobowych. Jeżeli przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi, prawo Unii może określać i precyzować zadania i cele, dla których dalsze przetwarzanie powinno być uznawane za zgodne z prawem i z pierwotnymi celami. Dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych powinny być uznawane za operacje przetwarzania zgodne z prawem i z pierwotnymi celami. Podstawa prawna przetwarzania danych osobowych przewidziana prawem Unii może być również podstawą prawną dalszego przetwarzania. Aby ustalić, czy cel dalszego przetwarzania danych osobowych jest zgodny z celem, w którym dane te zostały pierwotnie zebrane, administrator – po spełnieniu wszystkich wymogów warunkujących zgodność pierwotnego przetwarzania z prawem – powinien uwzględnić między innymi: wszelkie powiązania pomiędzy tymi celami a celami zamierzonego dalszego przetwarzania; kontekst, w którym dane

osobowe zostały zebrane, w szczególności rozsądne przesłanki pozwalające osobom, których dane dotyczą, oczekiwać dalszego wykorzystania danych, oparte na rodzaju ich powiązania z administratorem; charakter danych osobowych; konsekwencje zamierzonego dalszego przetwarzania dla osób, których dane dotyczą; oraz istnienie odpowiednich zabezpieczeń zarówno podczas pierwotnej, jak i zamierzonej operacji dalszego przetwarzania

(20) Jeśli przetwarzanie odbywa się na podstawie zgody osoby, której dane dotyczą, administrator powinien być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na operację przetwarzania. W szczególności w przypadku pisemnego oświadczenia składanego w innej sprawie powinny istnieć gwarancje, że osoba, której dane dotyczą, jest świadoma wyrażenia zgody oraz jej zakresu. Zgodnie z dyrektywą Rady 93/13/EWG[14] oświadczenie o wyrażeniu zgody przygotowane przez administratora powinno mieć zrozumiałą i łatwo dostępną formę, być sformułowane jasnym i prostym językiem i nie powinno zawierać nieuczciwych warunków. Aby wyrażenie zgody było świadome, osoba, której dane dotyczą, powinna znać przynajmniej tożsamość administratora oraz zamierzone cele przetwarzania danych osobowych. Wyrażenia zgody nie należy uznawać za dobrowolne, jeżeli osoba, której dane dotyczą, nie ma rzeczywistego lub wolnego wyboru oraz nie może odmówić ani wycofać zgody bez niekorzystnych konsekwencji.

(21) Szczególnej ochrony danych osobowych wymagają dzieci, gdyż mogą one być mniej świadome ryzyka, konsekwencji, zabezpieczeń i praw przysługujących im w związku z przetwarzaniem danych osobowych. Taka szczególna ochrona powinna mieć zastosowanie przede wszystkim do tworzenia profili osobowych i do zbierania danych osobowych dotyczących dzieci, gdy korzystają one z kierowanych bezpośrednio do nich usług, które są oferowane na stronach internetowych instytucji i organów unijnych, na przykład z usług komunikacji interpersonalnej lub internetowej sprzedaży biletów, oraz gdy przetwarzanie danych osobowych odbywa się za zgodą.

(22) Jeżeli odbiorcy posiadający jednostki organizacyjne w Unii i podlegający rozporządzeniu (UE) 2016/679 lub dyrektywie (UE) 2016/680 pragną, aby instytucje i organy unijne przekazywały im dane osobowe, powinni oni wykazać, że takie przekazywanie jest konieczne do osiągnięcia celu tych odbiorców oraz że jest proporcjonalne i nie wykracza poza zakres konieczny do osiągnięcia tego celu. Instytucje i organy unijne powinny wykazać taką konieczność, jeżeli same inicjują przekazywanie, zgodnie z zasadą przejrzystości.

(23) Dane osobowe, które z racji swego charakteru są szczególnie wrażliwe w świetle podstawowych praw i wolności, wymagają szczególnej ochrony, gdyż kontekst ich przetwarzania może powodować poważne ryzyko dla podstawowych praw i wolności. Do takich danych osobowych powinny zaliczać się dane osobowe ujawniające pochodzenie rasowe lub etniczne, przy czym użycie w niniejszym rozporządzeniu terminu „pochodzenie rasowe” nie oznacza, że Unia akceptuje teorie sugerujące istnienie odrębnych ras ludzkich. Przetwarzanie fotografii nie powinno zawsze stanowić przetwarzania szczególnych kategorii danych osobowych, gdyż fotografie są objęte definicją „danych biometrycznych” tylko w przypadkach, gdy są przetwarzane

[14] Dyrektywa Rady 93/13/EWG z dnia 5 kwietnia 1993 r. w sprawie nieuczciwych warunków w umowach konsumenckich (Dz.U. L 95 z 21.4.1993, s. 29).

specjalnymi metodami technicznymi, umożliwiającymi jednoznaczną identyfikację osoby fizycznej lub potwierdzenie jej tożsamości. Oprócz wymogów szczegółowych mających zastosowanie do przetwarzania danych wrażliwych zastosowanie powinny mieć zasady ogólne i inne przepisy niniejszego rozporządzenia, w szczególności jeżeli chodzi o warunki zgodności przetwarzania z prawem. Należy wyraźnie przewidzieć wyjątki od ogólnego zakazu przetwarzania takich szczególnych kategorii danych osobowych, m.in. w razie wyraźnej zgody osoby, której dane dotyczą, lub ze względu na szczególne potrzeby, w szczególności gdy przetwarzanie danych odbywa się w ramach uzasadnionych działań niektórych zrzeszeń lub fundacji, których celem jest umożliwienie korzystania z podstawowych wolności.

(24) Niezbędne z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego może być przetwarzanie szczególnych kategorii danych osobowych bez zgody osoby, której dane dotyczą. Przetwarzanie takie powinno podlegać konkretnym, odpowiednim środkom chroniącym prawa i wolności osób fizycznych. W tym kontekście „zdrowie publiczne" należy interpretować zgodnie z definicją z rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 1338/2008[15], czyli jako wszystkie elementy związane ze zdrowiem, mianowicie stan zdrowia, w tym zachorowalność i niepełnosprawność, czynniki warunkujące stan zdrowia, potrzeby w zakresie opieki zdrowotnej, zasoby opieki zdrowotnej, oferowane usługi opieki zdrowotnej i powszechny dostęp do nich, wydatki na opiekę zdrowotną i sposób jej finansowania oraz przyczyny zgonów. Przetwarzanie danych dotyczących zdrowia z uwagi na względy interesu publicznego nie powinno skutkować przetwarzaniem danych osobowych do innych celów przez osoby trzecie.

(25) Jeżeli dane osobowe przetwarzane przez administratora nie pozwalają mu zidentyfikować osoby fizycznej, nie powinien on mieć obowiązku uzyskania dodatkowych informacji w celu zidentyfikowania osoby, której dane dotyczą, wyłącznie po to, by zastosować się do przepisów niniejszego rozporządzenia. Administrator nie powinien jednak odmawiać przyjęcia dodatkowych informacji od osoby, której dane dotyczą, by ułatwić jej wykonywanie praw. Weryfikacja tożsamości powinna obejmować cyfrową identyfikację osoby, której dane dotyczą, na przykład poprzez mechanizm uwierzytelniania, taki jak te same dane uwierzytelniające, których osoba, której dane dotyczą, używa, by zalogować się do usług internetowych oferowanych przez administratora danych.

(26) Przetwarzanie danych osobowych do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych powinno podlegać odpowiednim zabezpieczeniom praw i wolności osoby, której dane dotyczą, zgodnie z niniejszym rozporządzeniem. Zabezpieczenia te powinny polegać na wdrożeniu środków technicznych i organizacyjnych zapewniających w szczególności poszanowanie zasady minimalizacji danych. Dalsze przetwarzanie danych osobowych do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych można prowadzić, jeżeli administrator ocenił, czy celów tych nie można osiągnąć przetwarzaniem danych osobowych, które albo od początku albo już dłużej nie pozwalają identyfikować osób, których dane

[15] Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 1338/2008 z dnia 16 grudnia 2008 r. w sprawie statystyk Wspólnoty w zakresie zdrowia publicznego oraz zdrowia i bezpieczeństwa w pracy (Dz.U. L 354 z 31.12.2008, s. 70).

dotyczą, pod warunkiem że istnieją odpowiednie zabezpieczenia (takie jak pseudonimizacja danych osobowych). Instytucje i organy unijne powinny ustanowić odpowiednie zabezpieczenia w odniesieniu do przetwarzania danych osobowych do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych przewidzianych w prawie Unii, które może obejmować wewnętrzne przepisy.

(27) Należy przewidzieć procedury ułatwiające osobie, której dane dotyczą, wykonywanie praw przysługujących jej na mocy niniejszego rozporządzenia, w tym mechanizmy żądania – i gdy ma to zastosowanie bezpłatnego uzyskiwania – w szczególności dostępu do danych osobowych i ich sprostowania lub usunięcia oraz możliwości wykonywania prawa do sprzeciwu. Administrator powinien zapewnić możliwość wnoszenia odnośnych żądań także drogą elektroniczną, w szczególności gdy dane osobowe są przetwarzane drogą elektroniczną. Administrator powinien być zobowiązany udzielić odpowiedzi na żądania osób, których dane dotyczą, bez zbędnej zwłoki – najpóźniej w terminie miesiąca, a jeżeli nie zamierza spełnić takiego żądania – podać tego przyczyny.

(28) Zasady rzetelnego i przejrzystego przetwarzania wymagają, by osoba, której dane dotyczą, była informowana o prowadzeniu operacji przetwarzania i o jej celach. Administrator powinien podać osobie, której dane dotyczą, wszelkie inne informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania, uwzględniając konkretne okoliczności i konkretny kontekst przetwarzania danych osobowych. Ponadto należy poinformować osobę, której dane dotyczą, o fakcie profilowania oraz o konsekwencjach takiego profilowania. Jeżeli gromadzi się dane osobowe od osoby, której dane dotyczą, należy ją też poinformować, czy ma ona obowiązek je podać, oraz o konsekwencjach ich niepodania. Informacje te można przekazać w połączeniu ze standardowymi znakami graficznymi, które w widoczny, zrozumiały i czytelny sposób przedstawią sens zamierzonego przetwarzania. Jeżeli znaki te są przedstawione elektronicznie, powinny nadawać się do odczytu maszynowego.

(29) Informacje o przetwarzaniu danych osobowych dotyczących osoby, której dane dotyczą, należy przekazać tej osobie w momencie zbierania danych, a jeżeli danych nie uzyskuje się od osoby, której dane dotyczą, lecz z innego źródła – w rozsądnym terminie, zależnie od okoliczności. Jeżeli dane osobowe można zgodnie z prawem ujawnić innemu odbiorcy, należy poinformować o tym osobę, której dane dotyczą, w momencie pierwszorazowego ujawnienia danych temu odbiorcy. Jeżeli administrator planuje przetwarzać dane osobowe w celu innym niż cel, w których dane osobowe zostały zebrane, powinien on przed takim dalszym przetwarzaniem poinformować osobę, której dane dotyczą, o tym innym celu oraz dostarczyć jej innych niezbędnych informacji. Jeżeli osobie, której dane dotyczą, nie można podać pochodzenia danych osobowych, ponieważ korzystano z różnych źródeł, informacje należy przedstawić w sposób ogólny.

(30) Każda osoba fizyczna powinna mieć prawo dostępu do zebranych danych jej dotyczących oraz powinna mieć możliwość łatwego wykonywania tego prawa w rozsądnych odstępach czasu, by mieć świadomość przetwarzania i móc zweryfikować zgodność przetwarzania z prawem. Obejmuje to prawo dostępu osób, których dane dotyczą, do danych dotyczących ich zdrowia, na przykład do danych w dokumentacji medycznej zawierającej takie informacje, jak diagnoza, wyniki badań, oceny dokonywane przez lekarzy prowadzących, stosowane terapie czy przeprowadzone

zabiegi. Dlatego też każda osoba, której dane dotyczą, powinna mieć prawo do wiedzy i informacji, w szczególności w zakresie celów, w jakich dane osobowe są przetwarzane, w miarę możliwości okresu, przez jaki dane osobowe są przetwarzane, odbiorców danych osobowych, założeń ewentualnego zautomatyzowanego przetwarzania danych osobowych oraz, przynajmniej w przypadku profilowania, konsekwencji takiego przetwarzania. Prawo to nie powinno negatywnie wpływać na prawa lub wolności innych osób, w tym tajemnice handlowe lub własność intelektualną, w szczególności na prawa autorskie chroniące oprogramowanie. Względy te nie powinny jednak skutkować odmową udzielenia osobie, której dane dotyczą, jakichkolwiek informacji. Jeżeli administrator przetwarza duże ilości informacji o osobie, której dane dotyczą, powinien on mieć możliwość zażądania, przed podaniem informacji, by osoba, której dane dotyczą, sprecyzowała informacje lub czynności przetwarzania, których dotyczy jej żądanie.

(31) Każda osoba fizyczna powinna mieć prawo do sprostowania danych osobowych jej dotyczących oraz prawo do „bycia zapomnianym", jeżeli zatrzymywanie takich danych narusza niniejsze rozporządzenie lub prawo Unii, któremu podlega administrator. Osoba, której dane dotyczą, powinna mieć prawo do tego, by jej dane osobowe zostały usunięte i przestały być przetwarzane, jeżeli dane te nie są już niezbędne do celów, w których były zbierane lub w inny sposób przetwarzane, jeżeli osoba, której dane dotyczą, cofnęła zgodę lub jeżeli wniosła sprzeciw wobec przetwarzania danych osobowych jej dotyczących, lub jeżeli przetwarzanie jej danych osobowych nie jest z innego powodu zgodne z niniejszym rozporządzeniem. Prawo to ma znaczenie w przypadkach, gdy osoba, której dane dotyczą, wyraziła zgodę jako dziecko, gdy nie była w pełni świadoma ryzyka związanego z przetwarzaniem, a w późniejszym czasie chce usunąć takie dane osobowe, w szczególności z internetu. Osoba, której dane dotyczą, powinna móc wykonywać to prawo, mimo że już nie jest dzieckiem. Dalsze zatrzymywanie danych osobowych powinno być jednak uznane za zgodne z prawem, jeżeli jest niezbędne do korzystania z wolności wypowiedzi i informacji, do wywiązania się z obowiązku prawnego, do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi, z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego, do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych lub do ustalenia, dochodzenia lub obrony roszczeń.

(32) Aby wzmocnić prawo do „bycia zapomnianym" w internecie, należy rozszerzyć prawo do usunięcia danych poprzez zobowiązanie administratora, który upublicznił te dane osobowe, do poinformowania administratorów, którzy przetwarzają takie dane osobowe o tym, że należy usunąć wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje. Spełniając ten obowiązek administrator powinien podjąć racjonalne działania z uwzględnieniem dostępnych technologii i dostępnych mu środków, w tym dostępnych środków technicznych, w celu poinformowania administratorów, którzy przetwarzają dane osobowe, o żądaniu osoby, której dane dotyczą.

(33) Wśród metod pozwalających ograniczyć przetwarzanie danych osobowych mogą się znaleźć między innymi: czasowe przeniesienie wybranych danych osobowych do innego systemu przetwarzania, uniemożliwienie użytkownikom dostępu do wybranych danych, lub czasowe usunięcie opublikowanych danych ze strony internetowej. W zautomatyzowanych zbiorach danych przetwarzanie należy zasadniczo ograniczyć

środkami technicznymi w taki sposób, by dane osobowe nie podlegały dalszemu przetwarzaniu ani nie mogły być zmieniane. Fakt ograniczenia przetwarzania danych osobowych należy wyraźnie zaznaczyć w systemie.

(34) Aby zyskać większą kontrolę nad swoimi danymi w ramach zautomatyzowanego przetwarzania danych osobowych, osoba, której dane dotyczą, powinna także mieć możliwość otrzymywania dotyczących jej danych osobowych, których dostarczyła administratorowi, w ustrukturyzowanym, powszechnie używanym, nadającym się do odczytu maszynowego i interoperacyjnym formacie oraz przesyłania ich innemu administratorowi. Administratorów danych należy zachęcać do opracowywania interoperacyjnych formatów, które umożliwiają przenoszenie danych. Prawo to powinno mieć zastosowanie w przypadkach, gdy osoba, której dane dotyczą, przekazała dane osobowe na podstawie własnej zgody lub gdy przetwarzanie jest niezbędne do wykonania umowy. Dlatego nie powinno ono mieć zastosowania w przypadkach, gdy przetwarzanie danych osobowych jest niezbędne do wywiązania się z obowiązku prawnego, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi. Przysługujące osobie, której dane dotyczą, prawo do przesłania lub otrzymania swoich danych osobowych nie powinno nakładać na administratorów obowiązku prowadzenia lub wprowadzenia kompatybilnych technicznie systemów przetwarzania. Jeżeli określony zestaw danych osobowych odnosi się do więcej niż jednej osoby, której dane dotyczą, prawo do otrzymania danych osobowych nie powinno powodować uszczerbku dla praw i wolności innych osób, których dane dotyczą, na podstawie niniejszego rozporządzenia. Prawo to powinno ponadto pozostawać bez uszczerbku dla prawa osoby, której dane dotyczą, do spowodowania, by dane osobowe zostały usunięte, oraz bez uszczerbku dla ograniczeń tego prawa określonych w niniejszym rozporządzeniu i nie powinno w szczególności skutkować usunięciem danych osobowych dotyczących osoby, której dane dotyczą, które osoba ta przekazała do celów wykonania umowy, o ile i w takim zakresie, w jakim te dane osobowe są niezbędne do wykonania tej umowy. O ile jest to technicznie możliwe, osoba, której dane dotyczą, powinna mieć prawo do spowodowania, by dane osobowe zostały przesłane przez jednego administratora bezpośrednio innemu administratorowi.

(35) Nawet jeżeli dane osobowe mogą być przetwarzane zgodnie z prawem, gdy przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi, każdej osobie, której dane dotyczą, powinno przysługiwać prawo sprzeciwu wobec przetwarzania danych osobowych dotyczących jej szczególnej sytuacji. Za wykazanie, że ważne prawnie uzasadnione interesy administratora mają nadrzędny charakter wobec interesów lub podstawowych praw i wolności osoby, której dane dotyczą, powinien odpowiadać administrator.

(36) Osoba, której dane dotyczą, powinna mieć prawo do tego, by nie podlegać decyzji – mogącej obejmować określone środki – w której analizuje się cechy osobiste tej osoby i która to decyzja opiera się wyłącznie na przetwarzaniu zautomatyzowanym i wywołuje wobec osoby, której dane dotyczą, skutki prawne lub w podobny sposób znacząco na nią wpływa, jak na przykład elektroniczne metody rekrutacji bez interwencji ludzkiej. Do takiego przetwarzania zalicza się „profilowanie” – które polega na dowolnym zautomatyzowanym przetwarzaniu danych osobowych pozwalającym ocenić czynniki osobowe osoby fizycznej, a w szczególności

analizować lub prognozować aspekty dotyczące efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się osoby, której dane dotyczą – o ile wywołuje skutki prawne względem tej osoby lub w podobny sposób znacząco na nią wpływa. Niemniej podejmowanie decyzji na podstawie takiego przetwarzania, w tym profilowania, powinno być dozwolone, w przypadku gdy jest to wyraźnie dopuszczone prawem Unii. Przetwarzanie takie powinno zawsze podlegać odpowiednim zabezpieczeniom, obejmującym informowanie osoby, której dane dotyczą, prawo do uzyskania interwencji człowieka, prawo do wyrażenia własnego stanowiska, prawo do uzyskania wyjaśnienia co do decyzji wynikłej z takiej oceny oraz prawo do zakwestionowania takiej decyzji. Takie przetwarzanie nie powinno dotyczyć dzieci. Aby zapewnić rzetelność i przejrzystość przetwarzania wobec osoby, której dane dotyczą, mając na uwadze konkretne okoliczności i kontekst przetwarzania danych osobowych, administrator powinien stosować odpowiednie matematyczne lub statystyczne procedury profilowania, wdrożyć środki techniczne i organizacyjne zapewniające w szczególności korektę czynników powodujących nieprawidłowości w danych osobowych i maksymalne zmniejszenie ryzyka błędów, zabezpieczyć dane osobowe w sposób uwzględniający potencjalne ryzyko dla interesów i praw osoby, której dane dotyczą, oraz zapobiegający m.in. skutkom w postaci dyskryminacji osób fizycznych z uwagi na pochodzenie rasowe lub etniczne, poglądy polityczne, wyznanie lub przekonania, przynależność do związków zawodowych, stan genetyczny lub zdrowotny, orientację seksualną lub skutkujący środkami mającymi taki efekt. Zautomatyzowane podejmowanie decyzji i profilowanie oparte na szczególnych kategoriach danych osobowych powinny być dozwolone wyłącznie przy zachowaniu szczególnych warunków.

(37) W aktach prawnych przyjętych na podstawie Traktatów lub w wewnętrznych przepisach instytucji i organów unijnych można przewidzieć ograniczenia dotyczące określonych zasad oraz prawa do informacji, dostępu do danych osobowych i ich sprostowania lub usuwania, prawa do przenoszenia danych, poufności łączności elektronicznej, zawiadamiania osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych oraz określonych powiązanych obowiązków administratorów, o ile jest to niezbędne i proporcjonalne w społeczeństwie demokratycznym, by zapewnić bezpieczeństwo publiczne, zapobieganie przestępczości, prowadzenie postępowań przygotowawczych, ściganie czynów zabronionych, lub wykonywanie kar, w tym ochronę przed zagrożeniami dla bezpieczeństwa publicznego, włączając ochronę życia ludzkiego – w szczególności w odpowiedzi na klęski żywiołowe lub katastrofy spowodowane przez człowieka – i zapobieganie takim zagrożeniom, bezpieczeństwo wewnętrzne instytucji i organów unijnych, ochronę innych ważnych celów leżących w ogólnym interesie publicznym Unii lub państwa członkowskiego, w szczególności ważnego interesu gospodarczego lub finansowego Unii lub państwa członkowskiego, prowadzenie rejestrów publicznych z uwagi na względy ogólnego interesu publicznego, ochronę osoby, której dane dotyczą, lub praw i wolności innych osób, w tym cele w dziedzinie ochrony socjalnej, zdrowia publicznego i cele humanitarne.

Jeżeli w aktach prawnych przyjętych na podstawie Traktatów lub w wewnętrznych przepisach instytucji i organów unijnych nie przewidziano ograniczenia, instytucje i organy unijne mogą narzucić w danym przypadku ograniczenie doraźne dotyczące poszczególnych zasad i praw osoby, której dane dotyczą, jeżeli takie ograniczenie nie narusza istoty podstawowych praw i wolności oraz – w odniesieniu do danej operacji przetwarzania – stanowi w demokratycznym społeczeństwie niezbędny i proporcjonalny środek, który zapewnia realizację jednego bądź

kilku celów wyszczególnionych w ust. 1. Takie ograniczenie należy zgłosić inspektorowi ochrony danych. Ograniczenia te powinny być zgodne z wymogami Karty praw podstawowych oraz Europejskiej konwencji o ochronie praw człowieka i podstawowych wolności.

(38) Należy nałożyć na administratora obowiązki i ustanowić odpowiedzialność prawną administratora za przetwarzanie danych osobowych przez niego samego lub w jego imieniu. W szczególności administrator powinien mieć obowiązek wdrożenia odpowiednich i skutecznych środków oraz powinien być w stanie wykazać, że czynności przetwarzania są zgodne z niniejszym rozporządzeniem oraz że są skuteczne. Środki te powinny uwzględniać charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw i wolności osób fizycznych. Ryzyko naruszenia praw lub wolności osób, o różnym prawdopodobieństwie i wadze zagrożeń, może wynikać z przetwarzania danych osobowych mogącego prowadzić do uszczerbku fizycznego lub szkód majątkowych lub niemajątkowych, w szczególności: jeżeli przetwarzanie może poskutkować dyskryminacją, kradzieżą tożsamości lub oszustwem dotyczącym tożsamości, stratą finansową, naruszeniem dobrego imienia, naruszeniem poufności danych osobowych chronionych tajemnicą zawodową, nieuprawnionym odwróceniem pseudonimizacji lub wszelką inną znaczną szkodą gospodarczą lub społeczną; jeżeli osoby, których dane dotyczą, mogą zostać pozbawione przysługujących im praw i wolności lub możliwości sprawowania kontroli nad swoimi danymi osobowymi; jeżeli przetwarzane są dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, wyznanie lub przekonania światopoglądowe, lub przynależność do związków zawodowych oraz jeżeli przetwarzane są dane genetyczne, dane dotyczące zdrowia lub dane dotyczące seksualności lub wyroków skazujących i naruszeń prawa lub związanych z tym środków bezpieczeństwa; jeżeli oceniane są czynniki osobowe, w szczególności analizowane lub prognozowane aspekty dotyczące efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się – w celu tworzenia lub wykorzystywania profili osobistych; jeżeli przetwarzane są dane osobowe osób wymagających szczególnej opieki, w szczególności dzieci; lub jeżeli przetwarzanie dotyczy dużej ilości danych osobowych i wpływa na dużą liczbę osób, których dane dotyczą. Prawdopodobieństwo i powagę ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, należy określić poprzez odniesienie się do charakteru, zakresu, kontekstu i celów przetwarzania danych. Ryzyko należy oszacować na podstawie obiektywnej oceny, w ramach której stwierdza się, czy z operacjami przetwarzania danych wiąże się ryzyko lub wysokie ryzyko.

(39) Ochrona praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych wymaga wdrożenia odpowiednich środków technicznych i organizacyjnych, by zapewnić spełnienie wymogów niniejszego rozporządzenia. Aby móc wykazać przestrzeganie niniejszego rozporządzenia, administrator powinien przyjąć wewnętrzne polityki i wdrożyć środki, które są zgodne w szczególności z zasadą uwzględniania ochrony danych w fazie projektowania oraz z zasadą domyślnej ochrony danych. Takie środki mogą polegać m.in. na minimalizacji przetwarzania danych osobowych, jak najszybszej pseudonimizacji danych osobowych, przejrzystości co do funkcji i przetwarzania danych osobowych, umożliwieniu osobie, której dane dotyczą, monitorowania przetwarzania danych, umożliwieniu administratorowi tworzenia i doskonalenia zabezpieczeń. Zasadę uwzględniania

ochrony danych w fazie projektowania i zasadę domyślnej ochrony danych należy też brać pod uwagę w przetargach publicznych.

(40) Ochrona praw i wolności osób, których dane dotyczą, oraz obowiązki i odpowiedzialność prawna administratorów i podmiotów przetwarzających wymagają dokonania w ramach niniejszego rozporządzenia jasnego podziału obowiązków, także w sytuacji, gdy administrator określa cele i sposoby przetwarzania wspólnie z innymi administratorami lub gdy operacji przetwarzania dokonuje się w imieniu administratora.

(41) Aby zapewnić przestrzeganie wymogów niniejszego rozporządzenia w przypadku przetwarzania, którego w imieniu administratora ma dokonać podmiot przetwarzający, administrator powinien, powierzając podmiotowi przetwarzającemu czynności przetwarzania, korzystać z usług wyłącznie podmiotów przetwarzających, które zapewniają wystarczające gwarancje – w szczególności jeżeli chodzi o wiedzę fachową, wiarygodność i zasoby – wdrożenia środków technicznych i organizacyjnych odpowiadających wymogom niniejszego rozporządzenia, w tym wymogom bezpieczeństwa przetwarzania. Stosowanie zatwierdzonego kodeksu postępowania lub zatwierdzonego mechanizmu certyfikacji przez podmioty przetwarzające inne niż instytucje i organy unijne może posłużyć za element wykazujący wywiązywanie się z obowiązków administratora. Przetwarzanie przez podmiot przetwarzający powinno być regulowane umową lub innym instrumentem prawnym, które podlegają prawu Unii lub prawu państwa członkowskiego, wiążą podmiot przetwarzający z administratorem, określają przedmiot i czas trwania przetwarzania, charakter i cele przetwarzania, rodzaj danych osobowych i kategorie osób, których dane dotyczą, oraz które powinny uwzględniać konkretne zadania i obowiązki podmiotu przetwarzającego w kontekście planowanego przetwarzania oraz ryzyko naruszenia praw lub wolności osoby, której dane dotyczą. Administrator i podmiot przetwarzający powinni mieć możliwość podjęcia decyzji o skorzystaniu z umowy indywidualnej lub ze standardowych klauzul umownych, które zostały przyjęte bezpośrednio przez Komisję albo które zostały przyjęte przez Europejskiego Inspektora Ochrony Danych, a następnie przyjęte przez Komisję. Po zakończeniu przetwarzania w imieniu administratora podmiot przetwarzający powinien – zgodnie z decyzją administratora – zwrócić lub usunąć dane osobowe, chyba że prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający, nakładają obowiązek przechowywania tych danych osobowych.

(42) Dla zachowania zgodności z niniejszym rozporządzeniem, administratorzy powinni prowadzić rejestry czynności przetwarzania, za które są odpowiedzialni, a podmioty przetwarzające – rejestry kategorii czynności przetwarzania, za które są odpowiedzialne. Instytucje i organy unijne powinny być zobowiązane do współpracy z Europejskim Inspektorem Ochrony Danych i na jego żądanie powinny udostępniać mu swoje rejestry w celu monitorowania tych operacji przetwarzania. Instytucje i organy unijne powinny mieć możliwość ustanowienia centralnego rejestru prowadzonych przez nie czynności przetwarzania. Ze względu na przejrzystość powinny mieć również możliwość publicznego udostępnienia takiego rejestru.

(43) W celu zachowania bezpieczeństwa i zapobiegania przetwarzaniu niezgodnemu z niniejszym rozporządzeniem administrator lub podmiot przetwarzający powinni oszacować ryzyko właściwe dla przetwarzania oraz wdrożyć środki – takie jak szyfrowanie – minimalizujące to ryzyko. Środki takie powinny zapewnić odpowiedni

poziom bezpieczeństwa, w tym poufność, oraz uwzględniać stan wiedzy technicznej oraz koszty ich wdrożenia w stosunku do ryzyka i charakteru danych osobowych podlegających ochronie. Oceniając ryzyko w zakresie bezpieczeństwa danych, należy wziąć pod uwagę ryzyko związane z przetwarzaniem danych osobowych – takie jak przypadkowe lub niezgodne z prawem zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych – i mogące w szczególności prowadzić do uszczerbku fizycznego, szkód majątkowych lub niemajątkowych.

(44) Instytucje i organy unijne powinny zapewniać poufność łączności elektronicznej zgodnie z art. 7 Karty. Instytucje i organy unijne powinny w szczególności zapewniać bezpieczeństwo swoich sieci łączności elektronicznej, chronić informacje mające związek z końcowymi urządzeniami telekomunikacyjnymi użytkowników końcowych łączącymi się z dostępnymi publicznie stronami internetowymi i aplikacjami mobilnymi tych instytucji i organów, zgodnie z rozporządzeniem (UE) XXXX/XX [nowe rozporządzenie o prywatności i łączności elektronicznej], a także chronić dane osobowe w spisach użytkowników.

(45) Przy braku odpowiedniej i szybkiej reakcji naruszenie ochrony danych osobowych może skutkować powstaniem uszczerbku fizycznego, szkód majątkowych lub niemajątkowych u osób fizycznych. Dlatego natychmiast po stwierdzeniu naruszenia ochrony danych osobowych administrator powinien zgłosić je Europejskiemu Inspektorowi Ochrony Danych bez zbędnej zwłoki, jeżeli to wykonalne, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia, chyba że administrator jest w stanie wykazać zgodnie z zasadą rozliczalności, że jest mało prawdopodobne, by naruszenie to mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych. Jeżeli nie można dokonać zgłoszenia w terminie 72 godzin, zgłoszeniu powinno towarzyszyć wyjaśnienie przyczyn opóźnienia, a informacje mogą być przekazywane stopniowo, bez dalszej zbędnej zwłoki. Jeżeli taka zwłoka jest uzasadniona, należy udostępnić jak najwcześniej mniej wrażliwe lub mniej szczegółowe informacje, zamiast rozwiązywać do końca problem leżący u podstawy zdarzenia przed jego zgłoszeniem.

(46) Administrator powinien bez zbędnej zwłoki poinformować osobę, której dane dotyczą, o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby, tak aby umożliwić tej sobie podjęcie niezbędnych działań zapobiegawczych. Informacja taka powinna zawierać opis charakteru naruszenia ochrony danych osobowych oraz zalecenia dla danej osoby fizycznej co do minimalizacji potencjalnych niekorzystnych skutków. Informacje należy przekazywać osobom, których dane dotyczą, tak szybko, jak jest to rozsądnie możliwe, w ścisłej współpracy z Europejskim Inspektorem Ochrony Danych, z poszanowaniem wskazówek przekazanych przez ten organ lub inne odpowiednie organy, takie jak organy ścigania.

(47) W rozporządzeniu (WE) nr 45/2001 przewidziano, że ogólnym obowiązkiem administratora jest zgłaszanie przetwarzania danych osobowych inspektorowi ochrony danych, który z kolei ma prowadzić rejestr zgłaszanych operacji przetwarzania. Obowiązek ten powodując jednak obciążenia administracyjne i finansowe i nie zawsze przyczyniał się do poprawy ochrony danych osobowych. Dlatego należy znieść te powszechne, ogólne obowiązki zgłaszania i zastąpić je skutecznymi procedurami i

mechanizmami koncentrującymi się w zamian na tych rodzajach operacji przetwarzania, które ze względu na swój charakter, zakres, kontekst i cele mogą powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych. Takie rodzaje operacji przetwarzania obejmują w szczególności operacje, które wiążą się w szczególności z użyciem nowych technologii lub które są nowe i nie zostały jeszcze poddane przez administratora ocenie skutków w zakresie ochrony danych lub stały się niezbędne z uwagi na upływ czasu od pierwotnego przetwarzania. W takim przypadku administrator powinien przed przetwarzaniem dokonać oceny skutków w zakresie ochrony danych, aby ocenić konkretne prawdopodobieństwo i powagę tego wysokiego ryzyka, uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz źródła ryzyka. Ocena skutków powinna w szczególności obejmować planowane środki, zabezpieczenia i mechanizmy mające minimalizować to ryzyko, zapewniać ochronę danych osobowych oraz wykazać przestrzeganie niniejszego rozporządzenia.

(48) Jeżeli ocena skutków w zakresie ochrony danych wykaże, że przy braku zabezpieczeń, środków bezpieczeństwa oraz mechanizmów minimalizujących ryzyko przetwarzanie powodowałoby wysokie ryzyko naruszenia praw lub wolności osób fizycznych, a administrator wyraża opinię, że ryzyka tego nie da się zminimalizować środkami rozsądnymi z punktu widzenia dostępnych technologii i kosztów wdrożenia, wtedy przed rozpoczęciem czynności przetwarzania należy skonsultować się z Europejskim Inspektorem Ochrony Danych. Takie wysokie ryzyko mogą powodować pewne rodzaje przetwarzania oraz zakres i częstotliwość przetwarzania, które mogą skutkować także szkodą lub ingerencją w prawa i wolności osoby fizycznej. Na wniosek o konsultacje Europejski Inspektor Ochrony Danych powinien odpowiedzieć w określonym terminie. Jednak brak reakcji ze strony Europejskiego Inspektora Ochrony Danych w tym terminie nie powinien wykluczać interwencji Europejskiego Inspektora Ochrony Danych zgodnie z jego zadaniami i uprawnieniami określonymi w niniejszym rozporządzeniu, w tym uprawnieniami do zakazania operacji przetwarzania. W ramach konsultacji powinna istnieć możliwość przedłożenia Europejskiemu Inspektorowi Ochrony Danych wyników oceny skutków w zakresie ochrony danych dokonanej w odniesieniu do danego przetwarzania, a w szczególności środków planowanych w celu zminimalizowania ryzyka naruszenia praw lub wolności osób fizycznych.

(49) Europejski Inspektor Ochrony Danych powinien być informowany o środkach administracyjnych i wewnętrznych przepisach instytucji i organów unijnych, w których przewidziano przetwarzanie danych osobowych, określono warunki ograniczeń praw osób, których dane dotyczą, lub zapewniono właściwe zabezpieczenia praw osób, których dane dotyczą, aby zapewnić zgodność zamierzonego przetwarzania z niniejszym rozporządzeniem, a w szczególności zminimalizować ewentualne ryzyko dla osoby, której dane dotyczą.

(50) Rozporządzeniem (UE) 2016/679 ustanowiono Europejską Radę Ochrony Danych jako niezależny organ Unii posiadający osobowość prawną. Europejska Rada Ochrony Danych powinna przyczyniać się do spójnego stosowania przepisów rozporządzenia (UE) 2016/679 i dyrektywy 2016/680 w całej Unii, m.in. poprzez doradzanie Komisji. Jednocześnie Europejski Inspektor Ochrony Danych powinien w dalszym ciągu wykonywać swoje funkcje nadzorcze i doradcze w odniesieniu do wszystkich instytucji i organów unijnych, w tym z inicjatywy własnej lub na wniosek. Aby zapewnić zgodność przepisów o ochronie danych w całej Unii, Komisja powinna mieć obowiązek przeprowadzania konsultacji po przyjęciu aktów ustawodawczych lub

podczas opracowywania aktów delegowanych i aktów wykonawczych, o których mowa w art. 289, 290 i 291 TFUE, oraz po przyjęciu zaleceń i wniosków odnoszących się do umów z państwami trzecimi i organizacjami międzynarodowymi, o których mowa w art. 218 TFUE i które mają wpływ na prawo do ochrony danych osobowych. W takich przypadkach Komisja powinna mieć obowiązek skonsultowania się z Europejskim Inspektorem Ochrony Danych, z wyjątkiem przypadków, w odniesieniu do których w rozporządzeniu (UE) 2016/679 przewidziano obowiązek konsultacji z Europejską Radą Ochrony Danych, na przykład w przypadku decyzji stwierdzających odpowiedni stopień ochrony lub aktów delegowanych w sprawie standardowych znaków graficznych i wymogów dotyczących mechanizmów certyfikacji. Ponadto, jeżeli dany akt ma szczególne znaczenie dla ochrony praw i wolności osób fizycznych w zakresie przetwarzania danych osobowych, Komisja powinna mieć możliwość skonsultowania się z Europejską Radą Ochrony Danych. W takich przypadkach Europejski Inspektor Ochrony Danych jako członek Europejskiej Rady Ochrony Danych powinien skoordynować swoje prace z pracami rady w celu wydania wspólnej opinii. Europejski Inspektor Ochrony Danych i w stosownych przypadkach Europejska Rada Ochrony Danych powinni przedstawić pisemne zalecenie w terminie ośmiu tygodni. W razie przypadku niecierpiącego zwłoki lub w innym uzasadnionym przypadku te ramy czasowe należy skrócić, na przykład gdy Komisja jest w trakcie prac nad aktami delegowanymi i wykonawczymi.

(51) W każdej instytucji unijnej lub organie unijnym inspektor ochrony danych powinien zapewnić stosowanie przepisów niniejszego rozporządzenia oraz doradzić administratorom i podmiotom przetwarzającym w kwestii wypełniania ich zobowiązań. Inspektor powinien być osobą posiadającą wiedzę fachową w zakresie przepisów i praktyk ochrony danych, której poziom należy ustalić w szczególności w świetle prowadzonych operacji przetwarzania danych oraz ochrony, której wymagają dane osobowe przetwarzane przez administratora lub podmiot przetwarzający. Tacy inspektorzy ochrony danych powinni być w stanie wykonywać swoje obowiązki i zadania w sposób niezależny.

(52) Jeżeli instytucje i organy unijne przekazują dane osobowe administratorom, podmiotom przetwarzającym lub innym odbiorcom w państwach trzecich lub organizacjom międzynarodowym, nie należy obniżać stopnia ochrony osób fizycznych zapewnianego w Unii niniejszym rozporządzeniem, także w przypadkach dalszego przekazywania danych osobowych: z państwa trzeciego lub organizacji międzynarodowej administratorom lub pomiotom przetwarzającym w tym samym lub w innym państwie trzecim lub tej samej lub innej organizacji międzynarodowej. W każdym przypadku przekazywanie danych do państw trzecich i organizacji międzynarodowych może się odbywać wyłącznie w pełnej zgodzie z niniejszym rozporządzeniem. Przekazywanie może mieć miejsce wyłącznie w przypadkach, gdy administrator lub podmiot przetwarzający przestrzegają warunków określonych w przepisach niniejszego rozporządzenia dotyczących przekazywania danych osobowych państwom trzecim lub organizacjom międzynarodowym – z zastrzeżeniem pozostałych przepisów niniejszego rozporządzenia.

(53) Zgodnie z art. 45 rozporządzenia (UE) 2016/679 Komisja może uznać, że państwo trzecie, terytorium lub określony sektor w państwie trzecim, lub organizacja międzynarodowa zapewnia odpowiedni stopień ochrony danych. W takich przypadkach przekazywanie danych osobowych do tego państwa trzeciego lub tej

organizacji międzynarodowej przez instytucję unijną lub organ unijny może się odbywać bez potrzeby uzyskania dodatkowego zezwolenia.

(54) W razie braku stwierdzenia odpowiedniego stopnia ochrony danych administrator lub podmiot przetwarzający powinni zastosować środki rekompensujące brak ochrony danych w państwie trzecim, zapewniając osobie, której dane dotyczą, odpowiednie zabezpieczenia. Takie odpowiednie zabezpieczenia mogą polegać na skorzystaniu ze standardowych klauzul ochrony danych przyjętych przez Komisję, standardowych klauzul ochrony danych przyjętych przez Europejskiego Inspektora Ochrony Danych lub klauzul umownych dopuszczonych przez Europejskiego Inspektora Ochrony Danych. Jeżeli podmiot przetwarzający nie jest instytucją unijną ani organem unijnym, na takie odpowiednie zabezpieczenia mogą również składać się wiążące reguły korporacyjne, kodeksy postępowania i mechanizmy certyfikacji stosowane na potrzeby międzynarodowego przekazywania danych zgodnie z rozporządzeniem (UE) 2016/679. Zabezpieczenia te powinny zapewniać, by przestrzegane były wymogi ochrony danych oraz prawa osób, których dane dotyczą, takie same jak w przypadku przetwarzania wewnątrzunijnego, w tym zapewniać możliwość skorzystania z egzekwowalnych praw osoby, której dane dotyczą, i skutecznych środków ochrony prawnej – w tym prawa do skutecznych administracyjnych lub sądowych środków zaskarżenia i do żądania odszkodowania – w Unii lub w państwie trzecim. Powinny one dotyczyć w szczególności przestrzegania ogólnych zasad związanych z przetwarzaniem danych osobowych oraz zasad uwzględniania ochrony danych w fazie projektowania i domyślnej ochrony danych. Również instytucje i organy unijne mogą przekazywać dane organom lub podmiotom publicznym w państwach trzecich lub organizacjom międzynarodowym o analogicznych obowiązkach lub funkcjach, w tym na podstawie przepisów, które powinny znaleźć się w uzgodnieniach administracyjnych, takich jak protokoły ustaleń, i które powinny przewidywać egzekwowalne i skuteczne prawa osób, których dane dotyczą. Jeżeli zabezpieczenia zawarte są w niewiążących prawnie uzgodnieniach administracyjnych, należy uzyskać zezwolenie Europejskiego Inspektora Ochrony Danych.

(55) Możliwość korzystania przez administratora lub podmiot przetwarzający ze standardowych klauzul ochrony danych przyjętych przez Komisję lub Europejskiego Inspektora Ochrony Danych nie powinna stanowić dla administratora lub podmiotu przetwarzającego przeszkody, by standardowe klauzule ochrony danych włączyć do szerszej umowy, takiej jak umowa między wspomnianym podmiotem przetwarzającym a innym podmiotem przetwarzającym, ani by dodać inne klauzule lub dodatkowe zabezpieczenia, pod warunkiem że nie są one bezpośrednio lub pośrednio sprzeczne ze standardowymi klauzulami umownymi przyjętymi przez Komisję lub Europejskiego Inspektora Ochrony Danych ani nie naruszają podstawowych praw lub wolności osób, których dane dotyczą. Należy zachęcać administratorów i podmioty przetwarzające, by w drodze zobowiązań umownych przewidywały dodatkowe zabezpieczenia, stanowiące uzupełnienie dla standardowych klauzul ochrony danych.

(56) Niektóre państwa trzecie przyjmują ustawy, rozporządzenia i inne akty prawne mające bezpośrednio regulować czynności przetwarzania podejmowane przez instytucje i organy unijne. Może to obejmować wyroki sądów lub trybunałów czy decyzje organów administracyjnych państwa trzeciego nakazujące administratorowi lub podmiotowi przetwarzającemu przekazać lub ujawnić dane osobowe, które nie mają za podstawę umowy międzynarodowej obowiązującej między wzywającym państwem

trzecim a Unią. Transgraniczne stosowanie tych ustaw, rozporządzeń i innych aktów prawnych może naruszać prawo międzynarodowe i uniemożliwiać zapewnienie osobom fizycznym ochrony ustanowionej niniejszym rozporządzeniem na terytorium Unii. Przekazywanie danych powinno być dopuszczalne wyłącznie w przypadkach, gdy spełnione są warunki przekazywania do państw trzecich ustanowione w niniejszym rozporządzeniu. Tak może być m.in. w przypadkach, gdy ujawnienie jest niezbędne ze względu na ważny interes publiczny uznany w prawie Unii.

(57) W określonych sytuacjach należy wprowadzić możliwość przekazywania danych w niektórych okolicznościach, jeżeli osoba, której dane dotyczą, wyraziła na to wyraźną zgodę, jeżeli przekazywanie jest sporadyczne i niezbędne w związku z umową lub roszczeniem – niezależnie od rodzaju postępowania: sądowego lub administracyjnego lub jakiegokolwiek innego postępowania pozasądowego, w tym postępowania przed organami regulacyjnymi. Należy także przewidzieć możliwość przekazywania danych, jeżeli wymaga tego ważny interes publiczny określony w prawie Unii lub jeżeli przekazanie następuje z rejestru utworzonego na mocy prawa i przeznaczonego do wglądu dla ogółu obywateli lub osób mających prawnie uzasadniony interes. W drugim z tych przypadków przekazanie nie powinno obejmować całości danych osobowych lub całych kategorii danych z rejestru, chyba że zezwala na to prawo Unii, a jeżeli rejestr jest przeznaczony do wglądu dla osób mających prawnie uzasadniony interes, przekazanie danych powinno nastąpić wyłącznie na żądanie tych osób lub jeżeli osoby te mają być odbiorcami, przy pełnym uwzględnieniu interesów i praw podstawowych osoby, której dane dotyczą.

(58) Wyjątki te powinny mieć w szczególności zastosowanie do przekazywania danych wymaganego i niezbędnego z uwagi na ważne względy interesu publicznego, na przykład do międzynarodowej wymiany danych między instytucjami i organami unijnymi a organami ds. konkurencji, organami podatkowymi lub celnymi, organami nadzoru finansowego, służbami odpowiedzialnymi za sprawy zabezpieczenia społecznego lub za zdrowie publiczne, na przykład w przypadku ustalania kontaktów zakaźnych w razie chorób zakaźnych lub w celu zmniejszenia lub wyeliminowania dopingu w sporcie. Przekazywanie danych osobowych należy uznać za zgodne z prawem również w przypadkach, gdy jest niezbędne w celu ochrony interesu, który ma istotne znaczenie dla żywotnych interesów osoby, której dane dotyczą, lub innej osoby, w tym integralności fizycznej lub życia, jeżeli osoba, której dane dotyczą, nie jest w stanie wyrazić zgody. W razie braku stwierdzenia odpowiedniego stopnia ochrony prawo Unii może z uwagi na ważne względy interesu publicznego wyraźnie nakładać ograniczenia na przekazywanie konkretnych kategorii danych do państwa trzeciego lub organizacji międzynarodowej. Każde przekazanie danych osobowych osoby, której dane dotyczą, fizycznie lub prawnie niezdolnej do wyrażenia zgody, do międzynarodowej organizacji humanitarnej, aby mogła wykonać zadanie nałożone na nią konwencjami genewskimi lub by mogła spełnić wymogi międzynarodowego prawa humanitarnego mającego zastosowanie w konfliktach zbrojnych, można uznać za niezbędne z uwagi na ważny wzgląd interesu publicznego lub za leżące w żywotnym interesie osoby, której dane dotyczą.

(59) W każdym przypadku, jeżeli Komisja nie wydała decyzji stwierdzającej odpowiedni stopień ochrony danych w państwie trzecim, administrator lub podmiot przetwarzający powinni zastosować rozwiązania, które pozwolą osobom, których dane dotyczą, dysponować – gdy przekazanie już dojdzie do skutku – egzekwowalnymi i

skutecznymi prawami względem przetwarzania ich danych w Unii, tak że osoby te nadal będą mogły korzystać z podstawowych praw i zabezpieczeń.

(60) Transgraniczne przekazywanie danych osobowych poza Unią może spowodować wzrost ryzyka, że osoby fizyczne nie będą mogły wykonywać prawa do ochrony danych osobowych, w szczególności w celu ochrony przed niezgodnym z prawem wykorzystaniem lub ujawnieniem tych informacji. Jednocześnie organy nadzorcze w Unii, w tym Europejski Inspektor Ochrony Danych, mogą nie być w stanie rozpatrzyć skargi lub przeprowadzić postępowania w sprawie działalności, która ma miejsce poza granicami ich jurysdykcji. Ich starania na rzecz współpracy w kontekście transgranicznym mogą także zostać zakłócone przez niewystarczające uprawnienia prewencyjne lub zaradcze, niespójne systemy prawne oraz przeszkody praktyczne, takie jak ograniczone środki. Należy więc upowszechniać ściślejszą współpracę między Europejskim Inspektorem Ochrony Danych a organami nadzorującymi ochronę danych, by pomóc im wymieniać informacje i prowadzić postępowania z ich międzynarodowymi odpowiednikami.

(61) Utworzenie rozporządzeniem (WE) nr 45/2001 urzędu Europejskiego Inspektora Ochrony Danych, który jest uprawniony do wypełniania zadań i wykonywania uprawnień w sposób całkowicie niezależny, stanowi zasadniczy element ochrony osób fizycznych w związku z przetwarzaniem danych osobowych. Niniejsze rozporządzenie powinno jeszcze bardziej wzmocnić i wyjaśnić rolę i niezależność tego urzędu.

(62) Aby zapewnić spójne monitorowanie i egzekwowanie przepisów o ochronie danych w całej Unii, Europejski Inspektor Ochrony Danych powinien mieć te same zadania i faktyczne uprawnienia co organy nadzorcze w państwach członkowskich, w tym uprawnienia do prowadzenia postępowań wyjaśniających, naprawcze, uprawnienia do nakładania kar oraz do udzielania zezwoleń i doradcze, w szczególności w przypadku skarg osób fizycznych, i uprawnienia do zgłaszania naruszeń niniejszego rozporządzenia Trybunałowi Sprawiedliwości Unii Europejskiej oraz do udziału w postępowaniu sądowym zgodnie z prawem pierwotnym. Wśród tych uprawnień powinno być także uprawnienie do wprowadzania czasowego lub definitywnego ograniczenia przetwarzania, w tym zakazania przetwarzania. Aby uniknąć nadmiernych kosztów i niedogodności dla danej osoby, której interesy mogą zostać naruszone, każdy środek Europejskiego Inspektora Ochrony Danych powinien być odpowiedni, niezbędny i proporcjonalny, aby zapewnić przestrzeganie niniejszego rozporządzenia, oraz uwzględniać okoliczności danej sprawy, z poszanowaniem prawa do wysłuchania danej osoby przed zastosowaniem indywidualnego środka. Każdy prawnie wiążący środek Europejskiego Inspektora Ochrony Danych powinien być sporządzony na piśmie, mieć jasny i jednoznaczny charakter, wskazywać datę wydania środka, nosić podpis Europejskiego Inspektora Ochrony Danych, podawać powody zastosowania środka oraz informować o prawie do skutecznego środka ochrony prawnej.

(63) Decyzje Europejskiego Inspektora Ochrony Danych dotyczące wyjątków, gwarancji, upoważnienia i warunków dotyczących operacji przetwarzania danych według definicji niniejszego rozporządzenia powinny być publikowane w sprawozdaniu o działalności. Niezależnie od publikacji rocznego sprawozdania o działalności Europejskiego Inspektora Ochrony Danych mogą publikować sprawozdania o konkretnych tematach.

(64) Krajowe organy nadzorcze monitorują stosowanie przepisów rozporządzenia (UE) 2016/679 oraz przyczyniają się do jego spójnego stosowania w całej Unii, aby chronić osoby fizyczne w związku z przetwarzaniem ich danych osobowych oraz ułatwiać swobodny przepływ danych osobowych na rynku wewnętrznym. Aby zwiększyć stopień zgodności stosowania przepisów o ochronie danych mających zastosowanie w państwach członkowskich i przepisów o ochronie danych mających zastosowanie do instytucji i organów unijnych, Europejski Inspektor Ochrony Danych powinien skutecznie współpracować z krajowymi organami nadzorczymi.

(65) W niektórych przypadkach prawo Unii przewiduje model skoordynowanego nadzoru sprawowanego wspólnie przez Europejskiego Inspektora Ochrony Danych i krajowe organy nadzorcze. Ponadto Europejski Inspektor Ochrony Danych pełni rolę organu nadzorczego Europolu; istnieje również szczególny model współpracy z krajowymi organami nadzorczymi, który funkcjonuje poprzez radę współpracy pełniącą funkcję doradczą. Aby poprawić skuteczny nadzór i egzekwowanie przepisów prawa materialnego o ochronie danych, należy wprowadzić w Unii jednolity spójny model skoordynowanego nadzoru. W związku z tym Komisja powinna złożyć – w stosownych przypadkach – wnioski ustawodawcze w celu zmiany unijnych aktów prawnych, w których przewidziano model skoordynowanego nadzoru, aby dostosować je do skoordynowanego modelu nadzoru przewidzianego w niniejszym rozporządzeniu. Europejska Rada Ochrony Danych powinna funkcjonować jako jednolite forum, aby zapewnić skuteczny i skoordynowany nadzór całej rady.

(66) Każda osoba, której dane dotyczą, powinna mieć prawo wniesienia skargi do Europejskiego Inspektora Ochrony Danych oraz prawo do skutecznego środka ochrony prawnej przed Trybunałem Sprawiedliwości Unii Europejskiej, zgodnie z przepisami Traktatów, jeżeli uzna, że jej prawa wynikające z niniejszego rozporządzenia są naruszane, lub jeżeli Europejski Inspektor Ochrony Danych nie reaguje na skargę, częściowo lub w całości ją odrzuca lub oddala, lub nie podejmuje działania, choć jest to niezbędne do ochrony praw tej osoby. Postępowanie wyjaśniające na podstawie skargi powinno być prowadzone – z zastrzeżeniem kontroli sądowej – w zakresie odpowiadającym konkretnej sprawie. Europejski Inspektor Ochrony Danych powinien w rozsądnym terminie poinformować osobę, której dane dotyczą, o postępach i wynikach rozpatrywania skargi. Jeżeli dana sprawa wymaga dalszej koordynacji działań z krajowym organem nadzorczym, osoba, której dane dotyczą, powinna zostać o tym uprzednio poinformowana. Aby ułatwić wnoszenie skarg, Europejski Inspektor Ochrony Danych powinien zastosować takie środki jak udostępnienie formularza skargi, który można wypełnić także elektronicznie, przy czym nie należy wykluczać innych sposobów komunikacji.

(67) Każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia niniejszego rozporządzenia, powinna mieć prawo uzyskania od administratora lub podmiotu przetwarzającego odszkodowania za poniesioną szkodę, z zastrzeżeniem warunków przewidzianych w Traktacie.

(68) Aby wzmocnić nadzorczą rolę Europejskiego Inspektora Ochrony Danych i skuteczne wdrażanie przepisów niniejszego rozporządzenia, Europejski Inspektor Ochrony Danych powinien mieć prawo do nakładania administracyjnych kar pieniężnych jako ostatecznej sankcji. Celem kar pieniężnych powinno być ukaranie za nieprzestrzeganie przepisów niniejszego rozporządzenia nie tyle poszczególnych osób, co instytucji i organów, aby powstrzymać przed kolejnymi naruszeniami niniejszego rozporządzenia

i upowszechniać kulturę ochrony danych osobowych wewnątrz instytucji i organów unijnych. W niniejszym rozporządzeniu należy wymienić rodzaje naruszeń oraz wskazać górne granice i kryteria ustalania związanych z nimi administracyjnych kar pieniężnych. Europejski Inspektor Ochrony Danych powinien określać wysokość kar pieniężnych indywidualnie dla każdego przypadku z uwzględnieniem wszystkich stosownych okoliczności danej sytuacji, z należytym uwzględnieniem charakteru, wagi, czasu trwania naruszenia i jego konsekwencji, a także środków podjętych w celu zastosowania się do obowiązków wynikających z niniejszego rozporządzenia oraz w celu zapobieżenia konsekwencjom naruszenia lub w celu zminimalizowania tych konsekwencji. Nakładając administracyjną karę pieniężną na organ unijny, Europejski Inspektor Ochrony Danych powinien wziąć pod uwagę proporcjonalność wysokości kary pieniężnej. Procedura administracyjna nakładania kar pieniężnych na instytucje i organy unijne powinna być zgodna z ogólnymi przepisami prawa Unii, w myśl wykładni ustalonej przez Trybunał Sprawiedliwości Unii Europejskiej.

(69) Jeżeli osoba, której dane dotyczą, uzna, że naruszane są jej prawa wynikające z niniejszego rozporządzenia, powinna mieć ona prawo zlecić podmiotowi, organizacji lub zrzeszeniu – które nie mają charakteru zarobkowego, zostały ustanowione zgodnie z prawem Unii lub z prawem państwa członkowskiego, mają statutowo na celu interes publiczny i działają w dziedzinie ochrony danych osobowych – wniesienie skargi w jej imieniu do Europejskiego Inspektora Ochrony Danych. Taki organ, organizacja lub zrzeszenie powinny mieć również możliwość wykonywania prawa do środka ochrony prawnej w imieniu osób, których dane dotyczą, lub wykonywania prawa do odszkodowania w imieniu osób, których dane dotyczą.

(70) Urzędnik lub inny funkcjonariusz Unii, który nie dopełni zobowiązań wynikających z niniejszego rozporządzenia, podlega karze dyscyplinarnej lub innej zgodnie z regułami i procedurami ustanowionymi w regulaminie pracowniczym urzędników Unii Europejskiej lub w warunkach zatrudnienia innych pracowników Unii Europejskiej.

(71) Aby zapewnić jednolite warunki wdrażania niniejszego rozporządzenia, należy powierzyć Komisji uprawnienia wykonawcze, tak jak to przewiduje niniejsze rozporządzenie. Uprawnienia te powinny być wykonywane zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 182/2011[16]. Procedurę sprawdzającą należy stosować do przyjmowania aktów wykonawczych w odniesieniu do standardowych klauzul umownych między administratorami a podmiotami przetwarzającymi oraz między podmiotami przetwarzającymi, do przyjęcia wykazu operacji przetwarzania, jeżeli wymagane są uprzednie konsultacje z Europejskim Inspektorem Ochrony Danych na potrzeby przetwarzania danych do celów wykonania zadania realizowanego przez administratorów w interesie publicznym, oraz do przyjęcia standardowych klauzul umownych zapewniających stosowne gwarancje dla międzynarodowego przekazywania danych.

(72) Należy chronić informacje poufne, które organy statystyczne Unii i państw członkowskich gromadzą do celów opracowywania oficjalnych statystyk europejskich i krajowych. Statystyki europejskie należy projektować, tworzyć i rozpowszechniać zgodnie z zasadami statystycznymi przewidzianymi w art. 338 ust. 2 TFUE. Dalsze

[16] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 182/2011 z dnia 16 lutego 2011 r. ustanawiające przepisy i zasady ogólne dotyczące trybu kontroli przez państwa członkowskie wykonywania uprawnień wykonawczych przez Komisję (Dz.U. L 55 z 28.2.2011, s. 13).

szczegółowe informacje o statystycznej poufności statystyki europejskiej zawiera rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 223/2009[17].

(73) Należy uchylić przepisy rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE. Odesłania do uchylonego rozporządzenia oraz uchylonej decyzji należy rozumieć jako odesłania do niniejszego rozporządzenia.

(74) Aby chronić pełną niezależność członków niezależnego organu nadzorczego, niniejsze rozporządzenie powinno pozostać bez wpływu na kadencję obecnego Europejskiego Inspektora Ochrony Danych i obecnego zastępcy inspektora. Obecny zastępca inspektora powinien pozostać na stanowisku do końca swojej kadencji, chyba że spełniony zostanie jeden z warunków wcześniejszego zakończenia kadencji Europejskiego Inspektora Ochrony Danych przewidzianych w niniejszym rozporządzeniu. Odpowiednie przepisy niniejszego rozporządzenia powinny mieć zastosowanie do zastępcy inspektora do końca jego kadencji.

(75) Zgodnie z zasadą proporcjonalności do osiągnięcia podstawowego celu polegającego na zapewnieniu jednakowego stopnia ochrony osób fizycznych oraz swobodnego przepływu danych osobowych w całej Unii niezbędne i właściwe jest ustanowienie przepisów dotyczących przetwarzania danych osobowych w instytucjach i organach unijnych. Niniejsze rozporządzenie nie wykracza poza to, co jest konieczne do osiągnięcia tych celów, zgodnie z art. 5 ust. 4 Traktatu o Unii Europejskiej.

(76) Zgodnie z art. 28 ust. 2 rozporządzenia (WE) nr 45/2001 skonsultowano się z Europejskim Inspektorem Ochrony Danych, który wydał opinię w dniu XX/XX/XXXX,

PRZYJMUJĄ NINIEJSZE ROZPORZĄDZENIE:

ROZDZIAŁ I

PRZEPISY OGÓLNE

Artykuł 1
Przedmiot i cele

1. W niniejszym rozporządzeniu ustanawia się przepisy o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez unijne instytucje, organy i jednostki organizacyjne oraz przepisy o swobodnym przepływie danych osobowych między nimi lub do odbiorców posiadających jednostkę organizacyjną w Unii

[17] Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 223/2009 z dnia 11 marca 2009 r. w sprawie statystyki europejskiej oraz uchylające rozporządzenie Parlamentu Europejskiego i Rady (WE, Euratom) nr 1101/2008 w sprawie przekazywania do Urzędu Statystycznego Wspólnot Europejskich danych statystycznych objętych zasadą poufności, rozporządzenie Rady (WE) nr 322/97 w sprawie statystyk Wspólnoty oraz decyzję Rady 89/382/EWG, Euratom w sprawie ustanowienia Komitetu ds. Programów Statystycznych Wspólnot Europejskich (Dz.U. L 87 z 31.3.2009, s. 164).

podlegającym rozporządzeniu (UE) 2016/679[18] lub przepisom prawa krajowego przyjętego zgodnie z dyrektywą (UE) 2016/680[19].

2. Niniejsze rozporządzenie chroni podstawowe prawa i wolności osób fizycznych, w szczególności ich prawo do ochrony danych osobowych.

3. Europejski Inspektor Ochrony Danych (EIOD) monitoruje stosowanie przepisów niniejszego rozporządzenia w odniesieniu do wszystkich operacji przetwarzania przeprowadzanych przez instytucję unijną lub organ unijny.

Artykuł 2
Zakres stosowania

1. Niniejsze rozporządzenie stosuje się do przetwarzania danych osobowych przez wszystkie instytucje i organy unijne, o ile takie przetwarzanie jest prowadzone podczas wykonywania czynności całkowicie lub częściowo podlegających prawu Unii.

2. Niniejsze rozporządzenie 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.

Artykuł 3
Definicje

1. Do celów niniejszego rozporządzenia stosuje się następujące definicje:

   a) definicje zawarte w rozporządzeniu (UE) 2016/679 z wyjątkiem definicji „administratora” zawartej w art. 4 pkt 7 tego rozporządzenia;

   b) definicję „łączności elektronicznej” zawartą w art. 4 ust. 2 lit. a) rozporządzenia (UE) XX/XXXX [rozporządzenia o prywatności elektronicznej];

   c) definicje „sieci łączności elektronicznej” i „użytkownika końcowego” zawarte odpowiednio w art. 2 pkt 1 i 14 dyrektywy 00/0000/UE [dyrektywy ustanawiającej europejski kodeks łączności elektronicznej];

   d) definicję „końcowego urządzenia” zawartą w art. 1 pkt 1 dyrektywy Komisji 2008/63/WE[20].

---

[18] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Tekst mający znaczenie dla EOG), Dz.U. L 119 z 4.5.2016, s. 1–88.

[19] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW, Dz.U. L 119 z 4.5.2016, s. 89–131.

2. Ponadto do celów niniejszego rozporządzenia stosuje się następujące definicje:

a) „instytucje i organy unijne” oznaczają unijne instytucje, organy i jednostki organizacyjne ustanowione Traktatem o funkcjonowaniu Unii Europejskiej, Traktatem o Unii Europejskiej lub Traktatem Euratom lub na ich podstawie;

b) „administrator” oznacza instytucję, organ, urząd lub agencję Unii lub dyrekcję generalną lub jakąkolwiek inną jednostkę organizacyjną, która samodzielnie lub wspólnie z innymi określa cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby przetwarzania danych są określone w szczególnym akcie Unii, prawo Unii może przewidywać wyznaczenie administratora lub może określać szczególne kryteria jego wyznaczania;

c) „użytkownik” oznacza każdą osobę fizyczną korzystającą z sieci lub z końcowego urządzenia telekomunikacyjnego, działających pod kontrolą instytucji unijnej lub organu unijnego;

d) „spis” oznacza dostępny publicznie spis użytkowników lub wewnętrzny spis użytkowników dostępny w instytucji unijnej lub organie unijnym lub wspólny dla instytucji i organów unijnych, zarówno w formie drukowanej, jak i elektronicznej.

ROZDZIAŁ II

ZASADY

Artykuł 4
Zasady dotyczące przetwarzania danych osobowych

1. Dane osobowe muszą być:

a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość”);

b) zbierane w konkretnych, wyraźnych i uzasadnionych celach i nieprzetwarzane w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 13 za niezgodne z pierwotnymi celami („ograniczenie celu”);

c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych”);

d) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe lub niekompletne w

[20] Dyrektywa Komisji 2008/63/WE z dnia 20 czerwca 2008 r. w sprawie konkurencji na rynkach końcowych urządzeń telekomunikacyjnych (Dz.U. L 162 z 21.6.2008, s. 20).

świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość”);

e) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 13, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą („ograniczenie przechowywania”);

f) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność”).

2. Administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie („rozliczalność”).

Artykuł 5
Zgodność przetwarzania z prawem

1. Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – spełniony jest co najmniej jeden z poniższych warunków:

a) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym na podstawie lub w ramach sprawowania władzy publicznej powierzonej unijnej instytucji lub unijnemu organowi;

b) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;

c) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;

d) osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;

e) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej.

2. Zadania, o których mowa w ust. 1 lit. a), są określone w prawie Unii.

Artykuł 6
Przetwarzanie w innym zgodnym celu

Jeżeli przetwarzanie w celu innym niż cel, w którym dane osobowe zostały zebrane, nie odbywa się na podstawie zgody osoby, której dane dotyczą, ani prawa Unii stanowiących w demokratycznym społeczeństwie niezbędny i proporcjonalny środek służący zagwarantowaniu celów, o których mowa w art. 25 ust. 1, administrator – aby ustalić, czy przetwarzanie w innym celu jest zgodne z celem, w którym dane osobowe zostały pierwotnie zebrane – bierze pod uwagę między innymi:

a) wszelkie związki między celami, w których zebrano dane osobowe, a celami zamierzonego dalszego przetwarzania;

b) kontekst, w którym zebrano dane osobowe, w szczególności relację między osobami, których dane dotyczą, a administratorem;

c) charakter danych osobowych, w szczególności czy przetwarzane są szczególne kategorie danych osobowych zgodnie z art. 10 lub dane osobowe dotyczące wyroków skazujących i naruszeń prawa zgodnie z art. 11;

d) ewentualne konsekwencje zamierzonego dalszego przetwarzania dla osób, których dane dotyczą;

e) istnienie odpowiednich zabezpieczeń, w tym ewentualnie szyfrowania lub pseudonimizacji.

Artykuł 7
Warunki wyrażenia zgody

1. Jeżeli przetwarzanie odbywa się na podstawie zgody, administrator musi być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych.

2. Jeżeli osoba, której dane dotyczą, wyrażą zgodę w pisemnym oświadczeniu, które dotyczy także innych kwestii, zapytanie o zgodę musi zostać przedstawione w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii, w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem. Część takiego oświadczenia osoby, której dane dotyczą, stanowiąca naruszenie niniejszego rozporządzenia nie jest wiążąca.

3. Osoba, której dane dotyczą, ma prawo w dowolnym momencie wycofać zgodę. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem. Osoba, której dane dotyczą, jest o tym informowana, zanim wyrazi zgodę. Wycofanie zgody musi być równie łatwe jak jej wyrażenie.

4. Oceniając, czy zgodę wyrażono dobrowolnie, w jak największym stopniu uwzględnia się, czy między innymi od zgody na przetwarzanie danych nie jest uzależnione wykonanie umowy, w tym świadczenie usługi, jeśli przetwarzanie danych osobowych nie jest niezbędne do wykonania tej umowy.

Artykuł 8

Warunki wyrażenia zgody przez dzieci w przypadku usług społeczeństwa informacyjnego

1. Jeżeli zastosowanie ma art. 5 ust. 1 lit. d), w przypadku usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku, zgodne z prawem jest przetwarzanie danych osobowych dziecka, które ukończyło 13 lat. Jeżeli dziecko nie ukończyło 13 lat, takie przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy zgodę wyraziła lub zaaprobowała ją osoba sprawująca władzę rodzicielską lub opiekę nad dzieckiem oraz wyłącznie w zakresie wyrażonej zgody.

2. W takich przypadkach administrator, uwzględniając dostępną technologię, podejmuje rozsądne starania, by zweryfikować, czy osoba sprawująca władzę rodzicielską lub opiekę nad dzieckiem wyraziła zgodę lub ją zaaprobowała.

3. Ustęp 1 nie wpływa na ogólne przepisy prawa umów państw członkowskich, takie jak przepisy o ważności, zawieraniu lub skutkach umowy wobec dziecka.

Artykuł 9

Przekazywanie danych osobowych odbiorcom innym niż instytucje i organy unijne posiadającym jednostkę organizacyjną w Unii i podlegającym rozporządzeniu (UE) 2016/679 lub dyrektywie (UE) 2016/680

1. Z zastrzeżeniem art. 4, 5, 6 i 10, dane osobowe przekazuje się odbiorcom posiadającym jednostkę organizacyjną w Unii i podlegającym rozporządzeniu (UE) 2016/679 lub prawu krajowemu przyjętemu zgodnie z dyrektywą (UE) 2016/680, wyłącznie jeżeli odbiorca stwierdzi:

   a) że dane są niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej; lub

   b) że przekazanie danych jest niezbędne, jest proporcjonalne do celów przekazania oraz jeżeli nie ma powodu, by zakładać, że prawa i wolności oraz uzasadnione interesy, osoby której dane dotyczą, mogłyby zostać naruszone.

2. Jeżeli przekazanie zgodnie z niniejszym artykułem odbywa się z inicjatywy administratora, administrator wykazuje, że przekazanie danych osobowych jest niezbędne i proporcjonalne do celów przekazania, stosując kryteria ustanowione w ust. 1 lit. a) i b).

Artykuł 10

Przetwarzanie szczególnych kategorii danych osobowych

1. Zabrania się przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby.

2. Ust. 1 nie ma zastosowania, jeżeli spełniony jest jeden z poniższych warunków:

a) osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach, chyba że prawo Unii przewiduje, iż osoba, której dane dotyczą, nie może uchylić zakazu, o którym mowa w ust. 1; lub

b) przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem Unii przewidującym odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą; lub

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

d) przetwarzania dokonuje się w ramach uprawnionej działalności prowadzonej z zachowaniem odpowiednich zabezpieczeń przez niezarobkowy podmiot, który stanowi zintegrowaną jednostkę w ramach instytucji unijnej lub organu unijnego oraz posiada cele polityczne, światopoglądowe, religijne lub związkowe, pod warunkiem że przetwarzanie dotyczy wyłącznie członków lub byłych członków tego podmiotu lub osób utrzymujących z nim stałe kontakty w związku z jego celami oraz że dane nie są ujawniane poza tym podmiotem bez zgody osób, których dane dotyczą;

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

f) przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez Trybunał Sprawiedliwości Unii Europejskiej; lub

g) przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii, które jest proporcjonalne do wyznaczonego celu, nie narusza istoty prawa do ochrony danych i przewiduje odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą;

h) przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub zgodnie z umową z pracownikiem służby zdrowia i z zastrzeżeniem warunków i zabezpieczeń, o których mowa w ust. 3;

i) przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa Unii, które przewiduje odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową;

j) przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, na podstawie prawa Unii, które jest proporcjonalne do wyznaczonego celu, nie narusza istoty prawa do ochrony danych i przewiduje odpowiednie, konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.

3. Dane osobowe, o których mowa w ust. 1, mogą być przetwarzane do celów, o których mowa w ust. 2 lit. h), jeżeli są przetwarzane przez – lub na odpowiedzialność – pracownika podlegającego obowiązkowi zachowania tajemnicy zawodowej na mocy prawa Unii.

Artykuł 11
Przetwarzanie danych osobowych dotyczących wyroków skazujących i naruszeń prawa

Przetwarzania danych osobowych dotyczących wyroków skazujących oraz naruszeń prawa lub powiązanych środków bezpieczeństwa na podstawie art. 5 ust. 1 można dokonywać wyłącznie, jeżeli jest ono dozwolone prawem Unii, które może obejmować przepisy wewnętrzne przewidujące odpowiednie szczególne zabezpieczenia praw i wolności osób, których dane dotyczą.

Artykuł 12
Przetwarzanie niewymagające identyfikacji

1. Jeżeli cele, w których administrator przetwarza dane osobowe, nie wymagają lub już nie wymagają zidentyfikowania przez niego osoby, której dane dotyczą, administrator nie ma obowiązku zachowania, uzyskania ani przetworzenia dodatkowych informacji w celu zidentyfikowania osoby, której dane dotyczą, wyłącznie po to, by zastosować się do niniejszego rozporządzenia.

2. Jeżeli w przypadkach, o których mowa w ust. 1 niniejszego artykułu, administrator może wykazać, że nie jest w stanie zidentyfikować osoby, której dane dotyczą, w miarę możliwości informuje o tym osobę, której dane dotyczą. W takich przypadkach zastosowania nie mają art. 17–22, chyba że osoba, której dane dotyczą, w celu wykonania praw przysługujących jej na mocy tych artykułów dostarczy dodatkowych informacji pozwalających ją zidentyfikować.

Artykuł 13
Zabezpieczenia mające zastosowanie do przetwarzania do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych

Przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych podlega odpowiednim zabezpieczeniom dla praw i wolności osoby, której dane dotyczą, zgodnie z niniejszym rozporządzeniem. Zabezpieczenia te polegają na wdrożeniu środków technicznych i organizacyjnych zapewniających poszanowanie zasady minimalizacji danych. Środki te mogą też obejmować pseudonimizację danych, o ile pozwala ona realizować powyższe cele. Jeżeli cele te można zrealizować w drodze dalszego przetwarzania danych, które nie pozwalają albo przestały pozwalać na zidentyfikować osoby, której dane dotyczą, cele należy realizować w ten sposób.

ROZDZIAŁ III

PRAWA OSOBY, KTÓREJ DANE DOTYCZĄ

SEKCJA 1

PRZEJRZYSTOŚĆ ORAZ TRYB KORZYSTANIA Z PRAW

Artykuł 14
Przejrzyste informowanie i przejrzysta komunikacja oraz tryb wykonywania praw przez osobę, której dane dotyczą

1. Administrator podejmuje odpowiednie środki, aby w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem – w szczególności gdy informacje są kierowane do dziecka – udzielić osobie, której dane dotyczą, wszelkich informacji, o których mowa w art. 15 i 16, oraz prowadzić z nią wszelką komunikację na mocy art. 17–24 i 38 w sprawie przetwarzania. Informacji udziela się na piśmie lub w inny sposób, w tym w stosownych przypadkach – elektronicznie. Jeżeli osoba, której dane dotyczą, tego zażąda, informacji można udzielić ustnie, o ile innymi sposobami potwierdzi się tożsamość osoby, której dane dotyczą.

2. Administrator ułatwia osobie, której dane dotyczą, wykonanie praw przysługujących jej na mocy art. 17–24. W przypadkach, o których mowa w art. 12 ust. 2, administrator nie odmawia podjęcia działań na żądanie osoby której dane dotyczą pragnącej wykonać prawa przysługujące jej na mocy art. 17–24, chyba że wykaże, iż nie jest w stanie zidentyfikować osoby, której dane dotyczą.

3. Administrator bez zbędnej zwłoki – a w każdym razie w terminie miesiąca od otrzymania żądania – udziela osobie, której dane dotyczą, informacji o działaniach podjętych w związku z żądaniem na podstawie art. 17–24. W razie potrzeby termin ten można przedłużyć o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań. W terminie miesiąca od otrzymania żądania administrator informuje osobę, której dane dotyczą o takim przedłużeniu terminu, z podaniem przyczyn opóźnienia. Jeśli osoba, której dane dotyczą, przekazała swoje żądanie elektronicznie, w miarę możliwości informacje są także przekazywane elektronicznie, chyba że osoba, której dane dotyczą, zażąda innej formy.

4. Jeżeli administrator nie podejmuje działań w związku z żądaniem osoby, której dane dotyczą, to niezwłocznie – najpóźniej w terminie miesiąca od otrzymania żądania – informuje osobę, której dane dotyczą, o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do Europejskiego Inspektora Ochrony Danych oraz skorzystania ze środków ochrony prawnej przed sądem.

5. Informacje podawane na mocy art. 15 i 16 oraz komunikacja i działania podejmowane na mocy art. 17–24 i 38 są wolne od opłat. Jeżeli żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze

względu na swój ustawiczny charakter, administrator może odmówić podjęcia działań w związku z żądaniem.

Obowiązek wykazania, że żądanie ma ewidentnie nieuzasadniony lub nadmierny charakter, spoczywa na administratorze.

6. Bez uszczerbku dla art. 12, jeżeli administrator ma uzasadnione wątpliwości co do tożsamości osoby fizycznej składającej żądanie, o którym mowa w art. 17–23, może zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby, której dane dotyczą.

7. Informacje, których udziela się osobom, których dane dotyczą, na mocy art. 15 i 16, można opatrzyć standardowymi znakami graficznymi, które w widoczny, zrozumiały i czytelny sposób przedstawią sens zamierzonego przetwarzania. Jeżeli znaki te są przedstawione elektronicznie, muszą się nadawać do odczytu maszynowego.

8. Jeżeli Komisja przyjmuje akty delegowane zgodnie z art. 12 ust. 8 rozporządzenia (UE) 2016/679 określające informacje przedstawiane za pomocą znaków graficznych i procedury ustanowienia standardowych znaków graficznych, instytucje i organy unijne przekazują informacje zgodnie z art. 15 i 16 w połączeniu ze standardowymi znakami graficznymi.

SEKCJA 2

INFORMACJE I DOSTĘP DO DANYCH OSOBOWYCH

Artykuł 15
Informacje podawane w przypadku zbierania danych od osoby, której dane dotyczą

1. Jeżeli dane osobowe osoby, której dane dotyczą, zbierane są od tej osoby, administrator podczas pozyskiwania danych osobowych podaje jej wszystkie następujące informacje:

   a) tożsamość i dane kontaktowe administratora;

   b) dane kontaktowe inspektora ochrony danych;

   c) cele przetwarzania danych osobowych oraz podstawę prawną przetwarzania;

   d) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;

   e) gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 49, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych.

2. Poza informacjami, o których mowa w ust. 1, podczas pozyskiwania danych osobowych administrator podaje osobie, której dane dotyczą, następujące inne informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania:

   a) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;

   b) informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub, w stosownych przypadkach, o prawie do wniesienia sprzeciwu wobec przetwarzania lub o prawie do przenoszenia danych;

   c) jeżeli przetwarzanie odbywa się na podstawie art. 5 ust. 1 lit. d) lub art. 10 ust. 2 lit. a) – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;

   d) informacje o prawie wniesienia skargi do Europejskiego Inspektora Ochrony Danych;

   e) informację, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;

   f) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 24 ust. 1 i 4, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

3. Jeżeli administrator planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym dane osobowe zostały zebrane, przed takim dalszym przetwarzaniem informuje on osobę, której dane dotyczą, o tym innym celu oraz udziela jej wszelkich innych stosownych informacji, o których mowa w ust. 2.

4. Ust. 1, 2 i 3 nie mają zastosowania, gdy – i w zakresie, w jakim – osoba, której dane dotyczą, dysponuje już tymi informacjami.

Artykuł 16
Informacje podawane w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą

1. Jeżeli danych osobowych nie pozyskano od osoby, której dane dotyczą, administrator podaje osobie, której dane dotyczą, następujące informacje:

   a) tożsamość i dane kontaktowe administratora;

   b) dane kontaktowe inspektora ochrony danych;

c) cele przetwarzania danych osobowych oraz podstawę prawną przetwarzania;

d) kategorie odnośnych danych osobowych;

e) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;

f) gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych odbiorcy w państwie trzecim lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 49, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych.

2. Poza informacjami, o których mowa w ust. 1, administrator podaje osobie, której dane dotyczą, następujące dalsze informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania wobec osoby, której dane dotyczą:

a) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;

b) informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub, w stosownych przypadkach, o prawie do wniesienia sprzeciwu wobec przetwarzania lub o prawie do przenoszenia danych;

c) jeżeli przetwarzanie odbywa się na podstawie art. 5 ust. 1 lit. d) lub art. 10 ust. 2 lit. a) – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;

d) informacje o prawie wniesienia skargi do Europejskiego Inspektora Ochrony Danych;

e) źródło pochodzenia danych osobowych, a gdy ma to zastosowanie – czy pochodzą one ze źródeł publicznie dostępnych;

f) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 24 ust. 1 i 4, oraz – co najmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

3. Informacje, o których mowa w ust. 1 i 2, administrator podaje:

a) w rozsądnym terminie po pozyskaniu danych osobowych – najpóźniej w ciągu miesiąca – mając na uwadze konkretne okoliczności przetwarzania danych osobowych;

b) jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą – najpóźniej przy pierwszej takiej komunikacji z osobą, której dane dotyczą; lub

c) jeżeli planuje się ujawnić dane osobowe innemu odbiorcy – najpóźniej przy ich pierwszym ujawnieniu.

4. Jeżeli administrator planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym te dane zostały pozyskane, przed takim dalszym przetwarzaniem informuje on osobę, której dane dotyczą, o tym innym celu oraz udziela jej wszelkich innych stosownych informacji, o których mowa w ust. 2.

5. Ust. 1– 4 nie mają zastosowania, gdy – i w zakresie, w jakim:

a) osoba, której dane dotyczą, dysponuje już tymi informacjami;

b) udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku; w szczególności w przypadku przetwarzania do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych lub o ile obowiązek, o którym mowa w ust. 1 niniejszego artykułu, może uniemożliwić lub poważnie utrudnić realizację celów takiego przetwarzania;

c) pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem Unii; lub

d) dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianym w prawie Unii.

Artykuł 17
Prawo dostępu przysługujące osobie, której dane dotyczą

1. Osoba, której dane dotyczą, jest uprawniona do uzyskania od administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz następujących informacji:

a) cele przetwarzania;

b) kategorie odnośnych danych osobowych;

c) informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;

d) w miarę możliwości planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu;

e) informacje o prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania;

f) informacje o prawie wniesienia skargi do Europejskiego Inspektora Ochrony Danych;

g) jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle;

h) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 24 ust. 1 i 4, oraz – co najmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

2. Jeżeli dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej, osoba, której dane dotyczą, ma prawo zostać poinformowana o odpowiednich zabezpieczeniach, o których mowa w art. 49, związanych z przekazaniem.

3. Administrator dostarcza osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu. Jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się powszechnie stosowaną drogą elektroniczną.

4. Prawo do uzyskania kopii, o której mowa w ust. 3, nie może niekorzystnie wpływać na prawa i wolności innych.

SEKCJA 3

SPROSTOWANIE I USUWANIE DANYCH

Artykuł 18
Prawo do sprostowania danych

Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe. Z uwzględnieniem celów przetwarzania, osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.

Artykuł 19
Prawo do usunięcia danych („prawo do bycia zapomnianym”)

1. Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli zachodzi jedna z następujących okoliczności:

a) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;

b) osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie zgodnie z art. 5 ust. 1 lit. d) lub art. 10 ust. 2 lit. a), i nie ma innej podstawy prawnej przetwarzania;

c) osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 23 ust. 1 wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania;

d) dane osobowe były przetwarzane niezgodnie z prawem;

e) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego, któremu podlega administrator;

f) dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego, o których mowa w art. 8 ust. 1.

2. Jeżeli administrator upublicznił dane osobowe, a na mocy ust. 1 ma obowiązek usunąć te dane osobowe, to – biorąc pod uwagę dostępną technologię i koszt realizacji – podejmuje rozsądne działania, w tym środki techniczne, by poinformować administratorów przetwarzających te dane osobowe, że osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje.

3. Ust. 1 i 2 nie mają zastosowania, w zakresie w jakim przetwarzanie jest niezbędne:

a) do korzystania z prawa do wolności wypowiedzi i informacji;

b) do wywiązania się z prawnego obowiązku, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;

c) z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego zgodnie z art. 10 ust. 2 lit. h) oraz i) i art. 10 ust. 3;

d) do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, o ile prawdopodobne jest, że prawo, o którym mowa w ust. 1, uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania; lub

e) do ustalenia, dochodzenia lub obrony roszczeń.

Artykuł 20
Prawo do ograniczenia przetwarzania

1. Osoba, której dane dotyczą, ma prawo żądania od administratora ograniczenia przetwarzania w następujących przypadkach:

a) osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych – na okres pozwalający administratorowi sprawdzić prawidłowość tych danych, w tym ich kompletności;

b) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się ich usunięciu, żądając w zamian ograniczenia ich wykorzystywania;

c) administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;

d) osoba, której dane dotyczą, wniosła sprzeciw na mocy art. 23 ust. 1 wobec przetwarzania – do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie administratora są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.

2. Jeżeli na mocy ust. 1 przetwarzanie zostało ograniczone, takie dane osobowe można przetwarzać, z wyjątkiem przechowywania, wyłącznie za zgodą osoby, której dane dotyczą, lub w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii lub państwa członkowskiego.

3. Przed uchyleniem ograniczenia przetwarzania administrator informuje o tym osobę, której dane dotyczą, która żądała ograniczenia na mocy ust. 1.

4. W zautomatyzowanych zbiorach danych ograniczenie przetwarzania danych osobowych należy zasadniczo zapewnić za pomocą środków technicznych. Fakt, że dostęp do danych osobowych jest ograniczony, jest wskazywany w systemie w taki sposób, aby było jasne, że dane osobowe nie mogą być wykorzystane.

Artykuł 21
Obowiązek powiadomienia o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania

Administrator informuje o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania, których dokonał zgodnie z art. 18, art. 19 ust. 1 i art. 20, każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Administrator informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.

Artykuł 22
Prawo do przenoszenia danych

1. Osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła administratorowi, oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe, jeżeli:

a) przetwarzanie odbywa się na podstawie zgody w myśl art. 5 ust. 1 lit. d) lub art. 10 ust. 2 lit. a) lub na podstawie umowy w myśl art. 5 ust. 1 lit. c); oraz

b) przetwarzanie odbywa się w sposób zautomatyzowany.

2. Wykonując prawo do przenoszenia danych na mocy ust. 1, osoba, której dane dotyczą, ma prawo żądania, by dane osobowe zostały przesłane przez administratora bezpośrednio innemu administratorowi, o ile jest to technicznie możliwe.

3. Wykonanie prawa, o którym mowa w ust. 1 niniejszego artykułu, pozostaje bez uszczerbku dla art. 19. Prawo to nie ma zastosowania do przetwarzania, które jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.

4. Prawo, o którym mowa w ust. 1, nie może niekorzystnie wpływać na prawa i wolności innych.

SEKCJA 4

PRAWO DO SPRZECIWU ORAZ ZAUTOMATYZOWANE PODEJMOWANIE DECYZJI W INDYWIDUALNYCH PRZYPADKACH

Artykuł 23
Prawo do sprzeciwu

1. Osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych opartego na art. 5 ust. 1 lit. a), w tym profilowania na podstawie tego przepisu. Administratorowi nie wolno już przetwarzać tych danych osobowych, chyba że wykaże on istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.

2. Najpóźniej przy okazji pierwszej komunikacji z osobą, której dane dotyczą, wyraźnie informuje się ją o prawie, o którym mowa w ust. 1, oraz przedstawia się je jasno i odrębnie od wszelkich innych informacji.

3. Z zastrzeżeniem art. 34 i 35 oraz w związku z korzystaniem z usług społeczeństwa informacyjnego, osoba, której dane dotyczą, może wykonać prawo do sprzeciwu za pośrednictwem zautomatyzowanych środków wykorzystujących specyfikacje techniczne.

4. Jeżeli dane osobowe są przetwarzane do celów badań naukowych lub historycznych lub do celów statystycznych, osoba, której dane dotyczą, ma prawo wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczącego jej danych osobowych, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.

Artykuł 24
Zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach, w tym profilowanie

1. Osoba, której dane dotyczą, ma prawo do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa.

2. Ust. 1 nie ma zastosowania, jeżeli ta decyzja:

   a) jest niezbędna do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a administratorem;

   b) jest dozwolona prawem Unii, które przewiduje właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą; lub

   c) opiera się na wyraźnej zgodzie osoby, której dane dotyczą.

3. W przypadkach, o których mowa w ust. 2 lit. a) i c), administrator danych wdraża właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą, a co najmniej prawa do uzyskania interwencji ludzkiej ze strony administratora, do wyrażenia własnego stanowiska i do zakwestionowania tej decyzji.

4. Decyzje, o których mowa w ust. 2, nie mogą opierać się na szczególnych kategoriach danych osobowych, o których mowa w art. 10 ust. 1, chyba że zastosowanie ma art. 10 ust. 2 lit. a) lub g) i istnieją właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą.

SEKCJA 5

OGRANICZENIA

Artykuł 25
Ograniczenia

1. Akty prawne przyjęte na podstawie Traktatów lub, w sprawach odnoszących się do działalności instytucji i organów unijnych, regulaminy przyjęte przez te ostatnie mogą ograniczyć zastosowanie art. 14–22, art. 34 i 38, a także art. 4 – o ile ich przepisy odpowiadają prawom i obowiązkom przewidzianym w art. 14–22 – w przypadku gdy ograniczenie takie nie narusza istoty podstawowych praw i wolności oraz jest w demokratycznym społeczeństwie środkiem niezbędnym i proporcjonalnym, służącym:

   a) bezpieczeństwu narodowemu, bezpieczeństwu publicznemu lub obronności państw członkowskich;

   b) zapobieganiu przestępczości, prowadzeniu postępowań przygotowawczych, wykrywaniu i ściganiu czynów zabronionych lub wykonywaniu kar, w tym

ochronie przed zagrożeniami dla bezpieczeństwa publicznego i zapobieganiu takim zagrożeniom;

c) innym ważnym celom leżącym w ogólnym interesie publicznym Unii lub państwa członkowskiego, w szczególności ważnemu interesowi gospodarczemu lub finansowemu Unii lub państwa członkowskiego, w tym kwestiom pieniężnym, budżetowym i podatkowym, zdrowiu publicznemu i zabezpieczeniu społecznemu;

d) bezpieczeństwu wewnętrznemu instytucji i organów unijnych, w tym ich sieci łączności elektronicznej;

e) ochronie niezależności sądów i postępowania sądowego;

f) zapobieganiu naruszeniom zasad etyki w zawodach regulowanych, prowadzeniu postępowań w takich sprawach, ich wykrywaniu oraz ściganiu;

g) funkcjom kontrolnym, inspekcyjnym lub regulacyjnym związanym, nawet sporadycznie, ze sprawowaniem władzy publicznej w przypadkach, o których mowa w lit. a) – c);

h) ochronie osoby, której dane dotyczą, lub praw i wolności innych osób;

i) egzekucji roszczeń cywilnoprawnych.

2. Jeżeli nie przewidziano ograniczenia w akcie prawnym przyjętym na podstawie Traktatów lub w przepisie wewnętrznym zgodnie z ust. 1, instytucje i organy unijne mogą ograniczyć zastosowanie art. 14–22, art. 34 i 38, a także art. 4 – w zakresie, w jakim ich przepisy odpowiadają prawom i obowiązkom przewidzianym w art. 14–22 – jeżeli ograniczenie takie nie narusza istoty podstawowych praw i wolności w odniesieniu do szczególnych operacji przetwarzania oraz jest w demokratycznym społeczeństwie środkiem niezbędnym i proporcjonalnym, służącym jednemu celowi, o którym mowa w ust. 1, lub ich większej liczbie. Takie ograniczenie zgłasza się właściwemu inspektorowi ochrony danych.

3. W przypadku przetwarzania danych osobowych do celów badań naukowych lub historycznych lub do celów statystycznych prawo Unii, które może obejmować przepisy wewnętrzne, może przewidywać wyjątki od praw, o których mowa w art. 17, 18, 20 i 23, z zastrzeżeniem warunków i zabezpieczeń, o których mowa w art. 13, w zakresie, w jakim jest prawdopodobne, że prawa te uniemożliwią lub poważnie utrudnią realizację wspomnianych konkretnych celów, i jeżeli wyjątki takie są konieczne do realizacji tych celów.

4. W przypadku przetwarzania danych osobowych do celów archiwalnych w interesie publicznym prawo Unii, które może obejmować przepisy wewnętrzne, może przewidywać wyjątki od praw, o których mowa w art. 17, 18, 20 i 21, 22 i 23 z zastrzeżeniem warunków i zabezpieczeń, o których mowa w art. 13, w zakresie, w jakim jest prawdopodobne, że prawa te uniemożliwią lub poważnie utrudnią realizację wspomnianych konkretnych celów, i jeżeli wyjątki takie są konieczne do realizacji tych celów.

5. Przepisy wewnętrzne, o których mowa w ust. 1, 3 i 4, są wystarczająco jasne i precyzyjne, by można je było w odpowiedni sposób opublikować.

6. Jeżeli nałożono ograniczenie zgodnie z ust. 1 lub 2, osoba, której dane dotyczą, zostaje poinformowana zgodnie z prawem Unii o podstawowych powodach, na których opiera się stosowanie ograniczenia, oraz jej prawie do wniesienia skargi do Europejskiego Inspektora Ochrony Danych.

7. Jeżeli osobie, której dane dotyczą, odmówiono dostępu do danych w oparciu o ograniczenie nałożone zgodnie z ust. 1 lub 2, Europejski Inspektor Ochrony Danych po rozważeniu skargi informuje ją, czy dane zostały przetworzone prawidłowo i jeżeli nie, czy dokonano koniecznych poprawek.

8. Można wstrzymać przekazanie informacji, o których mowa w ust. 6 i 7 i w art. 46 ust. 2, pominąć je lub go odmówić, jeżeli unieważniłoby to skutek ograniczenia nałożonego zgodnie z ust. 1 lub 2.

ROZDZIAŁ IV

ADMINISTRATOR I PODMIOT PRZETWARZAJĄCY

SEKCJA 1

OBOWIĄZKI OGÓLNE

Artykuł 26
Obowiązki administratora

1. 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.

2. Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki, o których mowa w ust. 1, obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych.

Artykuł 27
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.

Artykuł 28
Współadministratorzy

1. Jeżeli instytucja unijna lub organ unijny wraz z jednym administratorem lub z ich większą liczbą, którymi mogą, lecz nie muszą być unijne instytucje lub organy, wspólnie ustalają cele i sposoby przetwarzania, są oni współadministratorami. W drodze wspólnych uzgodnień współadministratorzy w przejrzysty sposób określają odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków ochrony danych, w szczególności w odniesieniu do wykonywania przez osobę, której dane dotyczą, przysługujących jej praw, oraz ich obowiązków w odniesieniu do podawania informacji, o których mowa w art. 15 i 16, chyba że przypadające im obowiązki i ich zakres określa prawo Unii lub prawo państwa członkowskiego, któremu administratorzy ci podlegają. W uzgodnieniach można wskazać punkt kontaktowy dla osób, których dane dotyczą.

2. Uzgodnienia, o których mowa w ust. 1, należycie odzwierciedlają odpowiednie zakresy obowiązków współadministratorów oraz relacje pomiędzy nimi a podmiotami, których dane dotyczą. Zasadnicza treść uzgodnień jest udostępniana podmiotom, których dane dotyczą.

3. Osoba, której dane dotyczą, może wykonywać przysługujące jej prawa wynikające z niniejszego rozporządzenia wobec każdego ze współadministratorów, uwzględniając ich role określone w uzgodnieniach, o których mowa w ust. 1.

Artykuł 29
Podmiot przetwarzający

1. Jeżeli przetwarzanie ma być dokonywane w imieniu administratora, korzysta on wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi niniejszego rozporządzenia i chroniło prawa osób, których dane dotyczą.

2. Podmiot przetwarzający nie korzysta z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody administratora. W przypadku ogólnej pisemnej zgody podmiot przetwarzający informuje administratora o

wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających, dając tym samym administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian.

3. Przetwarzanie przez podmiot przetwarzający odbywa się na podstawie umowy lub innego instrumentu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego i wiążą podmiot przetwarzający i administratora, określają przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora. Ta umowa lub inny instrument prawny stanowią w szczególności, że podmiot przetwarzający:

a) przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora – co dotyczy też przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej – chyba że obowiązek taki nakłada na niego prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający; w takim przypadku przed rozpoczęciem przetwarzania podmiot przetwarzający informuje administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny;

b) zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;

c) podejmuje wszelkie środki wymagane na mocy art. 33;

d) przestrzega warunków korzystania z usług innego podmiotu przetwarzającego, o których mowa w ust. 2 i 4;

e) biorąc pod uwagę charakter przetwarzania, w miarę możliwości pomaga administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III;

f) uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga administratorowi wywiązać się z obowiązków określonych w art. 33–40;

g) po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji administratora usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych;

h) udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w niniejszym artykule oraz umożliwia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich.

W związku z obowiązkiem określonym w akapicie pierwszym lit. h) podmiot przetwarzający niezwłocznie informuje administratora, jeżeli jego zdaniem wydane mu polecenie stanowi naruszenie niniejszego rozporządzenia lub innych przepisów Unii lub państwa członkowskiego o ochronie danych.

4. Jeżeli do wykonania w imieniu administratora konkretnych czynności przetwarzania podmiot przetwarzający korzysta z usług innego podmiotu przetwarzającego, na ten inny podmiot przetwarzający nałożone zostają – na mocy umowy lub innego aktu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego – te same obowiązki ochrony danych jak w umowie lub innym akcie prawnym między administratorem a podmiotem przetwarzającym, o których to obowiązkach mowa w ust. 3, w szczególności obowiązek zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom niniejszego rozporządzenia. Jeżeli ten inny podmiot przetwarzający nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec administratora za wypełnienie obowiązków tego innego podmiotu przetwarzającego spoczywa na pierwotnym podmiocie przetwarzającym.

5. Jeżeli podmiot przetwarzający nie jest instytucją unijną lub organem unijnym, wystarczającymi gwarancjami, o których mowa w ust. 1 i 4 niniejszego artykułu, może wykazać się między innymi dzięki stosowaniu zatwierdzonego kodeksu postępowania, o którym mowa w art. 40 ust. 5 rozporządzenia (UE) 2016/679 lub zatwierdzonego mechanizmu certyfikacji, o którym mowa w art. 42 rozporządzenia (UE) 2016/679.

6. Bez uszczerbku dla indywidualnych umów między administratorem a podmiotem przetwarzającym, umowa lub inny akt prawny, o których mowa w ust. 3 i 4 niniejszego artykułu, mogą się opierać w całości lub w części na standardowych klauzulach umownych, o których mowa w ust. 7 i 8 niniejszego artykułu, także gdy są one elementem certyfikacji udzielonej podmiotowi przetwarzającemu innemu niż instytucja unijna lub organ unijny zgodnie z art. 42 rozporządzenia (UE) 2016/679.

7. Komisja może określić standardowe klauzule umowne dotyczące kwestii, o których mowa w ust. 3 i 4 niniejszego artykułu, zgodnie z procedurą sprawdzającą, o której mowa w art. 70 ust. 2.

8. Europejski Inspektor Ochrony Danych może przyjąć standardowe klauzule umowne dotyczące kwestii, o których mowa w ust. 3 i 4.

9. Umowa lub inny akt prawny, o których mowa w ust. 3 i 4, mają formę pisemną, w tym formę elektroniczną.

10. Bez uszczerbku dla art. 65 i 66, jeżeli podmiot przetwarzający narusza niniejsze rozporządzenie przy określaniu celów i sposobów przetwarzania, uznaje się go za administratora w odniesieniu do tego przetwarzania.

Artykuł 30
Przetwarzanie z upoważnienia administratora i podmiotu przetwarzającego

Podmiot przetwarzający oraz każda osoba działająca z upoważnienia administratora lub podmiotu przetwarzającego i mająca dostęp do danych osobowych przetwarzają je wyłącznie na polecenie administratora, chyba że wymaga tego prawo Unii lub prawo państwa członkowskiego.

Artykuł 31
Rejestrowanie czynności przetwarzania

1. Każdy administrator prowadzi rejestr czynności przetwarzania danych osobowych, za które odpowiada. W rejestrze tym zamieszcza się wszystkie następujące informacje:

   a) imię i nazwisko lub nazwę oraz dane kontaktowe administratora, inspektora ochrony danych, a także gdy ma to zastosowanie – podmiotu przetwarzającego i współadministratora;

   b) cele przetwarzania;

   c) opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;

   d) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach członkowskich, 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 oraz 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. 33.

2. Każdy podmiot przetwarzający prowadzi rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora, zawierający następujące informacje:

   a) imię i nazwisko lub nazwa oraz dane kontaktowe podmiotu przetwarzającego lub podmiotów przetwarzających oraz każdego administratora, w imieniu którego działa podmiot przetwarzający, a także inspektora ochrony danych;

   b) kategorie przetwarzań dokonywanych w imieniu każdego z administratorów;

   c) gdy ma to zastosowanie – przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej oraz dokumentacja odpowiednich zabezpieczeń;

   d) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 33.

3. Rejestry, o których mowa w ust. 1 i 2, mają formę pisemną, w tym formę elektroniczną.

4. Instytucje i organy unijne udostępniają rejestr na żądanie Europejskiego Inspektora Ochrony Danych.

5. Instytucje i organy unijne mogą podjąć decyzję o prowadzeniu swoich rejestrów czynności przetwarzania w rejestrze centralnym. W takim przypadku mogą również podjąć decyzję o publicznym udostępnieniu rejestru.

Artykuł 32
Współpraca z Europejskim Inspektorem Ochrony Danych

Instytucje i organy unijne współpracują z Europejskim Inspektorem Ochrony Danych na jego żądanie w zakresie wykonywania jego zadań.

SEKCJA 2

BEZPIECZEŃSTWO DANYCH OSOBOWYCH I POUFNOŚĆ ŁĄCZNOŚCI ELEKTRONICZNEJ

Artykuł 33
Bezpieczeństwo przetwarzania

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, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym między innymi w stosownym przypadku:

   a) pseudonimizację i szyfrowanie danych osobowych;

   b) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;

   c) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;

   d) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

2. Oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub winny sposób przetwarzanych.

3. Administrator oraz podmiot przetwarzający podejmują działania w celu zapewnienia, by każda osoba fizyczna działająca z upoważnienia administratora lub podmiotu przetwarzającego, która ma dostęp do danych osobowych, przetwarzała je wyłącznie na polecenie administratora, chyba że wymaga tego od niej prawo Unii.

Artykuł 34
Poufność łączności elektronicznej

Instytucje i organy unijne zapewniają poufność łączności elektronicznej, w szczególności dzięki zabezpieczeniu swoich sieci łączności elektronicznej.

Artykuł 35
Ochrona informacji związanych z końcowymi urządzeniami komunikacyjnymi użytkowników końcowych

Instytucje i organy unijne chronią informacje mające związek z końcowymi urządzeniami telekomunikacyjnymi użytkowników końcowych łączącymi się z dostępnymi publicznie stronami internetowymi i aplikacjami mobilnymi tych instytucji i organów, zgodnie z rozporządzeniem (UE) XXXX/XX [nowe rozporządzenie o prywatności elektronicznej], a w szczególności z jego art. 8.

Artykuł 36
Spisy użytkowników

1. Dane osobowe zawarte są w spisach użytkowników i dostęp do takich spisów jest ograniczony do tego, co jest bezwzględnie konieczne do konkretnych celów spisu.

2. Instytucje i organy unijne podejmą wszelkie dostępne środki, aby zapobiec użyciu danych osobowych zawartych w tych spisach, niezależnie od tego, czy są one ogólnodostępne czy nie, do celów marketingu bezpośredniego.

Artykuł 37
Zgłaszanie naruszenia ochrony danych osobowych Europejskiemu Inspektorowi Ochrony Danych

1. 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 Europejskiemu Inspektorowi Ochrony Danych, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego Europejskiemu Inspektorowi Ochrony Danych po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

2. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi.

3. Zgłoszenie, o którym mowa w ust. 1, musi co najmniej:

   a) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;

   b) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych;

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.

4. Jeżeli – i w zakresie, w jakim – informacji nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki.

5. Administrator powiadamia inspektora ochrony danych o naruszeniu ochrony danych osobowych.

6. Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta umożliwia Europejskiemu Inspektorowi Ochrony Danych weryfikowanie przestrzegania niniejszego artykułu.

Artykuł 38
Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych

1. 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.

2. 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. 37 ust. 3 lit. b), c) i d).

3. Zawiadomienie, o którym mowa w ust. 1, nie jest wymagane w następujących przypadkach:

a) administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;

b) administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w ust. 1;

c) wymagałoby ono 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.

4. Jeżeli administrator nie zawiadomił jeszcze osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, Europejski Inspektor Ochrony Danych – biorąc pod uwagę prawdopodobieństwo, że to naruszenie ochrony danych osobowych spowoduje wysokie ryzyko – może od niego tego zażądać lub może stwierdzić, że spełniony został jeden z warunków, o których mowa w ust. 3.

SEKCJA 3

OCENA SKUTKÓW W ZAKRESIE OCHRONY DANYCH I UPRZEDNIE KONSULTACJE

Artykuł 39
Ocena skutków w zakresie ochrony danych

1. Jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę.

2. Dokonując oceny skutków w zakresie ochrony danych, administrator zasięga porady inspektora ochrony danych.

3. Ocena skutków w zakresie ochrony danych, o której mowa w ust. 1, jest wymagana w szczególności w przypadku:

   a) systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną;

   b) przetwarzania na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 10, lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 11; lub

   c) systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.

4. Europejski Inspektor Ochrony Danych ustanawia i podaje do publicznej wiadomości wykaz rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny skutków w zakresie ochrony danych na podstawie ust. 1.

5. Europejski Inspektor Ochrony Danych może także określić i podać do wiadomości publicznej wykaz rodzajów operacji przetwarzania niepodlegających wymogowi dokonania oceny skutków w zakresie ochrony danych.

6. Ocena zawiera co najmniej:

   a) systematyczny opis planowanych operacji przetwarzania i celów przetwarzania;

   b) ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów;

c) ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą, o którym mowa w ust. 1; oraz

d) środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie niniejszego rozporządzenia, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy.

7. Oceniając – w szczególności do celów oceny skutków w zakresie ochrony danych – skutki operacji przetwarzania wykonywanych przez właściwe podmioty przetwarzające inne niż instytucje i organy unijne, uwzględnia się przestrzeganie przez takie podmioty przetwarzające zatwierdzonych kodeksów postępowania, o których mowa w art. 40 rozporządzenia (UE) 2016/679.

8. W stosownych przypadkach administrator zasięga opinii osób, których dane dotyczą, lub ich przedstawicieli w sprawie zamierzonego przetwarzania, bez uszczerbku dla ochrony interesów publicznych lub bezpieczeństwa operacji przetwarzania.

9. Jeżeli prawo Unii nie stanowi inaczej, ust. 1–6 nie mają zastosowania, jeżeli przetwarzanie na podstawie art. 5 ust. 1 lit. a) lub b) ma podstawę prawną w akcie prawnym przyjętym na podstawie Traktatów, który reguluje daną operację przetwarzania lub zestaw operacji, a ocenę skutków w zakresie ochrony danych sporządzono już w ramach oceny skutków regulacji dokonanej przed przyjęciem tego aktu prawnego.

10. W razie potrzeby, przynajmniej gdy zmienia się ryzyko wynikające z operacji przetwarzania, administrator dokonuje przeglądu, by stwierdzić, czy przetwarzanie odbywa się zgodnie z oceną skutków w zakresie ochrony danych.

Artykuł 40
Uprzednie konsultacje

1. Administrator konsultuje się z Europejskim Inspektorem Ochrony Danych przed rozpoczęciem czynności przetwarzania, jeżeli ocena skutków w zakresie ochrony danych przewidziana w art. 39 wykaże, że przy braku zabezpieczeń, środków bezpieczeństwa oraz mechanizmów minimalizujących ryzyko przetwarzanie powodowałoby wysokie ryzyko naruszenia praw lub wolności osób fizycznych, a administrator wyraża opinię, że ryzyka tego nie da się zminimalizować środkami rozsądnymi z punktu widzenia dostępnych technologii i kosztów wdrożenia. Administrator zasięga porady inspektora ochrony danych w sprawie konieczności dokonania uprzednich konsultacji.

2. Jeżeli Europejski Inspektor Ochrony Danych jest zdania, że zamierzone przetwarzanie, o którym mowa w ust. 1, stanowiłoby naruszenie niniejszego rozporządzenia – w szczególności gdy administrator niedostatecznie zidentyfikował lub zminimalizował ryzyko – Europejski Inspektor Ochrony Danych w terminie do ośmiu tygodni od wpłynięcia wniosku o konsultacje udziela administratorowi, a gdy ma to zastosowanie także podmiotowi przetwarzającemu pisemnego zalecenia i może skorzystać z dowolnego ze swoich uprawnień, o których mowa w art. 59. Okres ten można przedłużyć o sześć tygodni ze względu na złożony charakter

zamierzonego przetwarzania. Europejski Inspektor Ochrony Danych informuje administratora, a gdy ma to zastosowanie także podmiot przetwarzający, o takim przedłużeniu w terminie miesiąca od wpłynięcia wniosku o konsultacje, z podaniem przyczyn tego opóźnienia. Bieg tych terminów można zawiesić, do czasu aż Europejski Inspektor Ochrony Danych uzyska wszelkie informacje, których zażądał do celów konsultacji.

3. Konsultując się z Europejskim Inspektorem Ochrony Danych zgodnie z ust. 1, administrator przedstawia mu:

a) gdy ma to zastosowanie – odpowiednie obowiązki administratora, współadministratorów oraz podmiotów przetwarzających uczestniczących w przetwarzaniu;

b) cele i sposoby zamierzonego przetwarzania;

c) środki i zabezpieczenia mające chronić prawa i wolności osób, których dane dotyczą, zgodnie z niniejszym rozporządzeniem;

d) dane kontaktowe inspektora ochrony danych;

e) ocenę skutków w zakresie ochrony danych, o której mowa w art. 39; oraz

f) wszelkie inne informacje, których żąda Europejski Inspektor Ochrony Danych.

4. W drodze aktu wykonawczego Komisja może ustalić wykaz przypadków, w których administratorzy muszą konsultować się z Europejskim Inspektorem Ochrony Danych i uzyskać jego uprzednią zgodę na przetwarzanie danych do celów wykonania zadania realizowanego przez administratora w interesie publicznym, w tym przetwarzania w związku z ochroną socjalną i zdrowiem publicznym.

SEKCJA 4

INFORMACJE I KONSULTACJE W SPRAWIE AKTÓW USTAWODAWCZYCH

Artykuł 41
Informacje

Instytucje i organy unijne informują Europejskiego Inspektora Ochrony Danych, gdy wdrażają środki administracyjne i wewnętrzne przepisy odnoszące się do przetwarzania danych osobowych, w których bierze udział instytucja unijna lub organ unijny, samodzielnie lub wspólnie z innymi.

Artykuł 42
Konsultacje w sprawie aktów ustawodawczych

1. Komisja konsultuje się z Europejskim Inspektorem Ochrony Danych po przyjęciu wniosków w sprawie aktów ustawodawczych oraz zaleceń lub wniosków przedłożonych Radzie zgodnie z art. 218 TFUE oraz podczas opracowywania aktów delegowanych lub aktów wykonawczych, które mają wpływ na ochronę praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych.

2. Jeżeli akt, o którym mowa w ust. 1, ma szczególne znaczenie dla ochrony praw i wolności osób fizycznych w zakresie przetwarzania danych osobowych, Komisja może również skonsultować się z Europejską Radą Ochrony Danych. W takich przypadkach Europejski Inspektor Ochrony Danych i Europejska Rada Ochrony Danych koordynują swoje prace w celu wydania wspólnej opinii.

3. Zalecenie, o którym mowa w ust. 1 i 2, przekazuje się na piśmie w terminie do ośmiu tygodni od wpłynięcia wniosku o konsultacje, o których mowa w ust. 1 i 2. W pilnych przypadkach lub z innych uzasadnionych przyczyn Komisja może skrócić termin.

4. Przepisy niniejszego artykułu nie mają zastosowania wtedy, gdy zgodnie z rozporządzeniem (UE) 2016/679 Komisja ma obowiązek skonsultowania się z Europejską Radą Ochrony Danych.

SEKCJA 5

OBOWIĄZEK REAGOWANIA NA SKARGI

Artykuł 43
Obowiązek reagowania na skargi

Jeżeli Europejski Inspektor Ochrony Danych wykonuje uprawnienia przewidziane w art. 59 ust. 2 lit. a), b) i c), administrator lub podmiot przetwarzający informuje Europejskiego Inspektora Ochrony Danych o swoim poglądzie w odpowiednim czasie określonym przez Europejskiego Inspektora Ochrony Danych, uwzględniając okoliczności każdej sprawy. Odpowiedź zawiera opis podjętych środków, jeżeli takie zostały podjęte, w odpowiedzi na uwagi Europejskiego Inspektora Ochrony Danych.

SEKCJA 6

INSPEKTOR OCHRONY DANYCH

Artykuł 44
Wyznaczenie inspektora ochrony danych

1. Każda instytucja unijna lub organ unijny wyznacza inspektora ochrony danych.

2. Instytucje i organy unijne mogą wyznaczyć jednego inspektora ochrony danych dla kilku takich instytucji lub organów, uwzględniając ich strukturę administracyjną i wielkość.

3. 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. 46.

4. Inspektor ochrony danych może być członkiem personelu instytucji unijnej lub organu unijnego lub wykonywać zadania na podstawie zamówienia publicznego na usługi.

5. Instytucje i organy unijne publikują dane kontaktowe inspektora ochrony danych i zawiadamiają o nich Europejskiego Inspektora Ochrony Danych.

Artykuł 45
Status inspektora ochrony danych

1. Instytucje i organy unijne zapewniają, by inspektor ochrony danych był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych.

2. Instytucje i organy unijne wspierają inspektora ochrony danych w wypełnianiu przez niego zadań, o których mowa w art. 46, 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.

3. Instytucje i organy unijne zapewniają, by inspektor ochrony danych nie otrzymywał instrukcji dotyczących wykonywania jego 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.

4. Osoby, których dane dotyczą, mogą kontaktować się z inspektorem ochrony danych we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy niniejszego rozporządzenia.

5. Inspektor ochrony danych oraz jego pracownicy są zobowiązani do zachowania tajemnicy lub poufności co do wykonywania swoich zadań, zgodnie z prawem Unii.

6. Inspektor ochrony danych może wykonywać inne zadania i obowiązki. Administrator lub podmiot przetwarzający zapewniają, by takie zadania i obowiązki nie powodowały konfliktu interesów.

7. Inspektor ochrony danych może być konsultowany przez administratora i podmiot przetwarzający, odpowiedni komitet personelu i przez dowolne osoby, bez korzystania z kanałów oficjalnych, w każdej sprawie dotyczącej interpretacji lub stosowania niniejszego rozporządzenia. Nikt nie ponosi szkody z powodu tego, że zwrócił uwagę odpowiedniego inspektora ochrony danych na fakt domniemanego naruszenia przepisów niniejszego rozporządzenia.

8. Inspektor ochrony danych zostaje powołany na okres od trzech do pięciu lat i może zostać powołany ponownie. Inspektor ochrony danych może być zwolniony ze stanowiska przez instytucję lub organ unijny, który go powołał, jedynie za zgodą Europejskiego Inspektora Ochrony Danych, jeżeli przestał spełniać warunki konieczne dla wykonywania jego obowiązków.

9. Po powołaniu na stanowisko inspektora ochrony danych, instytucja lub organ unijny, które go powołały, dokonują jego rejestracji u Europejskiego Inspektora Ochrony Danych.

Artykuł 46
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 o ochronie danych i doradzanie im w tej sprawie;

   b) zapewnianie stosowania przepisów niniejszego rozporządzenia wewnątrz instytucji lub organu w sposób niezależny oraz monitorowanie przestrzegania niniejszego rozporządzenia, innych obowiązujących aktów unijnych zawierających przepisy o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podziału obowiązków, działań zwiększających świadomość, szkoleń personelu uczestniczącego w operacjach przetwarzania oraz powiązanych z tym audytów;

   c) zapewnianie, by osoby, których dane dotyczą, były informowane o swoich prawach i obowiązkach wynikających z niniejszego rozporządzenia;

   d) udzielanie na żądanie porad co do konieczności zgłoszenia lub zawiadomienia o naruszeniu ochrony danych osobowych na podstawie przepisów art. 37 i 38;

   e) udzielanie na żądanie porad co do oceny skutków w zakresie ochrony danych oraz monitorowanie jej wykonania na podstawie art. 39, a także konsultowanie się z Europejskim Inspektorem Ochrony Danych w razie wątpliwości co do konieczności wykonania oceny skutków w zakresie ochrony danych;

   f) udzielanie na żądanie porad co do konieczności dokonania uprzednich konsultacji z Europejskim Inspektorem Ochrony Danych na podstawie art. 40 oraz konsultowanie się z Europejskim Inspektorem Ochrony Danych w razie wątpliwości co do konieczności dokonania uprzednich konsultacji;

   g) odpowiadanie na wnioski Europejskiego Inspektora Ochrony Danych i, w ramach jego kompetencji, współpraca i konsultowanie się z Europejskim Inspektorem Ochrony danych na wniosek tego organu lub z inicjatywy własnej.

2. Inspektor ochrony danych może formułować zalecenia w zakresie praktycznego usprawnienia ochrony danych, skierowane do administratora i podmiotu

przetwarzającego, oraz doradzać im w kwestiach związanych z zastosowaniem przepisów o ochronie danych. Ponadto może z własnej inicjatywy lub na wniosek administratora lub podmiotu przetwarzającego, odpowiedniego komitetu personelu lub dowolnej osoby badać sprawy i zdarzenia odnoszące się bezpośrednio do jego zadań i które zwróciły jego uwagę oraz złożyć sprawozdanie osobie, która zleciła dochodzenie, bądź administratorowi lub podmiotowi przetwarzającemu.

3. Każda instytucja unijna lub organ unijny przyjmuje dalsze przepisy wykonawcze dotyczące inspektora ochrony danych. Przepisy wykonawcze dotyczą w szczególności zadań, obowiązków i uprawnień inspektora ochrony danych.

ROZDZIAŁ V

Przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych

Artykuł 47
Ogólna zasada przekazywania

Przekazanie danych osobowych, które są przetwarzane lub mają być przetwarzane po przekazaniu do państwa trzeciego lub organizacji międzynarodowej, następuje tylko, gdy – z zastrzeżeniem innych przepisów niniejszego rozporządzenia – administrator i podmiot przetwarzający spełnią warunki określone w niniejszym rozdziale, w tym warunki dalszego przekazania danych z państwa trzeciego lub przez organizację międzynarodową do innego państwa trzeciego lub innej organizacji międzynarodowej. Wszystkie przepisy niniejszego rozdziału należy stosować z myślą o zapewnieniu, by nie został naruszony stopień ochrony osób fizycznych zagwarantowany w niniejszym rozporządzeniu.

Artykuł 48
Przekazywanie na podstawie decyzji stwierdzającej odpowiedni stopień ochrony

1. Przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej może nastąpić, gdy Komisja stwierdzi na podstawie art. 45 ust. 3 rozporządzenia (UE) 2016/679, że to państwo trzecie, terytorium lub określony sektor lub określone sektory w tym państwie trzecim lub dana organizacja międzynarodowa posiadają zapewniony odpowiedni stopień ochrony, a dane osobowe są przekazywane jedynie po to, aby umożliwić wykonywanie zadań wchodzących w zakres kompetencji administratora.

2. Instytucje i organy unijne poinformują Komisję i Europejskiego Inspektora Ochrony Danych o przypadkach, kiedy uważają, że państwo trzecie lub organizacja nie zapewniają odpowiedniego stopnia ochrony w rozumieniu ust. 1.

3. Instytucje i organy unijne podejmą niezbędne środki na potrzeby zapewnienia zgodności z decyzjami wydanymi przez Komisję, stwierdzającymi, czy zgodnie z art. 45 ust. 3 i 5 rozporządzenia (UE) 2016/679 państwo trzecie lub organizacja międzynarodowa zapewnia odpowiedni stopień ochrony lub czy już go nie zapewnia.

Artykuł 49
Przekazywanie z zastrzeżeniem odpowiednich zabezpieczeń

1. W razie braku decyzji na podstawie art. 45 ust. 3 rozporządzenia (UE) 2016/679 administrator lub podmiot przetwarzający mogą przekazać dane osobowe do państwa trzeciego lub organizacji międzynarodowej wyłącznie, gdy zapewnią odpowiednie zabezpieczenia, i pod warunkiem, że obowiązują egzekwowalne prawa osób, których dane dotyczą, i skuteczne środki ochrony prawnej.

2. Odpowiednie zabezpieczenia, o których mowa w ust. 1, można zapewnić – bez konieczności uzyskania specjalnego zezwolenia ze strony Europejskiego Inspektora Ochrony Danych – za pomocą:

   a) prawnie wiążącego i egzekwowalnego instrumentu między organami lub podmiotami publicznymi;

   b) standardowych klauzul ochrony danych przyjętych przez Komisję zgodnie z procedurą sprawdzającą, o której mowa w art. 70 ust. 2;

   c) standardowych klauzul ochrony danych przyjętych przez Europejskiego Inspektora Ochrony Danych i zatwierdzonych przez Komisję zgodnie z procedurą sprawdzającą, o której mowa w art. 70 ust. 2;

   d) wiążących reguł korporacyjnych, kodeksów postępowania i mechanizmów certyfikacji na podstawie art. 46 ust. 2 lit. b), e) i f) rozporządzenia (UE) 2016/679, jeżeli podmiot przetwarzający nie jest instytucją unijną ani organem unijnym.

3. Z zastrzeżeniem zezwolenia Europejskiego Inspektora Ochrony Danych odpowiednie zabezpieczenia, o których mowa w ust. 1, można także zapewnić w szczególności za pomocą:

   a) klauzul umownych między administratorem lub podmiotem przetwarzającym a administratorem, podmiotem przetwarzającym lub odbiorcą danych osobowych w państwie trzecim lub organizacji międzynarodowej; lub

   b) postanowień uzgodnień administracyjnych między organami lub podmiotami publicznymi, w których przewidziane będą egzekwowalne i skuteczne prawa osób, których dane dotyczą.

4. Instytucje i organy unijne poinformują Komisję i Europejskiego Inspektora Ochrony Danych o kategoriach przypadków, w których zastosowano przepisy niniejszego artykułu.

5. Zezwolenia wydane przez Europejskiego Inspektora Ochrony Danych na podstawie art. 9 ust. 7 rozporządzenia (WE) nr 45/2001 zachowują ważność do czasu ich zmiany, zastąpienia lub uchylenia w stosownych przypadkach przez Europejskiego Inspektora Ochrony Danych.

Artykuł 50
Przekazywanie lub ujawnianie niedozwolone na mocy prawa Unii

Wyrok sądu lub trybunału oraz decyzja organu administracji państwa trzeciego wymagające od administratora lub podmiotu przetwarzającego przekazania lub ujawnienia danych osobowych 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, bez uszczerbku dla innych podstaw przekazania na mocy niniejszego rozdziału.

Artykuł 51
Wyjątki w szczególnych sytuacjach

1. W razie braku decyzji określonej w art. 45 ust. 3 rozporządzenia (UE) 2016/679 lub braku odpowiednich zabezpieczeń określonych w art. 49 jednorazowe lub wielokrotne przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej mogą nastąpić wyłącznie pod warunkiem, że:

   a) osoba, której dane dotyczą, poinformowana o ewentualnym ryzyku, z którym – ze względu na brak decyzji stwierdzającej odpowiedni stopień ochrony oraz na brak odpowiednich zabezpieczeń – może się dla niej wiązać proponowane przekazanie, wyraźnie wyraziła na nie zgodę;

   b) przekazanie jest niezbędne do wykonania umowy między osobą, której dane dotyczą, a administratorem lub do wprowadzenia w życie środków przedumownych podejmowanych na żądanie osoby, której dane dotyczą;

   c) przekazanie jest niezbędne do zawarcia lub wykonania umowy zawartej w interesie osoby, których dane dotyczą, między administratorem a inną osobą fizyczną lub prawną;

   d) przekazanie jest niezbędne ze względu na ważne względy interesu publicznego;

   e) przekazanie jest niezbędne do ustalenia, dochodzenia lub ochrony roszczeń; lub

   f) przekazanie jest niezbędne do ochrony żywotnych interesów osoby, których dane dotyczą, lub innych osób, jeżeli osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody; lub

   g) przekazanie następuje z rejestru, który zgodnie z prawem Unii ma służyć za źródło informacji dla ogółu obywateli i który jest dostępny dla ogółu obywateli lub dla każdej osoby mogącej wykazać prawnie uzasadniony interes – ale wyłącznie w zakresie, w jakim w danym przypadku spełnione zostały warunki takiego dostępu określone w prawie Unii.

2. Przekazanie na mocy ust. 1 lit. g) nie obejmuje całości danych osobowych ani całych kategorii danych osobowych zawartych w rejestrze, chyba że zezwala na to prawo Unii. Jeżeli rejestr jest dostępny dla osób mających prawnie uzasadniony interes,

przekazanie następuje wyłącznie na żądanie tych osób lub gdy mają one być odbiorcami.

3. Interes publiczny, o którym mowa w ust. 1 lit. d), musi być uznany w prawie Unii.

4. W razie braku decyzji stwierdzającej odpowiedni stopień ochrony prawo Unii może z uwagi na ważne względy interesu publicznego wyraźnie nakładać ograniczenia na przekazywanie konkretnych kategorii danych osobowych do państwa trzeciego lub organizacji międzynarodowej.

5. Instytucje i organy unijne poinformują Komisję i Europejskiego Inspektora Ochrony Danych o kategoriach przypadków, w których zastosowano przepisy niniejszego artykułu.

Artykuł 52
Międzynarodowa współpraca na rzecz ochrony danych osobowych

We współpracy z Komisją i Europejską Radą Ochrony Danych Europejski Inspektor Ochrony Danych podejmuje wobec państw trzecich i organizacji międzynarodowych odpowiednie działania na rzecz:

a) wypracowania mechanizmów współpracy międzynarodowej ułatwiających skuteczne egzekwowanie przepisów o ochronie danych osobowych;

b) zapewnienia wzajemnej pomocy międzynarodowej w egzekwowaniu przepisów o ochronie danych osobowych, w tym poprzez zgłoszenia, przekazywanie skarg, pomoc w postępowaniu wyjaśniającym oraz wymianę informacji – z zastrzeżeniem odpowiednich zabezpieczeń ochrony danych osobowych i innych podstawowych praw i wolności;

c) włączenia stosownych podmiotów, których sprawa dotyczy, w dyskusję i działania mające na celu upowszechnianie międzynarodowej współpracy w dziedzinie egzekwowania przepisów o ochronie danych osobowych;

d) upowszechniania wymiany i dokumentowania przepisów i praktyk w dziedzinie ochrony danych osobowych, w tym konfliktów jurysdykcyjnych z państwami trzecimi.

ROZDZIAŁ VI

EUROPEJSKI INSPEKTOR OCHRONY DANYCH

Artykuł 53
Europejski Inspektor Ochrony Danych

1. Niniejszym ustanawia się urząd Europejskiego Inspektora Ochrony Danych.

2. Europejski Inspektor Ochrony Danych jest odpowiedzialny za zapewnienie, by podstawowe prawa i wolności osób fizycznych, w szczególności prawo do ochrony danych, były przestrzegane przez instytucje i organy unijne w odniesieniu do przetwarzania danych osobowych.

3. Europejski Inspektor Ochrony Danych jest odpowiedzialny za monitorowanie i zapewnienie zastosowania przepisów niniejszego rozporządzenia i każdego innego aktu Unii, odnoszącego się do podstawowych praw i wolności osób fizycznych, w odniesieniu do przetwarzania danych osobowych przez instytucje i organy unijne oraz za doradzanie instytucjom i organom unijnym i osobom, których dane dotyczą, we wszystkich kwestiach związanych z przetwarzaniem danych osobowych. W tym celu Europejski Inspektor Ochrony Danych wypełnia obowiązki przewidziane w art. 58 i korzysta z uprawnień nadanych w art. 59.

Artykuł 54
Powoływanie Europejskiego Inspektora Ochrony Danych

1. Parlament Europejski i Rada powołują Europejskiego Inspektora Ochrony Danych w drodze wspólnego porozumienia na okres pięciu lat, na podstawie listy ustalonej przez Komisję po ogłoszeniu publicznego naboru dla kandydatów. Nabór kandydatów umożliwia zainteresowanym osobom w całej Unii złożenie ich wniosków. Lista kandydatów ustalona przez Komisję jest publikowana. Na podstawie listy ustalonej przez Komisję właściwa komisja Parlamentu Europejskiego może podjąć decyzję o przeprowadzeniu przesłuchania w celu wyrażenia swoich preferencji.

2. Na liście ustalonej przez Komisję, na podstawie której wybiera się Europejskiego Inspektora Ochrony Danych, znajdują się osoby, których niezależność jest niekwestionowana i o których wiadomo, że mają doświadczenie i umiejętności wymagane do pełnienia obowiązków Europejskiego Inspektora Ochrony Danych, ponieważ na przykład należą lub należały do organów nadzorczych ustanowionych w art. 41 rozporządzenia (UE) 2016/679.

3. Kadencja Europejskiego Inspektora Ochrony Danych może być odnowiona jeden raz.

4. Europejski Inspektor Ochrony Danych zaprzestaje pełnienia obowiązków w następujących przypadkach:

   a) jeżeli Europejski Inspektor Ochrony Danych zostaje zastąpiony;

   b) jeżeli Europejski Inspektor Ochrony Danych zrezygnuje z urzędu;

   c) jeżeli Europejski Inspektor Ochrony Danych zostanie zwolniony lub przymusowo pozbawiony funkcji.

5. Europejski Inspektor Ochrony Danych może być zwolniony lub pozbawiony praw do emerytury lub innych świadczeń na jego rzecz przez Trybunał Sprawiedliwości Unii Europejskiej na wniosek Parlamentu Europejskiego, Rady lub Komisji, jeżeli przestanie spełniać warunki wymagane dla wykonania jego obowiązków lub jeśli jest winny poważnego uchybienia.

6. W przypadku zwykłej zmiany lub dobrowolnej rezygnacji Europejski Inspektor Ochrony Danych pełni swoją funkcję do czasu, gdy zostanie zastąpiony.

7. Przepisy art. 11–14 i 17 Protokołu w sprawie przywilejów i immunitetów Unii Europejskiej stosują się także do Europejskiego Inspektora Ochrony Danych.

Artykuł 55
Regulacje i ogólne warunki dotyczące wypełniania obowiązków przez Europejskiego Inspektora Ochrony Danych i jego personel oraz dotyczące zasobów finansowych

1. Europejskiego Inspektora Ochrony Danych traktuje się na równi z sędzią Trybunału Sprawiedliwości Unii Europejskiej, w odniesieniu do określania wynagrodzenia, dodatków, emerytury za wysługę lat i innych świadczeń w miejsce wynagrodzenia.

2. Władze budżetowe zapewniają, aby Europejski Inspektor Ochrony Danych otrzymał zasoby ludzkie i finansowe konieczne do wykonania swoich zadań.

3. Budżet Europejskiego Inspektora Ochrony Danych jest uwzględniany w odrębnej pozycji budżetu w sekcji IX ogólnego budżetu Unii Europejskiej.

4. Europejski Inspektor Ochrony Danych jest wspomagany przez sekretariat. Urzędnicy i inni pracownicy sekretariatu są powoływani przez Europejskiego Inspektora Ochrony Danych, który jest ich przełożonym. Działają oni pod jego wyłącznym kierownictwem. Ich liczba jest wyznaczana każdego roku w czasie procedury budżetowej.

5. Urzędnicy i inny pracownicy sekretariatu Europejskiego Inspektora Ochrony Danych podlegają zasadom i przepisom mającym zastosowanie do urzędników i innego personelu Unii Europejskiej.

6. Siedziba Europejskiego Inspektora Ochrony Danych mieści się w Brukseli.

Artykuł 56
Niezależność

1. Europejski Inspektor Ochrony Danych podczas wypełniania swoich zadań i wykonywania swoich uprawnień zgodnie z niniejszym rozporządzeniem działa w sposób w pełni niezależny.

2. Europejski Inspektor Ochrony Danych podczas wypełniania swoich zadań i wykonywania swoich uprawnień zgodnie z niniejszym rozporządzeniem pozostaje wolny od bezpośrednich i pośrednich wpływów zewnętrznych, nie zwraca się do nikogo o instrukcje ani ich od nikogo nie przyjmuje.

3. Europejski Inspektor Ochrony Danych powstrzymuje się od wszelkich czynności sprzecznych ze swoimi obowiązkami i podczas swojej kadencji nie podejmuje żadnego innego zajęcia zarobkowego ani niezarobkowego.

4. Europejski Inspektor Ochrony Danych po zakończeniu swojej kadencji postępuje godnie i rozważnie w odniesieniu do przyjmowania stanowisk i korzyści.

Artykuł 57
Tajemnica zawodowa

Europejski Inspektor Ochrony Danych oraz jego pracownicy – w trakcie kadencji i po jej zakończeniu – podlegają obowiązkowi zachowania tajemnicy służbowej w odniesieniu do wszelkich poufnych informacji, które uzyskali w trakcie wykonywania oficjalnych obowiązków.

Artykuł 58
Zadania

1. Bez uszczerbku dla innych zadań określonych na mocy niniejszego rozporządzenia Europejski Inspektor Ochrony Danych:

   a) monitoruje i egzekwuje zastosowanie przepisów niniejszego rozporządzenia i wszystkich innych aktów Unii odnoszących się do ochrony osób fizycznych w odniesieniu do przetwarzania danych osobowych przez instytucję unijną lub organ unijny, z wyjątkiem przetwarzania danych osobowych przez Trybunał Sprawiedliwości Unii Europejskiej działający jako władza sądownicza;

   b) upowszechnia w społeczeństwie wiedzę o ryzyku, przepisach, zabezpieczeniach i prawach związanych z przetwarzaniem oraz rozumienie tych zjawisk. Szczególną uwagę poświęca działaniom skierowanym do dzieci;

   c) upowszechnia wśród administratorów i podmiotów przetwarzających wiedzę o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia;

   d) udziela osobie, której dane dotyczą, na jej żądanie informacji o wykonywaniu praw przysługujących im na mocy niniejszego rozporządzenia, a w stosownym przypadku współpracuje w tym celu z organami nadzorczymi państw członkowskich;

   e) rozpatruje skargi wniesione przez osobę, której dane dotyczą, lub przez podmiot, organizację lub zrzeszenie zgodnie z art. 67, w odpowiednim zakresie prowadzi postępowania dotyczące tych skarg i w rozsądnym terminie informuje skarżącego o postępach i wynikach tych postępowań, w szczególności jeżeli niezbędne jest dalsze postępowanie lub koordynacja działań z innym organem nadzorczym;

   f) prowadzi postępowania w sprawie stosowania niniejszego rozporządzenia, w tym na podstawie informacji otrzymanych od innego organu nadzorczego lub innego organu publicznego;

   g) doradza wszystkim instytucjom i organom unijnym w sprawie prawnych i administracyjnych środków ochrony praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych;

   h) monitoruje zmiany w stosownych dziedzinach, o ile zmiany te mają wpływ na ochronę danych osobowych, w szczególności monitoruje rozwój technologii informacyjno-komunikacyjnych;

i) przyjmuje standardowe klauzule umowne, o których mowa w art. 29 ust. 8 i w art. 49 ust. 2 lit. c);

j) ustanawia i prowadzi wykaz związany z wymogiem dokonania oceny skutków w zakresie ochrony danych na mocy art. 39 ust. 4;

k) uczestniczy w działaniach Europejskiej Rady Ochrony Danych ustanowionej na podstawie art. 68 rozporządzenia (UE) 2016/679;

l) zapewnia obsługę sekretariatu na potrzeby Europejskiej Rady Ochrony Danych zgodnie z art. 75 rozporządzenia (UE) 2016/679;

m) wydaje zalecenia, o których mowa w art. 40 ust. 2, dotyczące przetwarzania;

n) zatwierdza klauzule umowne i przepisy, o których mowa w art. 49 ust. 3;

o) prowadzi wewnętrzny rejestr naruszeń niniejszego rozporządzenia i działań podjętych zgodnie z art. 59 ust. 2;

p) wypełnia inne zadania związane z ochroną danych osobowych; oraz

q) uchwala swój regulamin wewnętrzny.

2. Europejski Inspektor Ochrony Danych ułatwia wnoszenie skarg, o których mowa w ust. 1 lit. e), za pomocą gotowego formularza skargi, który można również wypełnić elektronicznie, co nie wyklucza innych sposobów komunikacji.

3. Europejski Inspektor Ochrony Danych pełni swoje zadania bez pobierania opłat od osoby, której dane dotyczą.

4. Jeżeli żądania są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, Europejski Inspektor Ochrony Danych może odmówić podjęcia działań w związku z żądaniem. Obowiązek wykazania, że żądanie ma ewidentnie nieuzasadniony lub nadmierny charakter, spoczywa na Europejskim Inspektorze Ochrony Danych.

Artykuł 59
Uprawnienia

1. Europejskiemu Inspektorowi Ochrony Danych przysługują następujące uprawnienia w zakresie prowadzonych postępowań:

a) nakazanie administratorowi i podmiotowi przetwarzającemu dostarczenia wszelkich informacji niezbędnych do realizacji jego zadań;

b) prowadzenie postępowań w formie audytów ochrony danych;

c) zawiadamianie administratora lub podmiotu przetwarzającego o podejrzeniu naruszenia niniejszego rozporządzenia;

d) uzyskiwanie od administratora i podmiotu przetwarzającego dostępu do wszelkich danych osobowych i wszelkich informacji niezbędnych do realizacji jego zadań;

e) uzyskiwanie dostępu do wszystkich pomieszczeń administratora i podmiotu przetwarzającego, w tym do sprzętu i środków służących do przetwarzania danych, zgodnie z procedurami określonymi w prawie unijnym lub w prawie państwa członkowskiego.

2. Europejskiemu Inspektorowi Ochrony Danych przysługują wszystkie następujące uprawnienia naprawcze:

a) wydawanie ostrzeżeń skierowanych do administratora lub podmiotu przetwarzającego dotyczących możliwości naruszenia przepisów niniejszego rozporządzenia poprzez planowane operacje przetwarzania;

b) udzielanie upomnień administratorowi lub podmiotowi przetwarzającemu w przypadku naruszenia przepisów niniejszego rozporządzenia przez operacje przetwarzania;

c) przekazanie sprawy do administratora lub podmiotu przetwarzającego i, jeżeli to konieczne, do Parlamentu Europejskiego, Rady i Komisji;

d) nakazanie administratorowi lub podmiotowi przetwarzającemu spełnienia żądania osoby, której dane dotyczą, wynikającego z praw przysługujących jej na mocy niniejszego rozporządzenia;

e) nakazanie administratorowi lub podmiotowi przetwarzającemu dostosowania operacji przetwarzania do przepisów niniejszego rozporządzenia, a w stosownych przypadkach wskazanie sposobu i terminu;

f) nakazanie administratorowi zawiadomienia osoby, której dane dotyczą, o naruszeniu ochrony danych;

g) wprowadzanie czasowego lub całkowitego ograniczenia przetwarzania, w tym zakazu przetwarzania;

h) nakazanie na mocy art. 18, 19 i 20 sprostowania lub usunięcia danych osobowych lub ograniczenia ich przetwarzania oraz nakazanie na mocy art. 19 ust. 2 i art. 21 powiadomienia o tych czynnościach odbiorców, których dane osobowe ujawniono;

i) zastosowanie administracyjnej kary pieniężnej na mocy art. 66 w razie nieprzestrzegania przez instytucję unijną lub organ unijny co najmniej jednego środka, o którym mowa w niniejszym ustępie, zależnie od okoliczności konkretnej sprawy;

j) nakazanie zawieszenia przepływu danych do odbiorcy w państwie członkowskim, w państwie trzecim lub do organizacji międzynarodowej.

3. Europejskiemu Inspektorowi Ochrony Danych przysługują następujące uprawnienia zatwierdzające i doradcze:

a) doradzanie osobom, których dane dotyczą, w kwestii korzystania z ich praw;

b) udzielanie porad administratorowi zgodnie z procedurą uprzednich konsultacji, o której mowa w art. 40;

c) wydawanie, z własnej inicjatywy lub na wniosek, opinii skierowanych do instytucji i organów unijnych oraz ogółu społeczeństwa we wszelkich sprawach związanych z ochroną danych osobowych;

d) przyjmowanie standardowych klauzul ochrony danych, o których mowa w art. 29 ust. 8 i art. 49 ust. 2 lit. c);

e) zatwierdzanie klauzul umownych, o których mowa w art. 49 ust. 3 lit. a);

f) zatwierdzanie uzgodnień administracyjnych, o których mowa w art. 49 ust. 3 lit. b).

4. Wykonywanie uprawnień powierzonych Europejskiemu Inspektorowi Ochrony Danych na mocy niniejszego artykułu podlega odpowiednim zabezpieczeniom – w tym prawu do skutecznego środka ochrony prawnej przed sądem i rzetelnego procesu, określonym w prawie Unii.

5. Europejski Inspektor Ochrony Danych ma prawo przekazać sprawę do Trybunału Sprawiedliwości Unii Europejskiej zgodnie z warunkami przewidzianymi w Traktacie oraz interweniować w sprawach wniesionych do Trybunału Sprawiedliwości Unii Europejskiej.

Artykuł 60
Sprawozdanie z działalności

1. Europejski Inspektor Ochrony Danych składa roczne sprawozdanie ze swojej działalności Parlamentowi Europejskiemu, Radzie i Komisji i jednocześnie je publikuje.

2. Europejski Inspektor Ochrony Danych przekazuje sprawozdanie z działalności innym instytucjom i organom unijnym, które mogą dołączyć komentarze, mając na względzie możliwe badanie sprawozdania w Parlamencie Europejskim.

ROZDZIAŁ VII

WSPÓŁPRACA I SPÓJNOŚĆ

Artykuł 61
Współpraca z krajowymi organami nadzorczymi

Europejski Inspektor Ochrony Danych współpracuje z organami nadzorczymi utworzonymi na mocy art. 41 rozporządzenia (UE) 2016/679 oraz art. 51 dyrektywy (UE) 2016/680 (zwanymi dalej „krajowymi organami nadzorczymi”), a także ze wspólnym organem

nadzorczym utworzonym na mocy art. 25 decyzji Rady 2009/917/WSiSW[21] w zakresie niezbędnym do wykonywania odnośnych obowiązków tych organów, w szczególności poprzez wzajemne przekazywanie istotnych informacji, wzywanie krajowych organów nadzorczych do wykonywania ich uprawnień lub odpowiadanie na wezwania takich organów.

Artykuł 62
Skoordynowany nadzór ze strony Europejskiego Inspektora Ochrony Danych i krajowych organów nadzorczych

1. W przypadku, w którym w danym akcie Unii zamieszczono odwołanie do niniejszego artykułu, Europejski Inspektor Ochrony Danych czynnie współpracuje z krajowymi organami nadzorczymi, aby zapewnić skuteczny nadzór nad dużymi systemami informatycznymi lub agencjami unijnymi.

2. Działając w zakresie swoich odpowiednich kompetencji i w ramach swoich obowiązków, Europejski Inspektor Ochrony Danych może prowadzić wymianę odpowiednich informacji, pomagać w przeprowadzaniu audytów i inspekcji, badać trudności w interpretacji lub stosowaniu niniejszego rozporządzenia i innych aktów Unii mających zastosowanie, analizować problemy związane z przeprowadzaniem niezależnego nadzoru lub korzystaniem z praw przez osoby, których dane dotyczą, sporządzać zharmonizowane wnioski dotyczące rozwiązań wszelkich problemów oraz propagować wiedzę na temat praw do ochrony danych, zależnie od potrzeb, wraz z krajowymi organami nadzoru.

3. Do celów określonych w ust. 2 Europejski Inspektor Ochrony Danych spotyka się z krajowymi organami nadzorczymi co najmniej dwa razy w roku w ramach Europejskiej Rady Ochrony Danych. Koszty tych spotkań i ich obsługa leżą w gestii Europejskiej Rady Ochrony Danych. Podczas pierwszego spotkania zostaje przyjęty regulamin wewnętrzny. Dalsze metody pracy opracowywane są wspólnie, w zależności od potrzeb.

4. Co dwa lata Europejska Rada Ochrony Danych przesyła wspólne sprawozdanie dotyczące działań związanych ze skoordynowanym nadzorem do Parlamentu Europejskiego, Rady i Komisji.

[21] Decyzja Rady 2009/917/WSiSW z dnia 30 listopada 2009 r. w sprawie stosowania technologii informatycznej do potrzeb celnych, Dz.U. L 323 z 10.12.2009, s. 20–30.

ROZDZIAŁ VIII

ŚRODKI OCHRONY PRAWNEJ, ODPOWIEDZIALNOŚĆ I SANKCJE

Artykuł 63
Prawo do wniesienia skargi do Europejskiego Inspektora Ochrony Danych

1. Bez uszczerbku dla środków ochrony prawnej, administracyjnej lub pozasądowej, każda osoba, której dane dotyczą, ma prawo wnieść skargę do Europejskiego Inspektora Ochrony Danych, jeżeli sądzi, że przetwarzanie danych osobowych jej dotyczących narusza niniejsze rozporządzenie.

2. Europejski Inspektor Ochrony Danych informuje osobę, której dane dotyczą, o postępach i efektach rozpatrywania skargi, w tym o możliwości skorzystania z sądowego środka ochrony prawnej na mocy art. 64.

3. Jeżeli Europejski Inspektor Ochrony Danych nie rozpatrzy skargi lub w ciągu trzech miesięcy nie poinformuje osoby, której dane dotyczą, o postępach i efektach rozpatrywania skargi, skargę uznaje się za odrzuconą.

Artykuł 64
Prawo do skutecznego środka ochrony prawnej

Trybunał Sprawiedliwości Unii Europejskiej jest właściwy w sporach odnoszących się do przepisów niniejszego rozporządzenia, w tym dotyczących roszczeń odszkodowawczych.

Artykuł 65
Prawo do odszkodowania

Każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia niniejszego rozporządzenia, ma prawo uzyskać od administratora lub podmiotu przetwarzającego odszkodowanie za poniesioną szkodę, z zastrzeżeniem warunków określonych w Traktatach.

Artykuł 66
Administracyjne kary pieniężne

1. Europejski Inspektor Ochrony Danych może nakładać administracyjne kary pieniężne na instytucje i organy unijne – w zależności od okoliczności w poszczególnych przypadkach – w sytuacji gdy instytucja unijna lub organ unijny nie zastosują się do poleceń Europejskiego Inspektora Ochrony Danych na podstawie art. 59 ust. 2 lit. d)–h) i j). W czasie podejmowania decyzji o nałożeniu administracyjnej kary pieniężnej oraz ustalaniu jej wysokości w każdym indywidualnym przypadku należytą uwagę zwraca się na:

a) charakter, wagę i czas trwania naruszenia przy uwzględnieniu charakteru, zakresu lub celu danego przetwarzania, liczby poszkodowanych osób, których dane dotyczą, oraz rozmiaru poniesionej przez nie szkody;

b) działania podjęte przez instytucję unijną lub organ unijny w celu zminimalizowania szkody poniesionej przez osoby, których dane dotyczą;

c) stopień odpowiedzialności instytucji unijnej lub organu unijnego z uwzględnieniem środków technicznych i organizacyjnych wdrożonych przez nich na mocy art. 27 i 33;

d) wszelkie wcześniejsze podobne naruszenia ze strony instytucji unijnej lub organu unijnego;

d) stopień współpracy z Europejskim Inspektorem Ochrony Danych w celu usunięcia naruszenia oraz złagodzenia jego ewentualnych negatywnych skutków;

e) kategorie danych osobowych, których dotyczyło naruszenie;

f) sposób, w jaki Europejski Inspektor Ochrony Danych dowiedział się o naruszeniu, w szczególności, czy i w jakim zakresie instytucja unijna lub organ unijny zgłosili naruszenie;

g) jeżeli wobec instytucji unijnej lub organu unijnego, których sprawa dotyczy, zostały wcześniej zastosowane w tej samej sprawie środki, o których mowa w art. 59 – przestrzeganie tych środków.

Procedurę, która prowadzi do nałożenia tych kar pieniężnych, należy przeprowadzić w rozsądnych ramach czasowych po uwzględnieniu okoliczności sprawy i właściwych czynności i procedur, o których mowa w art. 69.

2. Zgodnie z ust. 1 naruszenia obowiązków instytucji unijnej lub organu unijnego, o których to obowiązkach mowa w art. 8, 12, 27, 28, 29, 30, 31, 32, 33, 37, 38, 39, 40, 44, 45 i 46 podlegają administracyjnym karom pieniężnym w wysokości do 25 000 EUR za jedno naruszenie i do wysokości łącznej kwoty 250 000 EUR rocznie.

3. Zgodnie z ust. 1 administracyjnym karom pieniężnym w wysokości do 50 000 EUR za jedno naruszenie i do wysokości łącznej kwoty 500 000 EUR rocznie podlega naruszenie przez instytucję unijną lub organ unijny przepisów dotyczących następujących kwestii:

a) podstawowych zasad przetwarzania, w tym warunków zgody, o których to zasadach i warunkach mowa w art. 4, 5, 7 i 10;

b) praw osób, których dane dotyczą, o których mowa w art. 14–24;

c) przekazywania danych osobowych odbiorcy w państwie trzecim lub organizacji międzynarodowej, o którym to przekazywaniu mowa w art. 47–51.

4. Jeżeli instytucja unijna lub organ unijny wielokrotnie naruszają w ramach tych samych, powiązanych lub stałych operacji przetwarzania kilka przepisów lub ten sam

przepis niniejszego rozporządzenia, całkowita wysokość administracyjnej kary pieniężnej nie przekracza wysokości kary za najpoważniejsze naruszenie.

5. Przed podjęciem decyzji na podstawie niniejszego artykułu Europejski Inspektor Ochrony Danych umożliwia instytucji unijnej lub organowi unijnemu, będącym przedmiotem procedury prowadzonej przez Inspektora, wypowiedzenie się na temat kwestii, co do których Inspektor wyraził zastrzeżenia. Europejski Inspektor Ochrony Danych wydaje swoje decyzje wyłącznie w oparciu o zastrzeżenia, na których temat zainteresowane strony mogły się wypowiedzieć. Skarżący muszą być ściśle związani z postępowaniem.

6. W toku postępowania przestrzega się prawa stron do obrony. Strony mają prawo dostępu do akt Europejskiego Inspektora Ochrony Danych, z zastrzeżeniem uzasadnionych interesów osób fizycznych lub przedsiębiorstw w zakresie ochrony ich danych osobowych lub tajemnic handlowych.

7. Środki zgromadzone poprzez nakładanie kar pieniężnych przewidziane w niniejszym artykule stanowią dochód budżetu ogólnego Unii Europejskiej.

Artykuł 67
Reprezentowanie osób, których dane dotyczą

Osoba, której dane dotyczą, ma prawo umocować podmiot, organizację lub zrzeszenie – które nie mają charakteru zarobkowego, zostały należycie ustanowione zgodnie z prawem Unii lub prawem państwa członkowskiego, mają cele statutowe leżące w interesie publicznym 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 do Europejskiego Inspektora Ochrony Danych oraz wykonywania w jej imieniu praw, o których mowa w art. 63, oraz żądania w jej imieniu odszkodowania, o którym mowa w art. 65.

Artykuł 68
Skargi pracowników Unii

Każda osoba zatrudniona w instytucji unijnej lub organie unijnym może złożyć skargę do Europejskiego Inspektora Ochrony Danych, dotyczącą domniemanego naruszenia przepisów niniejszego rozporządzenia regulującego przetwarzanie danych osobowych, bez użycia oficjalnych dróg. Nikt nie może doznać szkody z powodu wniesienia skargi dotyczącej takiego naruszenia do Europejskiego Inspektora Ochrony Danych.

Artykuł 69
Kary

Niedopełnienie obowiązków określonych w niniejszym rozporządzeniu, niezależnie od tego, czy umyślne czy nieumyślne, powoduje, że urzędnik lub inny funkcjonariusz Unii Europejskiej podlega karze dyscyplinarnej lub innej karze zgodnie z przepisami i procedurami ustanowionymi przez regulamin pracowniczy urzędników Unii Europejskiej lub w warunkach zatrudnienia innych pracowników Wspólnot Europejskich.

ROZDZIAŁ IX

AKTY WYKONAWCZE

Artykuł 70
Procedura komitetowa

1. Komisję wspomaga komitet utworzony na mocy art. 93 rozporządzenia (UE) 2016/679. Komitet ten jest komitetem w rozumieniu rozporządzenia (UE) nr 182/2011.

2. W przypadku odesłania do niniejszego ustępu stosuje się art. 5 rozporządzenia (UE) nr 182/2011.

ROZDZIAŁ X

PRZEPISY KOŃCOWE

Artykuł 71
Uchylenie rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE

Rozporządzenie (WE) nr 45/2001[22] i decyzja nr 1247/2002/WE[23] tracą moc ze skutkiem od dnia 25 maja 2018 r. Odesłania do uchylonego rozporządzenia oraz uchylonej decyzji rozumie się jako odesłania do niniejszego rozporządzenia.

Artykuł 72
Środki przejściowe

1. Niniejsze rozporządzenie nie wpływa na decyzję Parlamentu Europejskiego i Rady 2014/886/UE[24] oraz obecną kadencję Europejskiego Inspektora Ochrony Danych i zastępcy inspektora.

2. W odniesieniu do określania wynagrodzenia, dodatków, emerytury za wysługę lat i innych świadczeń w miejsce wynagrodzenia zastępcę inspektora traktuje się na równi z sekretarzem Trybunału Sprawiedliwości Unii Europejskiej.

---

22 Rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych, Dz.U. L 8 z 12.1.2001.

23 Decyzja nr 1247/2002/WE Parlamentu Europejskiego, Rady i Komisji z dnia 1 lipca 2002 r. w sprawie regulaminu i ogólnych warunków regulujących wykonywanie obowiązków przez Europejskiego Pełnomocnika ds. Ochrony Danych, Dz.U. L 183 z 12.7.2002, s. 1.

24 Decyzja Parlamentu Europejskiego i Rady 2014/886/UE z dnia 4 grudnia 2014 r. w sprawie mianowania Europejskiego Inspektora Ochrony Danych i jego zastępcy, Dz.U. L 351 z 9.12.2014, s. 9.

3. Artykuł 54 ust. 4, 5 i 7 oraz art. 56 i 57 niniejszego rozporządzenia mają zastosowanie do obecnego zastępcy inspektora do końca jego kadencji, tj. do dnia 5 grudnia 2019 r.

4. Zastępca inspektora pomaga Europejskiemu Inspektorowi Ochrony Danych w wypełnianiu jego obowiązków i zastępuje Europejskiego Inspektora Ochrony Danych podczas jego nieobecności lub w sytuacji pozbawienia go możliwości wykonywania obowiązków do końca kadencji zastępcy inspektora, tj. do dnia 5 grudnia 2019 r.

Artykuł 73
Wejście w życie i stosowanie

1. Niniejsze rozporządzenie wchodzi w życie dwudziestego dnia po publikacji w *Dzienniku Urzędowym Unii Europejskiej*.

2. Niniejsze rozporządzenie ma zastosowanie od dnia 25 maja 2018 r.

Niniejsze rozporządzenie wiąże w całości i jest bezpośrednio stosowane we wszystkich państwach członkowskich.

Sporządzono w Brukseli dnia r.

W imieniu Parlamentu Europejskiego	*W imieniu Rady*
Przewodniczący	*Przewodniczący*

OCENA SKUTKÓW FINANSOWYCH REGULACJI

1. STRUKTURA WNIOSKU/INICJATYWY

1.1. Tytuł wniosku/inicjatywy

1.2. Dziedziny polityki w strukturze ABM/ABB, których dotyczy wniosek/inicjatywa

1.3. Charakter wniosku/inicjatywy

1.4. Cel(e)

1.5. Uzasadnienie wniosku/inicjatywy

1.6. Okres trwania działania i jego wpływ finansowy

1.7. Planowane tryby zarządzania

2. ŚRODKI ZARZĄDZANIA

2.1. Zasady nadzoru i sprawozdawczości

2.2. System zarządzania i kontroli

2.3. Środki zapobiegania nadużyciom finansowym i nieprawidłowościom

3. SZACUNKOWY WPŁYW FINANSOWY WNIOSKU/INICJATYWY

3.1. Działy wieloletnich ram finansowych i linie budżetowe po stronie wydatków, na które wniosek/inicjatywa ma wpływ

3.2. Szacunkowy wpływ na wydatki

3.2.1. Synteza szacunkowego wpływu na wydatki

3.2.2. Szacunkowy wpływ na środki operacyjne

3.2.3. Szacunkowy wpływ na środki administracyjne

3.2.4. Zgodność z obowiązującymi wieloletnimi ramami finansowymi

3.2.5. Udział osób trzecich w finansowaniu

3.3. Szacunkowy wpływ na dochody

OCENA SKUTKÓW FINANSOWYCH REGULACJI

1. STRUKTURA WNIOSKU/INICJATYWY

1.1. Tytuł wniosku/inicjatywy

Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez unijne instytucje, organy i jednostki organizacyjne oraz swobodnego przepływu takich danych i uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE.

1.2. Dziedziny polityki w strukturze ABM/ABB, których dotyczy wniosek/inicjatywa[25]

Wymiar sprawiedliwości – ochrona danych osobowych

1.3. Charakter wniosku/inicjatywy

☐ Wniosek/inicjatywa dotyczy **nowego działania**

☐ Wniosek/inicjatywa dotyczy **nowego działania będącego następstwem projektu pilotażowego/działania przygotowawczego**[26]

– Wniosek/inicjatywa wiąże się z **przedłużeniem bieżącego działania**

☐ Wniosek/inicjatywa dotyczy **działania, które zostało przekształcone pod kątem nowego działania**

1.4. Cel(e)

1.4.1. Wieloletnie cele strategiczne Komisji wskazane we wniosku/inicjatywie

Wejście w życie traktatu lizbońskiego – w szczególności wprowadzenie nowej podstawy prawnej (art. 16 TFUE) – stwarza możliwość ustanowienia kompleksowych ram ochrony danych obejmujących wszystkie obszary.

Dnia 27 kwietnia 2016 r. Unia przyjęła rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Tekst mający znaczenie dla EOG), Dz.U. L 119 z 4.5.2016, s. 1–88.

[25] ABM: activity-based management: zarządzanie kosztami działań; ABB: activity-based budgeting: budżet zadaniowy.

[26] O którym mowa w art. 54 ust. 2 lit. a) lub b) rozporządzenia finansowego.

W tym samym dniu Unia przyjęła dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW, Dz.U. L 119 z 4.5.2016, s. 89–131.

Celem niniejszego wniosku jest uzupełnienie kompleksowych ram ochrony danych obejmujących wszystkie obszary w Unii poprzez dostosowanie przepisów o ochronie danych mających zastosowanie do instytucji i organów unijnych do przepisów o ochronie danych zawartych w rozporządzeniu (UE) 2016/679. Ze względu na wymóg konsekwencji i spójności instytucje i organy unijne powinny zastosować podobny zestaw przepisów o ochronie danych jak sektor publiczny w państwach członkowskich.

1.4.2. Cele szczegółowe i działania ABM/ABB, których dotyczy wniosek/inicjatywa

Cel szczegółowy nr 1:

zapewnić spójne stosowanie przepisów o ochronie danych w całej Unii.

Cel szczegółowy nr 2:

zracjonalizować obecny model zarządzania ochroną danych w instytucjach i organach unijnych.

Cel szczegółowy nr 3:

zapewnić lepsze przestrzeganie przepisów o ochronie danych w instytucjach i organach unijnych oraz ich egzekwowanie.

1.4.3. Oczekiwane wyniki i wpływ

Należy wskazać, jakie efekty przyniesie wniosek/inicjatywa beneficjentom/grupie docelowej.

Jeżeli chodzi o instytucje i organy unijne działające w charakterze administratorów danych, powinny one skorzystać z przejścia z obecnych procesów administracyjnych (podejście *ex ante*) związanych z ochroną danych na podejście opierające się na skutecznym przestrzeganiu przepisów prawa materialnego dotyczącego ochrony danych i nowych zasad oraz koncepcji dotyczących ochrony danych wprowadzonych rozporządzeniem (UE) 2016/679, które będą miały zastosowanie w całej Unii, i na skuteczniejszym ich egzekwowaniu (podejście *ex post*).

Osoby fizyczne, których dane przetwarzają instytucje i organy unijne, będą mogły lepiej kontrolować swoje dane osobowe i będą miały zaufanie do otoczenia cyfrowego. Będą również miały do czynienia z lepszą rozliczalnością instytucji i organów unijnych.

Europejski Inspektor Ochrony Danych będzie mógł się w większym stopniu skoncentrować na swojej roli nadzorczej. Zadania polegające na udzielaniu zaleceń Komisji zostaną bardziej precyzyjnie rozdzielone między Europejską Radę Ochrony Danych utworzoną rozporządzeniem (UE) 2016/679 a Europejskim Inspektorem Ochrony Danych, dzięki czemu zadania tych podmiotów nie będą się powielać.

1.4.4. Wskaźniki wyników i wpływu

Należy określić wskaźniki, które umożliwią monitorowanie realizacji wniosku/inicjatywy.

Wskaźniki obejmują następujące elementy:

liczbę opinii wydanych przez Europejską Radę Ochrony Danych i Europejskiego Inspektora Ochrony Danych;

podział działań inspektorów ochrony danych;

wykorzystanie oceny skutków w zakresie ochrony danych;

liczbę skarg złożonych przez osoby, których dane dotyczą;

grzywny nałożone na administratorów danych odpowiedzialnych za naruszenie ochrony danych.

1.5. Uzasadnienie wniosku/inicjatywy

1.5.1. Potrzeby, które mają zostać zaspokojone w perspektywie krótko- lub długoterminowej

W rozporządzeniu (UE) 2016/679 (art. 2 ust. 3, art. 98, motyw 17) współprawodawcy unijni wezwali do dostosowania rozporządzenia (WE) nr 45/2001 do zasad i przepisów ustanowionych w rozporządzeniu (UE) 2016/679, aby zapewnić silne i spójne ramy ochrony danych w Unii oraz umożliwić zastosowanie obydwu instrumentów w tym samym czasie, tj. dnia 25 maja 2018 r.

1.5.2. Wartość dodana z tytułu zaangażowania Unii Europejskiej

Przepisy o ochronie danych mające zastosowanie do instytucji i organów unijnych można wprowadzić wyłącznie w drodze aktu UE.

1.5.3. Główne wnioski wyciągnięte z podobnych działań

Niniejszy wniosek opiera się na doświadczeniach zdobytych w związku z rozporządzeniem (WE) nr 45/2001 oraz na ocenie jego stosowania przeprowadzonej w ramach badania oceniającego (przeprowadzonego przez zewnętrznego wykonawcę w okresie od września 2014 r. do czerwca 2015 r.)[27].

1.5.4. Spójność z innymi właściwymi instrumentami oraz możliwa synergia (ang. Compatibility and possible synergy with other appropriate instruments).

Niniejszy wniosek opiera się na rozporządzeniu (UE) 2016/679 i stanowi sfinalizowanie prac nad utworzeniem solidnych, spójnych i nowoczesnych ram ochrony danych w Unii – neutralnych pod względem technologicznym i zachowujących aktualność.

[27] JUST/2013/FRAC/FW/0157/A4 w związku z wielokrotną umową ramową JUST/2011/EVAL/01 (RS 2013/05) – sprawozdanie „Evaluation Study on Regulation (EC) 45/2001", Ernst and Young.

1.6. Okres trwania działania i jego wpływ finansowy

☐ Wniosek/inicjatywa o ograniczonym **okresie trwania**

– ☐ Okres trwania wniosku/inicjatywy: od [DD/MM]RRRR r. do [DD/MM]RRRR r.

– ☐ Okres trwania wpływu finansowego: od RRRR r. do RRRR r.

- Wniosek/inicjatywa o **nieograniczonym okresie trwania**
- Wprowadzenie w życie z okresem rozruchu od [2017 r.] do dnia 25 maja 2018 r., po którym następuje faza operacyjna.

1.7. Planowane tryby zarządzania[28]

- Bezpośrednie zarządzanie przez Komisję

– ☐ w ramach jej służb, w tym za pośrednictwem jej pracowników w delegaturach Unii;

– ☐ przez agencje wykonawcze

☐ **Zarządzanie dzielone** z państwami członkowskimi

☐ **Zarządzanie pośrednie** poprzez przekazanie zadań związanych z wykonaniem budżetu:

– ☐ państwom trzecim lub organom przez nie wyznaczonym;

– ☐ organizacjom międzynarodowym i ich agencjom (należy wyszczególnić);

– ☐EBI oraz Europejskiemu Funduszowi Inwestycyjnemu;

– ☐ organom, o których mowa w art. 208 i 209 rozporządzenia finansowego;

– ☐ organom prawa publicznego;

– ☐ podmiotom podlegającym prawu prywatnemu, które świadczą usługi użyteczności publicznej, o ile zapewniają one odpowiednie gwarancje finansowe;

– ☐ podmiotom podlegającym prawu prywatnemu państwa członkowskiego, którym powierzono realizację partnerstwa publiczno-prywatnego oraz które zapewniają odpowiednie gwarancje finansowe;

– ☐ osobom odpowiedzialnym za wykonanie określonych działań w dziedzinie wspólnej polityki zagranicznej i bezpieczeństwa na mocy tytułu V Traktatu o Unii Europejskiej oraz określonym we właściwym podstawowym akcie prawnym.

---

[28] Wyjaśnienia dotyczące trybów zarządzania oraz odniesienia do rozporządzenia finansowego znajdują się na następującej stronie: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html

– *W przypadku wskazania więcej niż jednego trybu należy podać dodatkowe informacje w części „Uwagi”.*

Uwagi

Wniosek jest ograniczony do wszystkich instytucji i organów unijnych i tylko na nie ma wpływ.

2. ŚRODKI ZARZĄDZANIA

2.1. Zasady nadzoru i sprawozdawczości

Należy określić częstotliwość i warunki.

Niniejszy wniosek jest ograniczony do stosowania przepisów o ochronie danych przez instytucje i organy unijne. Sprawowanie nadzoru nad stosowaniem tych przepisów oraz ich egzekwowanie należy do zadań Europejskiego Inspektora Ochrony Danych. Monitorowanie oraz sprawozdawczość zapewnia zatem Europejski Inspektor Ochrony Danych. W szczególności zgodnie z art. 60 niniejszego wniosku Europejski Inspektor Ochrony Danych jest zobowiązany do składania rocznych sprawozdań z działalności wchodzącej w zakres jego kompetencji Parlamentowi Europejskiemu, Radzie i Komisji oraz do jednoczesnego publikowania tych sprawozdań.

2.2. System zarządzania i kontroli

2.2.1. Zidentyfikowane ryzyko

Badanie oceniające stosowanie rozporządzenia (WE) nr 45/2001 przeprowadził zewnętrzny wykonawca w okresie od września 2014 r. do czerwca 2015 r. Dotyczy ono również skutków wprowadzenia kluczowych koncepcji i zasad zawartych w rozporządzeniu (UE) 2016/679 w instytucjach i organach unijnych.

W nowym modelu ochrony danych szczególny nacisk zostanie położony na skuteczne przestrzeganie przepisów o ochronie danych oraz skuteczny nadzór nad egzekwowaniem tych przepisów. Będzie to wymagało zmiany w kulturze ochrony danych w instytucjach i organach unijnych polegającej na przejściu z administracyjnego podejścia *ex ante* na podejście oparte na skuteczności *ex post*.

2.2.2. Informacje dotyczące struktury wewnętrznego systemu kontroli

Istniejące metody kontroli stosowane przez instytucje i organy unijne

2.2.3. Oszacowanie kosztów i korzyści wynikających z kontroli i ocena prawdopodobnego ryzyka błędu

Istniejące metody kontroli stosowane przez instytucje i organy unijne

2.3. Środki zapobiegania nadużyciom finansowym i nieprawidłowościom

Określić istniejące lub przewidywane środki zapobiegania i ochrony.

Istniejące metody kontroli zapobiegania oszustwom stosowane przez instytucje i organy unijne

3. SZACUNKOWY WPŁYW FINANSOWY WNIOSKU/INICJATYWY

3.1. Działy wieloletnich ram finansowych i linie budżetowe po stronie wydatków, na które wniosek/inicjatywa ma wpływ

- Istniejące linie budżetowe

Według działów wieloletnich ram finansowych i linii budżetowych.

Dział wieloletnich ram finansowych	Linia budżetowa	Rodzaj wydatków	Wkład			
	Numer [Dział……...……]	Zróżnicowane/niezróżnicowane[29]	państw EFTA[30]	krajów kandydujących[31]	państw trzecich	w rozumieniu art. 21 ust. 2 lit. b) rozporządzenia finansowego
	[XX.YY.YY.YY]	Zróżnicowane/niezróżnicowane	TAK/ NIE	TAK/ NIE	TAK/ NIE	TAK/ NIE

- Nowe linie budżetowe, o których utworzenie się wnioskuje

Według działów wieloletnich ram finansowych i linii budżetowych.

Dział wieloletnich ram finansowych	Linia budżetowa	Rodzaj wydatków	Wkład			
	Numer [Dział……...……]	Zróżnicowane/niezróżnicowane	państw EFTA	krajów kandydujących	państw trzecich	w rozumieniu art. 21 ust. 2 lit. b) rozporządzenia finansowego
	[XX.YY.YY.YY]		TAK/ NIE	TAK/ NIE	TAK/ NIE	TAK/ NIE

[29] Środki zróżnicowane / środki niezróżnicowane.

[30] EFTA: Europejskie Stowarzyszenie Wolnego Handlu.

[31] Kraje kandydujące oraz w stosownych przypadkach potencjalne kraje kandydujące Bałkanów Zachodnich.

3.2. Szacunkowy wpływ na wydatki

Wpływ na wydatki niniejszego wniosku jest ograniczony do wydatków instytucji i organów unijnych. Ocena kosztów związanych z niniejszym wnioskiem wskazuje jednak, że nie prowadzi on do powstania istotnych dodatkowych kosztów dla instytucji i organów unijnych.

Jeżeli chodzi o administratorów danych w instytucjach i organach unijnych, badanie oceniające rozporządzenie (WE) nr 45/2001 wskazuje, że ich działalność związana z ochroną danych odpowiada około 70 ekwiwalentom pełnego czasu pracy (EPC), tj. około 9,3 mln EUR rocznie. Około 20 % ich działań związanych z ochroną danych jest obecnie poświęconych zgłoszeniom dotyczącym przetwarzania danych. Działalność tę zniesiono niniejszym rozporządzeniem, co odpowiada rocznym oszczędnościom w wysokości 1,922 mln EUR w odniesieniu do administratorów danych w instytucjach i organach unijnych. Oczekuje się, że oszczędności te zostaną zrównoważone zwiększonym zaangażowaniem administratorów danych we wdrażanie nowych zasad i koncepcji wprowadzonych niniejszym rozporządzeniem.

Ściślej rzecz ujmując, z ankiety przeprowadzonej w ramach badania oceniającego wynika, że wprowadzenie:

a) zasady minimalizacji danych wiązałoby się z minimalnym wpływem na instytucje i organy unijne lub jego brakiem;

b) zasady przejrzystości nie miałoby znaczącego wpływu na instytucje i organy unijne;

c) zwiększonych obowiązków informacyjnych doprowadziłoby do zwiększania obciążenia pracą administratorów danych i inspektorów ochrony danych;

d) prawa do bycia zapomniany nie miałoby znaczącego wpływu na instytucje i organy unijne;

e) prawa do przenoszenia danych wiązałoby się z minimalnym wpływem na instytucje i organy unijne lub z jego brakiem;

f) ocen skutków w zakresie ochrony danych miałoby umiarkowanie znaczący wpływ na obciążenie pracą administratorów danych i inspektorów ochrony danych, ponieważ niektóre instytucje i organy unijne przygotowują już te oceny skutków, a liczba przypadków, w których będzie należało je sporządzać, jest ograniczona;

g) zgłoszeń dotyczących naruszeń ochrony danych osobowych zwiększyłyby obciążenie pracą administratorów danych, ale tego rodzaju naruszenia nie są częste;

h) a zasady uwzględniania ochrony danych w fazie projektowania i domyślnej ochrony danych są już stosowane przez kilka instytucji i organów unijnych.

Ponadto w ocenie skutków sporządzonej przed przyjęciem wniosku w sprawie pakietu dotyczącego reformy ochrony danych stwierdzono, że: „organy publiczne ani administratorzy danych nie ponosiliby żadnego obciążenia administracyjnego w wyniku wprowadzenia zasady uwzględnienia ochrony danych już w fazie projektowania”[32].

Jeżeli chodzi o inspektorów ochrony danych, w badaniu oceniającym oszacowano koszt obecnej sieci inspektorów ochrony danych i koordynatorów ds. ochrony danych w instytucjach i organach unijnych na 82,9 EPC lub 10,9 mln EUR rocznie. Spędzają oni 26 % czasu związanego z ochroną danych na działania zniesione niniejszym rozporządzeniem, tj. sporządzanie zgłoszeń (zamiast administratorów danych), ocenę otrzymanych zgłoszeń oraz prowadzenie rejestrów i przeprowadzanie kontroli wstępnych. Prowadzi to do dalszych oszczędności w wysokości 2,834 mln EUR rocznie w odniesieniu do instytucji i organów unijnych. Ponadto niniejsze rozporządzenie stwarza możliwość uzyskania potencjalnych dodatkowych oszczędności, umożliwiając instytucjom i organom unijnym zlecanie na zewnątrz wykonywania zadań inspektora ochrony danych zamiast powierzania ich własnemu personelowi.

Zawężenie zakresu zadań inspektora ochrony danych zostanie zrównoważone wykonywaniem przez nich rozszerzonych obowiązków informacyjnych, uczestniczeniem w sporządzaniu ocen skutków w zakresie ochrony danych (w określonych okolicznościach, jeżeli oceny te będą wymagane) oraz w uprzednich konsultacjach z Europejskim Inspektorem Ochrony Danych (których zakres będzie znacznie bardziej ograniczony w porównaniu z obecnym obowiązkiem dotyczącym kontroli wstępnej).

Jeżeli chodzi o Europejskiego Inspektora Ochrony Danych, jego roczny budżet jest stosunkowo stabilny od 2011 r. i oscyluje wokół kwoty około 8 mln EUR. Obecnie liczba personelu w dziale ds. nadzoru i egzekwowania oraz dziale ds. polityki i konsultacji EIOD jest podobna i utrzymuje się na stałym poziomie od 2008 r. Przywiązanie większej wagi w niniejszym rozporządzeniu do nadzorczej roli Europejskiego Inspektora Ochrony Danych zostanie zrównoważone bardziej ukierunkowaną rolą doradczą i wyeliminowaniem powielania zadań Europejskiej Rady Ochrony Danych. Przesunięcia personelu Europejskiego Inspektora Ochrony Danych można zatem dokonać wewnętrznie.

[32] Dokument roboczy służb Komisji, ocena skutków, SEC(2012) 72 final, s. 110.

W niniejszym wniosku przewidziano możliwość nakładania administracyjnych kar pieniężnych na instytucje i organy unijne przez Europejskiego Inspektora Ochrony Danych. Na każdą instytucję unijną lub każdy organ unijny można nałożyć karę w maksymalnej wysokości 250 000 EUR rocznie (25 000 EUR za każde naruszenie) lub 500 000 rocznie (50 000 EUR za każde naruszenie) z tytułu najcięższych naruszeń niniejszego rozporządzenia. Oczekuje się, że tego rodzaju kary będą nakładane jedynie w najbardziej poważnych okolicznościach i w następstwie nieprzestrzegania przepisów przez instytucję unijną lub organ unijny, w przypadku gdy Europejski Inspektor Ochrony Danych wykonuje swoje uprawnienia naprawcze. Oczekuje się zatem, że skutek finansowy takich kar jest ograniczony.

3.2.1. Synteza szacunkowego wpływu na wydatki

w mln EUR (do trzech miejsc po przecinku)

Dział wieloletnich ram finansowych	Numer	[Dział……...…….]

Dyrekcja Generalna <…….>			Rok **N**[33]	Rok **N+1**	Rok **N+2**	Rok **N+3**	Wprowadzić taką liczbę kolumn dla poszczególnych lat, jaka jest niezbędna, by odzwierciedlić cały okres wpływu (por. pkt 1.6)			**OGÓŁEM**
• Środki operacyjne										
Numer linii budżetowej	Zobowiązania	(1)								
	Płatności	(2)								
Numer linii budżetowej	Zobowiązania	(1a)								
	Płatności	(2a)								
Środki administracyjne finansowane ze środków przydzielonych na określone programy operacyjne[34]										

[33] Rok N jest rokiem, w którym rozpoczyna się wprowadzanie w życie wniosku/inicjatywy.

[34] Wsparcie techniczne lub administracyjne oraz wydatki na wsparcie w zakresie wprowadzania w życie programów lub działań UE (dawne linie „BA"), pośrednie badania naukowe, bezpośrednie badania naukowe.

Numer linii budżetowej		(3)								
Środki OGÓŁEM dla Dyrekcji Generalnej <…….>	Zobowiązania	=1+1a +3								
	Płatności	=2+2a +3								

• OGÓŁEM środki operacyjne	Zobowiązania	(4)								
	Płatności	(5)								
• OGÓŁEM środki administracyjne finansowane ze środków przydzielonych na określone programy operacyjne		(6)								
Środki OGÓŁEM na DZIAŁ <…> wieloletnich ram finansowych	Zobowiązania	=4+6								
	Płatności	=5+6								

Jeżeli wpływ wniosku/inicjatywy nie ogranicza się do jednego działu:

• OGÓŁEM środki operacyjne	Zobowiązania	(4)								
	Płatności	(5)								
• OGÓŁEM środki administracyjne finansowane ze środków przydzielonych na określone programy operacyjne		(6)								
Środki OGÓŁEM na DZIAŁY 1–4 wieloletnich ram finansowych (Kwota referencyjna)	Zobowiązania	=4+6								
	Płatności	=5+6								

Dział wieloletnich ram finansowych	**5**	„Wydatki administracyjne”

w mln EUR (do trzech miejsc po przecinku)

		Rok **N**	Rok **N+1**	Rok **N+2**	Rok **N+3**	Wprowadzić taką liczbę kolumn dla poszczególnych lat, jaka jest niezbędna, by odzwierciedlić cały okres wpływu (por. pkt 1.6)			**OGÓŁEM**
Dyrekcja Generalna <…….>									
• Zasoby ludzkie									
• Pozostałe wydatki administracyjne									
OGÓŁEM Dyrekcja Generalna <…….>	Środki								

Środki OGÓŁEM na DZIAŁ 5 wieloletnich ram finansowych	(Środki na zobowiązania ogółem = środki na płatności ogółem)								

w mln EUR (do trzech miejsc po przecinku)

		Rok **N**[35]	Rok **N+1**	Rok **N+2**	Rok **N+3**	Wprowadzić taką liczbę kolumn dla poszczególnych lat, jaka jest niezbędna, by odzwierciedlić cały okres wpływu (por. pkt 1.6)			**OGÓŁEM**
Środki OGÓŁEM na DZIAŁY 1–5 wieloletnich ram finansowych	Zobowiązania								
	Płatności								

[35] Rok N jest rokiem, w którym rozpoczyna się wprowadzanie w życie wniosku/inicjatywy.

3.2.2. Szacunkowy wpływ na środki operacyjne

- Wniosek/inicjatywa nie wiąże się z koniecznością wykorzystania środków operacyjnych

☐ Wniosek/inicjatywa wiąże się z koniecznością wykorzystania środków operacyjnych, jak określono poniżej:

Środki na zobowiązania w mln EUR (do trzech miejsc po przecinku)

Określić cele i produkty			Rok **N**		Rok **N+1**		Rok **N+2**		Rok **N+3**		Wprowadzić taką liczbę kolumn dla poszczególnych lat, jaka jest niezbędna, by odzwierciedlić cały okres wpływu (por. pkt 1.6)						**OGÓŁEM**	
	PRODUKT																	
⇩	Rodzaj[36]	Średni koszt	Nie	Koszt	Nie	Koszt	Nie	Koszt	Nie	Koszt	Nie	Koszt	Nie	Koszt	Nie	Koszt	Liczba ogółem	Koszt całkowity
CEL SZCZEGÓŁOWY nr 1[37]…																		
– Produkt																		
– Produkt																		
– Produkt																		
Cel szczegółowy nr 1 – suma cząstkowa																		
CEL SZCZEGÓŁOWY nr 2 ...																		
– Produkt																		
Cel szczegółowy nr 2 – suma cząstkowa																		

[36] Produkty odnoszą się do produktów i usług, które zostaną zapewnione (np. liczba sfinansowanych wymian studentów, liczba kilometrów zbudowanych dróg itp.).

[37] Zgodnie z opisem w pkt 1.4.2. „Cele szczegółowe …”.

KOSZT OGÓŁEM																

3.2.3. Szacunkowy wpływ na środki administracyjne

3.2.3.1. Streszczenie

- Wniosek/inicjatywa nie wiąże się z koniecznością wykorzystania środków administracyjnych

☐ Wniosek/inicjatywa wiąże się z koniecznością wykorzystania środków administracyjnych, jak określono poniżej:

w mln EUR (do trzech miejsc po przecinku)

	Rok **N**[38]	Rok **N+1**	Rok **N+2**	Rok **N+3**	Wprowadzić taką liczbę kolumn dla poszczególnych lat, jaka jest niezbędna, by odzwierciedlić cały okres wpływu (por. pkt 1.6)			**OGÓŁEM**
DZIAŁ 5 wieloletnich ram finansowych								
Zasoby ludzkie								
Pozostałe wydatki administracyjne								
DZIAŁ 5 wieloletnich ram finansowych								

Poza DZIAŁEM 5[39] **wieloletnich ram finansowych**								
Zasoby ludzkie								
Pozostałe wydatki administracyjne								
Poza DZIAŁEM 5 wieloletnich ram finansowych								

OGÓŁEM								

Potrzeby w zakresie środków na zasoby ludzkie i inne środki o charakterze administracyjnym zostaną pokryte z zasobów dyrekcji generalnej już przydzielonych na zarządzanie tym działaniem lub przesuniętych w ramach dyrekcji generalnej,

[38] Rok N jest rokiem, w którym rozpoczyna się wprowadzanie w życie wniosku/inicjatywy.

[39] Wsparcie techniczne lub administracyjne oraz wydatki na wsparcie w zakresie wprowadzania w życie programów lub działań UE (dawne linie „BA"), pośrednie badania naukowe, bezpośrednie badania naukowe.

uzupełnionych w razie potrzeby wszelkimi dodatkowymi zasobami, które mogą zostać przydzielone zarządzającej dyrekcji generalnej w ramach procedury rocznego przydziału środków oraz w świetle istniejących ograniczeń budżetowych.

3.2.3.2. Szacowane zapotrzebowanie na zasoby ludzkie

- Wniosek/inicjatywa nie wiąże się z koniecznością wykorzystania zasobów ludzkich.

☐ Wniosek/inicjatywa wiąże się z koniecznością wykorzystania zasobów ludzkich, jak określono poniżej:

Wartości szacunkowe należy wyrazić w ekwiwalentach pełnego czasu pracy

	Rok **N**	Rok **N+1**	Rok **N+2**	Rok **N+3**	Wprowadzić taką liczbę kolumn dla poszczególnych lat, jaka jest niezbędna, by odzwierciedlić cały okres wpływu (por. pkt 1.6)		
• Stanowiska przewidziane w planie zatrudnienia (stanowiska urzędników i pracowników zatrudnionych na czas określony)							
XX 01 01 01 (w centrali i w biurach przedstawicielstw Komisji)							
XX 01 01 02 (w delegaturach)							
XX 01 05 01 (pośrednie badania naukowe)							
10 01 05 01 (bezpośrednie badania naukowe)							
•Personel zewnętrzny (w ekwiwalentach pełnego czasu pracy)[40]							
XX 01 02 01 (CA, SNE, INT z globalnej koperty finansowej)							
XX 01 02 02 (CA, LA, SNE, INT i JED w delegaturach)							
XX 01 04**yy** [41] – w centrali							
XX 01 04**yy** [41] – w delegaturach							
XX 01 05 02 (CA, SNE, INT – pośrednie badania naukowe)							
10 01 05 02 (CA, SNE, INT – bezpośrednie badania naukowe)							
Inna linia budżetowa (określić)							
OGÓŁEM							

XX oznacza odpowiednią dziedzinę polityki lub odpowiedni tytuł w budżecie.

40 CA = personel kontraktowy; LA = personel miejscowy; SNE = oddelegowany ekspert krajowy; INT = personel tymczasowy; JED = młodszy oddelegowany ekspert.

41 W ramach podpułapu na personel zewnętrzny ze środków operacyjnych (dawne linie „BA").

Potrzeby w zakresie zasobów ludzkich zostaną pokryte z zasobów dyrekcji generalnej już przydzielonych na zarządzanie tym działaniem lub przesuniętych w ramach dyrekcji generalnej, uzupełnionych w razie potrzeby wszelkimi dodatkowymi zasobami, które mogą zostać przydzielone zarządzającej dyrekcji generalnej w ramach procedury rocznego przydziału środków oraz w świetle istniejących ograniczeń budżetowych.

Opis zadań do wykonania:

Urzędnicy i pracownicy zatrudnieni na czas określony	
Personel zewnętrzny	

3.2.4. Zgodność z obowiązującymi wieloletnimi ramami finansowymi

- Wniosek/inicjatywa jest zgodny(-a) z obowiązującymi wieloletnimi ramami finansowymi.

☐ Wniosek/inicjatywa wymaga przeprogramowania odpowiedniego działu w wieloletnich ramach finansowych.

Należy wyjaśnić, na czym ma polegać przeprogramowanie, określając linie budżetowe, których ma ono dotyczyć, oraz podając odpowiednie kwoty.

☐ Wniosek/inicjatywa wymaga zastosowania instrumentu elastyczności lub zmiany wieloletnich ram finansowych.

Należy wyjaśnić, który wariant jest konieczny, określając linie budżetowe, których ma on dotyczyć, oraz podając odpowiednie kwoty.

3.2.5. Udział osób trzecich w finansowaniu

- Wniosek/inicjatywa nie przewiduje współfinansowania ze strony osób trzecich

Wniosek/inicjatywa przewiduje współfinansowanie szacowane zgodnie z poniższym:

Środki w mln EUR (do trzech miejsc po przecinku)

	Rok **N**	Rok **N+1**	Rok **N+2**	Rok **N+3**	Wprowadzić taką liczbę kolumn dla poszczególnych lat, jaka jest niezbędna, by odzwierciedlić cały okres wpływu (por. pkt 1.6)			Ogółem
Określić organ współfinansujący								
OGÓŁEM środki objęte współfinansowaniem								

3.3. Szacunkowy wpływ na dochody

- Wniosek/inicjatywa nie ma wpływu finansowego na dochody.

☐ Wniosek/inicjatywa ma wpływ finansowy określony poniżej:

– ☐ wpływ na zasoby własne

– ☐ wpływ na dochody różne

w mln EUR (do trzech miejsc po przecinku)

Linia budżetowa po stronie dochodów:	Środki zapisane w budżecie na bieżący rok budżetowy	Wpływ wniosku/inicjatywy[42]						
		Rok **N**	Rok **N+1**	Rok **N+2**	Rok **N+3**	Wprowadzić taką liczbę kolumn dla poszczególnych lat, jaka jest niezbędna, by odzwierciedlić cały okres wpływu (por. pkt 1.6)		
Artykuł …….								

W przypadku wpływu na dochody różne „przeznaczone na określony cel" należy wskazać linie budżetowe po stronie wydatków, które ten wpływ obejmie.

Należy określić metodę obliczania wpływu na dochody.

[42] W przypadku tradycyjnych zasobów własnych (opłaty celne, opłaty wyrównawcze od cukru) należy wskazać kwoty netto, tzn. kwoty brutto po odliczeniu 25 % na poczet kosztów poboru.