KOMISJA EUROPEJSKA

Bruksela, dnia 25.1.2012 r.
COM(2012) 11 final

2012/0011 (COD)

Wniosek

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY

w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych)

(Tekst mający znaczenie dla EOG)

{SEC(2012) 72 final}
{SEC(2012) 73 final}

UZASADNIENIE

1. KONTEKST WNIOSKU

Niniejsze uzasadnienie uszczegóławia proponowane nowe ramy prawne ochrony danych osobowych w UE, nakreślone w komunikacie COM (2012) 9 wersja ostateczna[1]. Na proponowane nowe ramy prawne składają się dwa wnioski ustawodawcze:

– wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych), oraz

– wniosek dotyczący dyrektywy Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy na potrzeby zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich i ścigania albo wykonywania kar kryminalnych oraz swobodnego przepływu takich danych[2].

Niniejsze uzasadnienie dotyczy wniosku ustawodawczego w sprawie ogólnego rozporządzenia o ochronie danych.

Podstawowy dokument ustanawiający obowiązujące unijne przepisy o ochronie danych osobowych, dyrektywa 95/46/WE[3], został przyjęty w 1995 r. z myślą o realizacji dwóch celów: ochrony podstawowego prawa do ochrony danych oraz zagwarantowania swobodnego przepływu danych między państwami członkowskimi. Powyższa dyrektywa została uzupełniona przez decyzję ramową 2008/977/WSiSW jako instrument ogólny na szczeblu Unii w zakresie ochrony danych osobowych w obszarze współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych[4].

Szybki rozwój technologiczny przyniósł nowe wyzwania w zakresie ochrony danych osobowych. Niezwykle wzrosła skala wymiany i zbierania danych. Technologia umożliwia zarówno przedsiębiorstwom prywatnym, jak i organom publicznym, wykorzystywanie danych osobowych do wykonywania powierzonych im zadań na niespotykaną dotąd skalę. Osoby fizyczne coraz części udostępniają informacje osobowe publicznie i globalnie. Technologia całkowicie zmieniła zarówno gospodarkę, jak i życie społeczne.

Budowanie zaufania do internetu jest kluczowym elementem rozwoju gospodarczego. Brak zaufania sprawia, że konsumenci nie są pewni, czy kupować w internecie i korzystać z nowych usług. Zagrożenia te spowalniają rozwój innowacyjnego wykorzystania nowych

---

1 „Ochrona prywatności w połączonym świecie – europejskie ramy ochrony danych w XXI wieku" COM(2012) 9 wersja ostateczna.

2 COM(2012) 10 wersja ostateczna.

3 Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, Dz.U. L 281 z 23.11.1995, s. 31.

4 Decyzja ramowa Rady 2008/977/WSiSW z dnia 27 listopada 2008 r. w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych, Dz.U. L 350 z 30.12.2008, s. 60 („decyzja ramowa").

technologii. Ochrona danych odgrywa zatem kluczową rolę w Europejskiej agendzie cyfrowej[5] i szerzej w strategii „Europa 2020”[6].

Artykuł 16 ust. 1 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE), który został wprowadzony traktatem lizbońskim, ustanawia zasadę, zgodnie z którą każda osoba ma prawo do ochrony danych osobowych jej dotyczących. Ponadto w art. 16 ust. 2 TFUE traktat lizboński wprowadził szczególną podstawę prawną dla przyjęcia przepisów dotyczących ochrony danych osobowych. W art. 8 Karty praw podstawowych UE zapisano ochronę danych osobowych jako jedno z praw podstawowych.

Rada Europejska wezwała Komisję do oceny funkcjonowania unijnych instrumentów o ochronie danych oraz przedstawienia, w razie potrzeby, dalszych inicjatyw ustawodawczych lub nieustawodawczych[7]. W rezolucji w sprawie programu sztokholmskiego[8] Parlament Europejski poparł koncepcję kompleksowego systemu ochrony danych w UE, wzywając między innymi do rewizji decyzji ramowej. Komisja podkreśliła w swoim planie działania służącym realizacji programu sztokholmskiego[9] potrzebę zagwarantowania spójnego stosowania podstawowego prawa do ochrony danych osobowych w kontekście wszystkich polityk UE.

W komunikacie w sprawie „Całościowego podejścia do kwestii ochrony danych osobowych w Unii Europejskiej”[10] Komisja stwierdziła, że UE potrzebuje bardziej całościowej i spójnej polityki w zakresie podstawowego prawa do ochrony danych osobowych.

Obecnie obowiązujące ramy nie zmieniły się, jeśli chodzi o ich cele i zasady, jednak nie zapobiegły one rozdrobnieniu sposobów realizacji ochrony danych osobowych w całej Unii, ugruntowaniu niepewności prawnej oraz upowszechnieniu istniejącego w społeczeństwie poglądu, zgodnie z którym z działalnością prowadzoną w internecie wiążą się istotne ryzyka[11]. Dlatego właśnie nadszedł czas, by stworzyć silniejsze i bardziej spójne ramy ochrony danych w UE, poparte zdecydowanym egzekwowaniem, które umożliwią rozwój gospodarki cyfrowej na rynku wewnętrznym, zapewnią osobom fizycznym kontrolę nad ich własnymi danymi oraz wzmocnią pewność prawną i praktyczną dla operatorów gospodarczych i organów publicznych.

2. WYNIKI KONSULTACJI Z ZAINTERESOWANYMI STRONAMI ORAZ OCENY SKUTKÓW

Niniejsza inicjatywa jest rezultatem szeroko zakrojonych konsultacji ze wszystkimi głównymi zainteresowanymi stronami w sprawie przeglądu obowiązujących ram prawnych ochrony

---

5 COM(2010) 245 wersja ostateczna.

6 COM(2010) 2020 wersja ostateczna.

7 „Program sztokholmski – otwarta i bezpieczna Europa dla dobra i ochrony obywateli”, Dz.U. C 115 z 4.5.2010, s. 1.

8 Rezolucja Parlamentu Europejskiego w sprawie komunikatu Komisji do Parlamentu Europejskiego i Rady: –„Przestrzeń wolności, bezpieczeństwa i sprawiedliwości w służbie obywateli” – program sztokholmski, przyjęta dnia 25 listopada 2009 r. (P7_TA(2009)0090)..

9 COM(2010) 171 wersja ostateczna.

10 COM(2010) 609 wersja ostateczna.

11 Specjalna ankieta Eurobarometru (EB) nr 359 „Ochrona danych i tożsamość elektroniczna w UE (2011)”: http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf .

danych osobowych, które trwały ponad dwa lata i objęły konferencję na wysokim szczeblu zorganizowaną w maju 2009 r.[12] oraz dwie fazy konsultacji społecznych:

– od 9 lipca do 31 grudnia 2009 r. *Konsultacje w sprawie ram prawnych w zakresie podstawowego prawa do ochrony danych osobowych.* Komisja otrzymała 168 odpowiedzi, 127 od osób fizycznych, organizacji i zrzeszeń biznesowych oraz 12 od organów publicznych[13];

– od 4 listopada 2010 r. do 15 stycznia 2011 r. *Konsultacje w sprawie kompleksowego podejścia Komisji do ochrony danych osobowych w Unii Europejskiej*. Komisja otrzymała 305 odpowiedzi, z czego 54 od obywateli, 31 od organów publicznych oraz 220 od organizacji prywatnych, w szczególności zrzeszeń biznesowych i organizacji pozarządowych[14].

Przeprowadzono również specjalne konsultacje z najważniejszymi zainteresowanymi stronami. W czerwcu i lipcu 2010 r. zorganizowano specjalne spotkania z organami państw członkowskich oraz z zainteresowanymi stronami z sektora prywatnego, a także organizacjami zajmującymi się prywatnością, ochroną danych oraz organizacjami konsumenckimi[15]. W listopadzie 2010 r. Viviane Reding, wiceprzewodnicząca Komisji Europejskiej, zorganizowała wspólną debatę na temat reformy ochrony danych. W dniu 28 stycznia 2011 r. (Dzień Ochrony Danych) Komisja Europejska i Rada Europy zorganizowały konferencję wysokiego szczebla w celu omówienia kwestii związanych z reformą ram prawnych UE, a także z potrzebą wypracowania wspólnych standardów ochrony danych na całym świecie[16]. Węgierska i polska prezydencja Rady były gospodarzami dwóch konferencji na temat ochrony danych, które odbyły się, odpowiednio, w dniach 16-17 czerwca 2011 r. i 21 września 2011 r.

Przez cały rok 2011 odbywały się specjalne warsztaty i seminaria. W styczniu ENISA[17] zorganizowała warsztaty na temat zawiadamiania o naruszeniach ochrony danych osobowych w Europie[18]. W lutym Komisja zorganizowała warsztaty z organami państw członkowskich, aby omówić kwestie ochrony danych w obszarze współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych, w tym wdrożenia decyzji ramowej, zaś Agencja Praw Podstawowych przeprowadziła konsultacje z zainteresowanymi stronami na temat „Ochrony danych i prywatności". W dniu 13 lipca 2011 r. odbyła się dyskusja na temat kluczowych aspektów reformy z krajowymi organami ds. ochrony danych. Konsultacje z obywatelami UE przeprowadzono za pośrednictwem kwestionariusza Eurobarometru w listopadzie-grudniu 2010 r.[19]. Zainicjowano również szereg analiz[20]. „Grupa Robocza Art.

---

12 http://ec.europa.eu/justice/newsroom/data-protection/events/090519_en.htm.

13 Z opiniami niezaklasyfikowanymi jako poufne można się zapoznać na stronie internetowej Komisji. http://ec.europa.eu/justice/newsroom/data-protection/opinion/090709_en.htm.

14 Z opiniami niezaklasyfikowanymi jako poufne można się zapoznać na stronie internetowej Komisji. http://ec.europa.eu/justice/newsroom/data-protection/opinion/101104_en.htm.

15 http://ec.europa.eu/justice/newsroom/data-protection/events/100701_en.htm.

16 http://www.coe.int/t/dghl/standardsetting/dataprotection/Data_protection_day2011_en.asp.

17 Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji, zajmująca się kwestiami bezpieczeństwa związanego z sieciami łączności i systemami informacyjnymi.

18 Zob. http://www.enisa.europa.eu/act/it/data-breach-notification/.

19 Specjalna ankieta Eurobarometru (EB) nr 359 „Ochrona danych i tożsamość elektroniczna w UE (2011: http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf.

20 Zob. „Analiza korzyści ekonomicznych z technologii zwiększających ochronę prywatności" oraz *Comparative study on different approaches to new privacy challenges, in particular in the light of*

29”[21] przedstawiła wiele opinii i wniosła cenny wkład w prace Komisji[22]. Również Europejski Inspektor Ochrony Danych wydał kompleksową opinię na temat zagadnień poruszonych w komunikacie Komisji z listopada 2010 r.[23].

Parlament Europejski zatwierdził swoją rezolucją z dnia 6 lipca 2011 r. sprawozdanie, w którym poparł podejście Komisji do reformy ram ochrony danych[24]. Rada Unii Europejskiej przyjęła w dniu 24 lutego 2011 r. konkluzje, w których wyraziła ogólne poparcie dla zamiaru zreformowania przez Komisję ram ochrony danych oraz zgodziła się na wiele elementów składających się na podejście Komisji. Również Europejski Komitet Ekonomiczno-Społeczny poparł cel Komisji, by zagwarantować spójniejsze stosowanie unijnych przepisów dotyczących ochrony danych[25] we wszystkich państwach członkowskich oraz odpowiednią rewizję dyrektywy 95/46/WE[26].

W czasie konsultacji w sprawie kompleksowego podejścia znaczna większość zainteresowanych stron zgodziła się, że ogólne zasady zachowują ważność, lecz istnieje potrzeba dostosowania obecnych ram, by móc lepiej reagować na wyzwania stawiane przez szybki rozwój nowych technologii (zwłaszcza internetu) i postępującą globalizację, przy jednoczesnym zachowaniu technologicznej neutralności ram prawnych. Ostre słowa krytyki na temat obecnego rozdrobnienia ochrony danych osobowych w Unii padły w szczególności ze strony zainteresowanych podmiotów gospodarczych, które apelowały o większą pewność prawną i ujednolicenie przepisów na temat ochrony danych osobowych. Złożoność przepisów dotyczących międzynarodowego przekazywania danych osobowych jest uważaną za istotną przeszkodę w prowadzonej przez te podmioty działalności, gdyż muszą one systematycznie przekazywać dane osobowe z UE do innych części świata.

Zgodnie ze swoją polityką dążenia do lepszych uregulowań prawnych Komisja przeprowadziła ocenę skutków innych możliwych wariantów politycznych. Ocena skutków została oparta na trzech celach polityki zakładających poprawę wymiaru ochrony danych związanego z rynkiem wewnętrznym, zapewnienie osobom fizycznym możliwości skuteczniejszego egzekwowania prawa do ochrony danych oraz stworzenie całościowych,

---

technological developments, styczeń 2010 r. (http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf)..

21 Grupa robocza została ustanowiona w 1996 r. (poprzez art. 29 dyrektywy 95/46/WE) jako organ o charakterze doradczym, złożony z przedstawicieli krajowych organów nadzorujących ochronę danych, Europejskiego Inspektora Ochrony Danych oraz Komisji. Bliższe informacje dostępne są na następującej stronie: http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm..

22 Zob. w szczególności następujące opinie: w sprawie „Przyszłości prywatności” (2009 r. WP 168), w sprawie pojęcia „administratora” i „podmiotu przetwarzającego” (1/2010, WP 169); w sprawie internetowej reklamy behawioralnej (2/2010, WP 171); w sprawie zasady rozliczalności (3/2010, WP 173); w sprawie prawa właściwego (8/2010, WP 179) oraz w sprawie zgody (15/2011, WP 187). Na wniosek Komisji przyjęła także trzy poniższe stanowiska doradcze: w sprawie zawiadomień, w sprawie danych wrażliwych oraz w sprawie praktycznego wdrożenia art. 28 ust. 6 dyrektywy w sprawie ochrony danych. Są one dostępne na następującej stronie: http://ec.europa.eu/justice/data-protection/article-29/documentation/index_en.htm

23 Dostępna na stronie internetowej Europejskiego Inspektora Ochrony Danych: http://www.edps.europa.eu/EDPSWEB/.

24 Rezolucja PE z dnia 6 lipca 2011 r. w sprawie całościowego podejścia do kwestii ochrony danych osobowych w Unii Europejskiej (2011/2025(INI)) http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2011-0323+0+DOC+XML+V0//PL (sprawozdawca: poseł Axel Voss (EPP/DE)).

25 SEC(2012)72.

26 CESE 999/2011

spójnych ram obejmujących wszystkie obszary właściwości Unii, w tym współpracę policyjną i współpracę wymiarów sprawiedliwości w sprawach karnych. Oceniono trzy warianty polityki wiążące się z różnym stopniem interwencji: wariant pierwszy polegał na minimalnych zmianach legislacyjnych i korzystaniu z komunikatów zawierających wykładnię oraz środków wsparcia realizacji polityki, takich jak programy finansowania i narzędzia techniczne; wariant drugi obejmował szereg przepisów legislacyjnych dotyczących każdej z kwestii zidentyfikowanej w trakcie analizy, zaś wariant trzeci zakładał centralizację ochrony danych na szczeblu UE poprzez precyzyjne i szczegółowe przepisy dla wszystkich sektorów oraz ustanowienie agencji UE ds. monitorowania i egzekwowania wykonania przepisów.

Zgodnie z ustaloną metodologią Komisji i przy pomocy grupy sterującej złożonej z przedstawicieli różnych służb oceniono każdy wariant polityki pod kątem skuteczności w realizacji celów polityki, jego oddziaływania na zainteresowane podmioty (w tym na budżet instytucji UE), jego oddziaływania społecznego i wpływu na prawa podstawowe. Nie ustalono żadnego wpływu na środowisko naturalne. Analiza ogólnego wpływu doprowadziła do opracowania preferowanego wariantu polityki, który opiera się na drugim wariancie z pewnymi elementami pochodzącymi z dwóch pozostałych wariantów i który został włączony do obecnego wniosku. Zgodnie z oceną skutków jego wdrażanie doprowadzi między innymi do znacznej poprawy, jeżeli chodzi o pewność prawa dla administratorów i obywateli, zmniejszenie ciężaru administracyjnego, spójność egzekwowania ochrony danych w Unii, faktyczną możliwość skuteczniejszego egzekwowania prawa do ochrony danych osobowych na terytorium UE przez osoby fizyczne oraz skuteczny nadzór nad ochroną danych i egzekwowanie stosownych przepisów. Wdrożenie preferowanych wariantów polityki ma także przyczynić się do realizacji celu Komisji polegającego na uproszczeniu i zmniejszeniu obciążenia administracyjnego oraz celów Europejskiej agendy cyfrowej, planu działania służącego realizacji programu sztokholmskiego oraz strategii „Europa 2020”.

Rada ds. Ocen Skutków przedstawiła opinię na temat projektu oceny skutków w dniu 9 września 2011 r. Po wydaniu opinii przez Radę w ocenie skutków wprowadzono w szczególności następujące zmiany:

– wyjaśniono cele obecnych ram prawnych (w jakim zakresie zostały one osiągnięte, a w jakim nie), jak również cele zamierzonej reformy;

– dodano więcej argumentów i dodatkowe wyjaśnienia do części opisującej problemy;

– dodano sekcję dotyczącą proporcjonalności;

– dokonano całościowego przeglądu i rewizji wszystkich obliczeń i szacunków dotyczących obciążenia administracyjnego w scenariuszu bazowym i w wariancie preferowanym oraz wyjaśniono relację między kosztami zawiadomień a całkowitymi kosztami rozdrobnienia (w tym załącznika 10);

– doprecyzowano wpływ na mikroprzedsiębiorców oraz małych i średnich przedsiębiorców, zwłaszcza wpływ obowiązku wyznaczania inspektorów ochrony danych oraz przeprowadzania ocen skutków ochrony danych.

Razem z wnioskami publikuje się sprawozdanie z oceny skutków oraz streszczenie.

3. ASPEKTY PRAWNE WNIOSKU

3.1. Podstawa prawna

Niniejszy wniosek oparty jest na art. 16 TFUE będącym nową podstawą prawną przyjmowania przepisów o ochronie danych, wprowadzoną traktatem lizbońskim. Postanowienie to umożliwia przyjmowanie przepisów dotyczących ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez państwa członkowskie w wykonywaniu działań wchodzących w zakres zastosowania prawa Unii. Umożliwia ono także przyjmowanie przepisów dotyczących swobodnego przepływu danych osobowych, w tym danych osobowych przetwarzanych przez państwa członkowskie lub podmioty prywatne.

Rozporządzenie uważa się za najbardziej odpowiedni instrument prawny służący do zdefiniowania ram ochrony danych osobowych w Unii. Bezpośrednie stosowanie rozporządzenia zgodnie z art. 288 TFUE zmniejszy rozdrobnienie prawne i zapewni większą pewność prawa poprzez wprowadzenie ujednoliconego zestawu podstawowych przepisów, zwiększając w ten sposób ochronę praw podstawowych osób fizycznych i przyczyniając się do funkcjonowania rynku wewnętrznego.

Odesłanie do art. 114 ust. 1 TFUE jest niezbędne wyłącznie ze względu na zmianę dyrektywy 2002/58/WE w zakresie, w jakim dyrektywa ta również przewiduje ochronę słusznych interesów abonentów będących osobami prawnymi.

3.2. Pomocniczość i proporcjonalność

Zgodnie z zasadą pomocniczości (art. 5 ust. 3 TFUE), Unia podejmuje działania tylko wówczas, gdy cele zamierzonego działania nie mogą zostać osiągnięte w sposób wystarczający przez państwa członkowskie i jeśli ze względu na rozmiary lub skutki proponowanego działania możliwe jest lepsze ich osiągnięcie na poziomie Unii. W świetle problemów zarysowanych powyżej, analiza pod kątem pomocniczości wskazuje na potrzebę działania na szczeblu UE na podstawie następujących przesłanek:

– prawo do ochrony danych osobowych zapisane w art. 8 Karty praw podstawowych wymaga tego samego poziomu ochrony danych w całej Unii; brak wspólnych przepisów UE wiązałby się z ryzykiem istnienia różnych poziomów ochrony w państwach członkowskich oraz wystąpienia ograniczeń w transgranicznym przepływie danych osobowych między państwami członkowskimi mającymi różne standardy;

– dane osobowe przekazywane są ponad granicami, zarówno wewnętrznymi, jak i zewnętrznymi, w coraz szybszym tempie; obok tego istnieją praktyczne wyzwania w zakresie egzekwowania przepisów o ochronie danych, zachodzi również konieczność współpracy między państwami członkowskimi i ich organami, którą należy zorganizować na szczeblu UE, by zagwarantować jednolite stosowanie prawa UE. UE jest również najlepiej predysponowana, by zagwarantować skutecznie i konsekwentnie ten sam poziom ochrony osób fizycznych w zakresie danych osobowych przekazywanych do państw trzecich;

– państwa członkowskie nie mogą same ograniczyć problemów w obecnej sytuacji, zwłaszcza w obliczu rozdrobnienia w krajowych przepisach. Istnieje zatem szczególna potrzeba ustanowienia zharmonizowanych, spójnych ram umożliwiających sprawne

przekazanie danych osobowych ponad granicami na terytorium UE, przy równoczesnym zagwarantowaniu skutecznej ochrony dla wszystkich osób fizycznych w całej UE;

– proponowane działania legislacyjne UE będą bardziej skuteczne niż podobne działania na szczeblu państw członkowskich, ze względu na charakter i skalę problemów, które nie ograniczają się do szczebla jednego czy kilku państw członkowskich.

Zasada proporcjonalności wymaga, by każda interwencja była ukierunkowana i nie wykraczała poza to, co jest konieczne dla osiągnięcia celów. Zasadą tą kierowano się opracowywaniu niniejszego wniosku, począwszy od określenia i oceny innych możliwych wariantów polityki, aż po sporządzenie wniosku ustawodawczego.

3.3. Podsumowanie zagadnień praw podstawowych

Prawo do ochrony danych osobowych ustanowione jest art. 8 karty oraz art. 16 TFUE, jak również art. 8 EKPC. Jak podkreślił Trybunał Sprawiedliwości UE[27], prawo do ochrony danych osobowych nie jest prawem absolutnym i powinno być analizowane w kontekście funkcji, jaką pełni w społeczeństwie[28]. Ochrona danych jest ściśle powiązana z poszanowaniem życia prywatnego i rodzinnego chronionego na podstawie art. 7 karty. Znajduje to odzwierciedlenie w art. 1 ust. 1 dyrektywy 95/46/WE, który przewiduje, że państwa członkowskie chronią podstawowe prawa i wolności osób fizycznych, a w szczególności ich prawo do prywatności w kontekście przetwarzania danych osobowych.

Inne prawa podstawowe zapisane w karcie, na które wniosek może potencjalnie mieć wpływ, to: wolność wypowiedzi (art. 11 karty); wolność działalności gospodarczej (art. 16); prawo własności, w szczególności ochrona własności przemysłowej (art. 17 ust. 2); zakaz dyskryminacji innych osób ze względu na takie czynniki jak: rasa, pochodzenie etniczne, cechy genetyczne, religia lub przekonania, poglądy polityczne lub wszelkie inne poglądy, niepełnosprawność lub orientacja seksualna (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).

3.4. Szczegółowe wyjaśnienie wniosku

3.4.1. ROZDZIAŁ I – PRZEPISY OGÓLNE

Artykuł 1 definiuje zakres przedmiotowy rozporządzenia oraz, jak wskazano w art. 1 dyrektywy 95/46/WE, określa dwa cele rozporządzenia.

Artykuł 2 określa zakres materialny rozporządzenia.

Artykuł 3 określa zakres terytorialny rozporządzenia.

Artykuł 4 zawiera definicje terminów użytych w rozporządzeniu. Podczas gdy część definicji przejęto z dyrektywy 95/46/WE, inne zostały zmienione, uzupełnione o dodatkowe elementy

---

[27] Trybunał Sprawiedliwości UE, wyrok z dnia 9.11.2010 r.; sprawy połączone C-92/09 i C-93/09 Volker und Markus Schecke oraz Eifert [2010] Zb.Orz. I-0000.

[28] 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, zastrzeżeniem zasady proporcjonalności, są one konieczne i rzeczywiście odpowiadają celom interesu ogólnego uznawanym przez Unię Europejską lub potrzebom ochrony praw i wolności innych osób.

lub na nowo wprowadzone („naruszenie ochrony danych osobowych” w oparciu o art. 2 lit. h) dyrektywy o e-prywatności 2002/58/WE[29] zmienionej dyrektywą 2009/136/WE[30], „dane genetyczne”, „dane biometryczne”, „dane dotyczące zdrowia”, „główna siedziba”, „przedstawiciel”, „przedsiębiorstwo”, „grupa przedsiębiorstw”, „wiążące reguły korporacyjne”, definicja „dziecka” w oparciu o Konwencję Organizacji Narodów Zjednoczonych o prawach dziecka[31] oraz „organu nadzorczego”).

W definicji zgody dodano kryterium „wyraźna”, by uniknąć mylnego odniesienia do zgody „jednoznacznej” oraz by wprowadzić jednolitą i spójną definicję zgody, gwarantując w ten sposób, że podmiot danych będzie świadomy tego, że wyraża zgodę oraz na co wyraża zgodę.

3.4.2. ROZDZIAŁ II – ZASADY

Artykuł 5 określa zasady dotyczące przetwarzania danych osobowych, które odpowiadają zasadom wskazanym w art. 6 dyrektywy 95/46/WE. Do nowych, dodatkowych elementów należą w szczególności zasada przejrzystości, wyjaśnienie zasady minimalizacji danych oraz ustalenie zasad ponoszenia całkowitej odpowiedzialności przez administratora.

Artykuł 6 określa, na podstawie art. 7 dyrektywy 95/46/WE, kryteria zgodnego z prawem przetwarzania danych, które zostały doprecyzowane, jeśli chodzi o kryterium równowagi interesów, zgodność ze zobowiązaniami prawnymi oraz interes publiczny.

Artykuł 7 wyjaśnia warunki, które muszą być spełnione, by zgoda stanowiła ważną podstawę prawną zgodnego z prawem przetwarzania danych.

Artykuł 8 określa dalsze warunki zgodności z prawem przetwarzania danych osobowych dzieci w odniesieniu do usług społeczeństwa informacyjnego oferowanych im bezpośrednio.

W art. 9 wyrażono ogólny zakaz przetwarzania szczególnych kategorii danych osobowych oraz przedstawiono wyjątki od tej zasady ogólnej w oparciu o art. 8 dyrektywy 95/46/EW.

Artykuł 10 precyzuje, że administrator nie ma obowiązku uzyskania dodatkowych informacji w celu identyfikacji podmiotu danych jedynie po to, by zapewnić zgodność z przepisami niniejszego rozporządzenia.

---

29 Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej), Dz.U. L 201 z 31.7.2002, s. 37.

30 Dyrektywa Parlamentu Europejskiego i Rady 2009/136/WE z dnia 25 listopada 2009 r. zmieniająca dyrektywę 2002/22/WE w sprawie usługi powszechnej i związanych z sieciami i usługami łączności elektronicznej praw użytkowników, dyrektywę 2002/58/WE dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej oraz rozporządzenie (WE) nr 2006/2004 w sprawie współpracy między organami krajowymi odpowiedzialnymi za egzekwowanie przepisów prawa w zakresie ochrony konsumentów. Tekst mający znaczenie dla EOG, Dz.U. L 337 z 18.12.2009, s. 11.

31 Przyjęta i otwarta do podpisu, ratyfikacji i przystąpienia w rezolucji Zgromadzenia Ogólnego Organizacji Narodów Zjednoczonych nr 44/25 z dnia 20.11.1989 r.

3.4.3. ROZDZIAŁ III – PRAWA PODMIOTU DANYCH

3.4.3.1. Sekcja 1 – Przejrzystość oraz tryby wykonywania praw

Artykuł 11 nakłada na administratorów obowiązek podawania przejrzystych oraz łatwo dostępnych i zrozumiałych informacji, zainspirowany w szczególności rezolucją madrycką w sprawie międzynarodowych standardów ochrony danych osobowych i prywatności[32].

Artykuł 12 zobowiązuje administratora do zapewnienia procedur i mechanizmów ułatwiających podmiotowi danych wykonywanie przysługujących mu praw, w tym sposobów umożliwiających składanie wniosków drogą elektroniczną i żądanie uzyskania odpowiedzi na wniosek podmiotu danych w określonym terminie, a także do uzasadnienia odmowy udzielenia odpowiedzi.

Artykuł 13 przedstawia prawa przysługujące odbiorcom, opracowane na podstawie art. 12 lit. c) dyrektywy 95/46/WE, rozszerzone na wszystkich odbiorców, w tym współadministratorów i podmioty przetwarzające.

3.4.3.2. Sekcja 2 – Informacje i dostęp do danych

Artykuł 14 doprecyzowuje obowiązki informacyjne administratora wobec podmiotu danych, na podstawie art. 10 i 11 dyrektywy 95/46/WE, obejmujące obowiązek przekazywania podmiotowi danych dodatkowych informacji, w tym na temat okresu przechowywania i prawa do składania skarg, w odniesieniu do międzynarodowego przekazywania danych oraz źródła pochodzenia danych. W artykule tym utrzymano ponadto możliwe odstępstwa przewidziane w dyrektywie 95/46/WE, np. obowiązek taki nie wystąpi wówczas, gdy rejestracja lub ujawnianie są wyraźnie przewidziane przez prawo. Mogłoby to na przykład dotyczyć postępowań prowadzonych przez organy ds. konkurencji, organy podatkowe lub administrację celną lub przez służby odpowiedzialne za sprawy ubezpieczeń społecznych.

Artykuł 15 przedstawia prawo dostępu podmiotu danych do jego danych osobowych, w oparciu o art. 12 lit. a) dyrektywy 95/46/WE. Dodano do niego nowe elementy, takie jak informowanie podmiotów danych o okresie przechowywania, prawach do poprawiania i do usuwania danych oraz zgłaszania skarg.

3.4.3.3. Sekcja 3 – Poprawianie i usuwanie

Artykuł 16 określa prawo podmiotu danych do poprawienia danych w oparciu o art. 12 lit. b) dyrektywy 95/46/WE.

Artykuł 17 przedstawia prawo podmiotu danych do bycia zapomnianym i do usunięcia danych. Rozwija ponadto i doprecyzowuje prawo do usunięcia danych przewidziane w art. 12 lit. b) dyrektywy 95/46/WE oraz wymienia warunki wykonania prawa do bycia zapomnianym, w tym obowiązek administratora, który podał dane osobowe do wiadomości publicznej, poinformowania osób trzecich o wniosku podmiotu danych dotyczącym usunięcia wszelkich linków do danych, kopii lub replikacji tych danych osobowych. W artykule tym

---

[32] Przyjęta przez Międzynarodową Konferencję Rzeczników Ochrony Danych Osobowych i Prywatności w dniu 5 listopada 2009 r. Por. także art. 13 ust. 3 wniosku dotyczącego rozporządzenia w sprawie wspólnych europejskich przepisów dotyczących sprzedaży (COM(2011) 635 wersja ostateczna).

przewidziano także prawo do ograniczenia przetwarzania w niektórych przypadkach, unikając w ten sposób dwuznacznego terminu „blokowanie”.

Artykuł 18 wprowadza prawo podmiotu danych do przenoszenia danych, tj. do przenoszenia ich z jednego elektronicznego systemu przetwarzania do innego, któremu administrator nie może zapobiec. Przepis ten przewiduje, jako warunek konieczny i w celu jeszcze większego ułatwienia osobom fizycznym dostępu do ich danych osobowych, prawo do uzyskania od administratora tych danych w zorganizowanym i powszechnie stosowanym formacie elektronicznym.

3.4.3.4. Sekcja 4 – Prawo wniesienia sprzeciwu i profilowanie

Artykuł 19 przyznaje podmiotowi danych prawo wniesienia sprzeciwu. Opiera się on na art. 14 dyrektywy 95/46/WE, z pewnymi zmianami, w tym jeśli chodzi o ciężar dowodu i jego zastosowanie do marketingu bezpośredniego.

Artykuł 20 dotyczy prawa podmiotu danych do niepodlegania środkowi opartemu na profilowaniu. Opiera się on, ze zmianami i dodatkowymi gwarancjami, na art. 15 ust. 1 dyrektywy 95/46/WE dotyczącym zautomatyzowanych decyzji indywidualnych, i uwzględnia zalecenie Rady Europy w sprawie profilowania[33].

3.4.3.5. Sekcja 5 – Ograniczenia

Artykuł 21 wyjaśnia upoważnienie Unii lub państw członkowskich do utrzymania lub wprowadzenia ograniczeń dotyczących zasad określonych w art. 5 oraz praw podmiotów danych, wymienionych w art. 11-20 oraz art. 32. Przepis ten opiera się na art. 13 dyrektywy 95/46/WE oraz na wymaganiach wynikających z Karty praw podstawowych oraz Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności, zgodnie z wykładnią Trybunału Sprawiedliwości UE i Europejskiego Trybunału Praw Człowieka.

3.4.4. ROZDZIAŁ IV – ADMINISTRATOR I PODMIOT PRZETWARZAJĄCY

3.4.4.1. Sekcja 1 – Obowiązki ogólne

Artykuł 22 uwzględnia wnioski z dyskusji na temat „zasady odpowiedzialności” i szczegółowo opisuje obowiązek przestrzegania przez administratora przepisów niniejszego rozporządzenia oraz wykazywania takiej zgodności, w tym poprzez przyjmowanie służących temu wewnętrznych polityk i mechanizmów.

Artykuł 23 przedstawia obowiązki administratora wynikające z zasad uwzględnienia ochrony danych już w fazie projektowania oraz ochrony danych jako opcji domyślnej.

Artykuł 24 w sprawie współadministratorów wyjaśnia kompetencje współadministratorów, jeśli chodzi o ich stosunki wewnętrzne oraz wobec podmiotu danych.

Artykuł 25 zobowiązuje, pod pewnymi warunkami, administratorów niemających siedziby w Unii, o ile rozporządzenie dotyczy ich działalności w zakresie przetwarzania, do wyznaczenia przedstawiciela w Unii.

---

33 CM/Rec (2010)13

Artykuł 26 wyjaśnia status i obowiązki podmiotów przetwarzających, częściowo na podstawie art. 17 ust. 2 dyrektywy 95/46/WE, dodając do niego nowe elementy, między innymi taki, że podmiot przetwarzający, który przetwarza dane w zakresie przekraczającym zalecenia administratora, należy uznać za współadministratora.

Artykuł 27 dotyczący przetwarzania z upoważnienia administratora i podmiotu przetwarzającego opiera się na art. 16 dyrektywy 95/46/WE.

Artykuł 28 wprowadza dla administratorów i podmiotów przetwarzających obowiązek prowadzenia dokumentacji dotyczącej operacji przetwarzania podlegających ich odpowiedzialności, zamiast ogólnego zawiadomienia przekazywanego organowi nadzorczemu, o którym mowa w art. 18 ust. 1 i art. 19 dyrektywy 95/46/WE.

Artykuł 29 wyjaśnia obowiązki administratora i podmiotu przetwarzającego w zakresie współpracy z organem nadzorczym.

3.4.4.2. Sekcja 2 – Bezpieczeństwo danych

Artykuł 30 zobowiązuje administratora i podmiot przetwarzający do wprowadzenia odpowiednich środków mających na celu zapewnienie bezpieczeństwa przetwarzania, na podstawie art. 17 ust. 1 dyrektywy 95/46/WE, rozszerzając ten obowiązek na podmioty przetwarzające, niezależnie od warunków umowy zawartej z administratorem.

Artykuły 31 i 32 wprowadzają obowiązek zawiadomienia o naruszeniu ochrony danych osobowych, w oparciu o obowiązek zawiadomienia o naruszeniu danych osobowych przewidziany w art. 4 ust. 3 dyrektywy o e-prywatności 2002/58/WE.

3.4.4.3. Sekcja 3 – Ocena skutków w zakresie ochrony danych i uprzednie zezwolenie

Artykuł 33 wprowadza obowiązek przeprowadzania przez administratorów i podmioty przetwarzające oceny skutków w zakresie ochrony danych przed podjęciem ryzykownych operacji przetwarzania.

Artykuł 34 dotyczy przypadków, w których zezwolenie organu nadzorczego oraz zasięgnięcie jego opinii są obowiązkowe przed przystąpieniem do przetwarzania, w oparciu o koncepcję kontroli wstępnej, o której mowa w art. 20 dyrektywy 95/46/WE.

3.4.4.4. Sekcja 4 – Inspektor ochrony danych

Artykuł 35 wprowadza obowiązek powołania inspektora ochrony danych dla sektora publicznego oraz, w sektorze prywatnym, dla dużych przedsiębiorstw lub tam, gdzie główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które wymagają regularnego i systematycznego monitorowania. Artykuł ten opiera się na art. 18 ust. 2 dyrektywy 95/46/WE, który przewidywał możliwość wprowadzenia przez państwo członkowskie takiego wymogu w ramach zastąpienia ogólnego obowiązku zawiadomienia.

Artykuł 36 określa status inspektora ochrony danych.

Artykuł 37 opisuje główne zadania inspektora ochrony danych.

3.4.4.5. Sekcja 5 – Kodeksy postępowania i certyfikacja

Artykuł 38 dotyczy kodeksów postępowania, w oparciu o pojęcie wprowadzone w art. 27 ust. 1 dyrektywy 95/46/WE, i wyjaśnia treść tych kodeksów i procedur oraz przewiduje uprawnienie Komisji do podejmowania decyzji w sprawie ogólnego obowiązywania kodeksów postępowania.

Artykuł 39 wprowadza możliwość ustanawiania mechanizmów certyfikacji oraz pieczęci i oznaczeń w zakresie ochrony danych.

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

Artykuł 40 ustanawia zasadę ogólną, według której zgodność z obowiązkami określonymi w tym rozdziale jest obligatoryjna w przypadku przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych, w tym wtórnego przekazywania danych.

Artykuł 41 określa kryteria, warunki i procedury przyjmowania przez Komisję decyzji stwierdzającej odpowiedni poziom ochrony w oparciu o art. 25 dyrektywy 95/46/WE. Kryteria, które zostaną uwzględnione w ocenie odpowiedniego stopnia ochrony, w sposób wyraźny obejmują praworządność, sądowe środki ochrony prawnej oraz niezależny nadzór. Artykuł ten wyraźnie potwierdza możliwość dokonywania przez Komisję oceny poziomu ochrony zapewnianego na terytorium państwa trzeciego lub w określonym sektorze w tym państwie, w którym odbywa się przetwarzanie.

Artykuł 42 wymaga, by w przypadku przekazywania danych do państw trzecich, gdy Komisja nie podjęła decyzji stwierdzającej odpowiedni poziom ochrony, wprowadzono odpowiednie gwarancje, w szczególności standardowe klauzule ochrony danych, wiążące reguły korporacyjne oraz klauzule umowne. Możliwość wykorzystania standardowych klauzul ochrony danych stosowanych przez Komisję opiera się na art. 26 ust. 4 dyrektywy 95/46/WE. Nowością jest, że takie standardowe klauzule ochrony danych mogą obecnie być przyjmowane także przez organ nadzorczy i uznawane przez Komisję za ogólnie obowiązujące. Wiążące reguły korporacyjne zostały obecnie wyraźnie wymienione w tekście prawnym. Wariant klauzul umownych daje administratorowi lub podmiotowi przetwarzającemu pewną elastyczność, lecz podlega obowiązkowi uzyskania uprzedniego zezwolenia organu nadzorczego.

Artykuł 43 szczegółowo opisuje warunki przekazywania na podstawie wiążących reguł korporacyjnych, w oparciu o obecnie stosowane praktyki i wymogi organów nadzorczych.

Artykuł 44 przedstawia i wyjaśnia odstępstwa dotyczące przekazywania danych, w oparciu o obowiązujące przepisy art. 26 dyrektywy 95/46/WE. Dotyczą one w szczególności przekazywania danych wymaganego i niezbędnego do ochrony istotnego interesu publicznego, na przykład w sytuacji międzynarodowego przekazywania danych między organami ds. konkurencji, władzami podatkowymi lub administracją celną bądź między służbami odpowiedzialnymi za sprawy ubezpieczeń społecznych lub zarządzanie rybołówstwem. Ponadto przekazywanie danych może, w niektórych okolicznościach, być usprawiedliwione ze względu na słuszny interes administratora lub podmiotu przetwarzającego, lecz wyłącznie po dokonaniu oceny i udokumentowaniu okoliczności takiej operacji przekazania.

Artykuł 45 wyraźnie przewiduje mechanizmy współpracy międzynarodowej na rzecz ochrony danych osobowych między Komisją a organami nadzorczymi państw trzecich, w szczególności takimi, które uważane są za zapewniające odpowiedni poziom ochrony, z uwzględnieniem zalecenia Organizacji Współpracy Gospodarczej i Rozwoju (OECD) w sprawie transgranicznej współpracy w zakresie egzekwowania przepisów chroniących prawo do prywatności z dnia 12 czerwca 2007 r.

3.4.6. ROZDZIAŁ VI – NIEZALEŻNE ORGANY NADZORCZE

3.4.6.1. Sekcja 1 – Niezależny status

Artykuł 46 zobowiązuje państwa członkowskie, na podstawie art. 28 ust. 1 dyrektywy 95/46/WE, do ustanowienia organów nadzorczych, rozszerzając zakres powierzonych im zadań o wzajemną współpracę i współpracę z Komisją.

Artykuł 47 wyjaśnia warunki niezależności organów nadzorczych, co stanowi realizację orzeczeń Trybunału Sprawiedliwości Unii Europejskiej[34], i zostało także zainspirowane art. 44 rozporządzenia (WE) nr 45/2001[35].

Artykuł 48 określa ogólne warunki członkostwa w organie nadzorczym, co stanowi realizację odpowiednich orzeczeń[36], i zostało także zainspirowane art. 42 ust. 2-6 rozporządzenia (WE) 45/2001.

Artykuł 49 podaje zasady dotyczące ustanowienia organu nadzorczego, które mają określać przepisy państw członkowskich.

Artykuł 50 dotyczy tajemnicy służbowej obowiązującej członków i personel organu nadzorczego na podstawie art. 28 ust. 7 dyrektywy 95/46/WE.

3.4.6.2. Sekcja 2 – Obowiązki i uprawnienia

Artykuł 51 określa kompetencje organów nadzorczych. Zasadę ogólną, opartą na art. 28 ust. 6 dyrektywy 95/46/WE (kompetencje na terytorium własnego państwa członkowskiego), uzupełnia nowa kompetencja organu głównego w przypadku, gdy administrator lub podmiot przetwarzający mają siedzibę w kilku państwach członkowskich, co ma zapewnić jednolitość stosowania („punkt kompleksowej obsługi”). Sądy, w zakresie sprawowanych funkcji sądowniczych, są zwolnione z kontroli organu nadzorczego, lecz nie są zwolnione ze stosowania materialnych przepisów dotyczących ochrony danych.

Artykuł 52 określa obowiązki organu nadzorczego, w tym dotyczące rozpatrywania skarg i prowadzenia postępowań w ich sprawie oraz szerzenia w społeczeństwie wiedzy na temat ryzyka, przepisów, gwarancji i praw.

---

[34] Trybunał Sprawiedliwości UE, wyrok z 9 marca 2010 r., Komisja przeciwko Niemcom, sprawa C-518/07, Zb.Orz z 2010 r., s. I-1885).

[35] 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.

[36] Op. cit. przypis 34.

Artykuł 53 określa uprawnienia organu nadzorczego, częściowo w oparciu o art. 28 ust. 3 dyrektywy 95/46/WE i art. 47 rozporządzenia (WE) 45/2001, dodając kilka nowych elementów, w tym uprawnienie do nakładania sankcji administracyjnych.

Artykuł 54 nakłada na organy nadzorcze obowiązek sporządzania rocznych sprawozdań z działalności, na podstawie art. 28 ust. 5 dyrektywy 95/46/WE.

3.4.7. ROZDZIAŁ VII – WSPÓŁPRACA I ZGODNOŚĆ

3.4.7.1. Sekcja 1 – Współpraca

Artykuł 55 wprowadza jasne przepisy dotyczące obowiązkowej wzajemnej pomocy, przedstawiając skutki braku zastosowania się do żądania innego organu nadzorczego, na podstawie art. 28 ust. 6 akapit drugi dyrektywy 95/46/WE.

Artykuł 56 wprowadza przepisy dotyczące wspólnych operacji, co zostało zainspirowane art. 17 decyzji Rady 2008/615/WSiSW[37], w tym prawo organów nadzorczych do udziału w takich operacjach.

3.4.7.2. Sekcja 2 – Zgodność

Artykuł 57 wprowadza mechanizm zgodności w celu zapewnienia jednolitości stosowania w odniesieniu do operacji przetwarzania, które mogą dotyczyć podmiotów danych w kilku państwach członkowskich.

Artykuł 58 przedstawia procedury i warunki wydawania opinii przez Europejską Radę Ochrony Danych.

Artykuł 59 dotyczy opinii Komisji w sprawach rozstrzyganych w ramach mechanizmu zgodności, które mogą popierać opinię Europejskiej Rady Ochrony Danych lub różnić się od takiej opinii, a także projektów środków organu nadzorczego. W przypadku podniesienia przez Europejską Radę Ochrony Danych dowolnej kwestii na mocy art. 58 ust. 3 można oczekiwać, że Komisja wykorzysta przysługujące jej uprawnienie i w razie konieczności wyda opinię.

Artykuł 60 dotyczy decyzji Komisji zawierających żądanie, by właściwy organ zawiesił swój projekt środka, jeśli jest to konieczne do zapewnienia właściwego stosowania niniejszego rozporządzenia.

Artykuł 61 przewiduje możliwość przyjęcia środków tymczasowych w trybie pilnym.

Artykuł 62 określa wymogi w zakresie przyjmowania aktów wykonawczych przez Komisję w ramach mechanizmu zgodności.

Artykuł 63 przewiduje obowiązek organu nadzorczego w zakresie egzekwowania środków we wszystkich zainteresowanych państwach członkowskich, a także stanowi, iż stosowanie mechanizmu zgodności jest warunkiem koniecznym ważności prawnej i egzekwowania danego środka.

---

[37] Decyzja Rady 2008/615/WSiSW z dnia 23 czerwca 2008 r. w sprawie intensyfikacji współpracy transgranicznej, szczególnie w zwalczaniu terroryzmu i przestępczości transgranicznej, Dz.U. L 210 z 6.8.2008, s. 1.

3.4.7.3. Sekcja 3 – Europejska Rada Ochrony Danych

Artykuł 64 ustanawia Europejską Radę Ochrony Danych, w której skład wchodzą szefowie organów nadzorczych wszystkich państw członkowskich oraz Europejski Inspektor Ochrony Danych. Europejska Rada Ochrony Danych zastępuje Grupę Roboczą ds. Ochrony Osób Fizycznych w zakresie Przetwarzania Danych Osobowych powołaną na mocy art. 29 dyrektywy 95/46/WE. Wyjaśnia się, że Komisja nie jest członkiem Europejskiej Rady Ochrony Danych, lecz ma prawo uczestniczyć w jej działaniach i być w niej reprezentowana.

Artykuł 65 podkreśla i wyjaśnia niezależność Europejskiej Rady Ochrony Danych.

Artykuł 66 opisuje zadania Europejskiej Rady Ochrony Danych na podstawie art. 30 ust. 1 dyrektywy 95/46/WE i przedstawia elementy dodatkowe, odzwierciedlając w ten sposób szerszy zakres działalności Europejskiej Rady Ochrony Danych w Unii i poza nią. Aby umożliwić lepsze reagowanie w pilnych sytuacjach, daje Komisji możliwość wnioskowania o wydanie opinii w określonym terminie.

Artykuł 67 nakłada na Europejską Radę Ochrony Danych obowiązek sporządzania rocznych sprawozdań z działalności, na podstawie art. 30 ust. 6 dyrektywy 95/46/WE.

Artykuł 68 ustanawia procedury podejmowania decyzji przez Europejską Radę Ochrony Danych, w tym obowiązek przyjęcia regulaminu, który powinien także objąć jej zasady funkcjonowania.

Artykuł 69 zawiera przepisy dotyczące przewodniczącego i wiceprzewodniczących Europejskiej Rady Ochrony Danych.

Artykuł 70 opisuje zadania przewodniczącego.

Artykuł 71 stanowi, że obsługę sekretariatu Europejskiej Rady Ochrony Danych zapewnia Europejski Inspektor Ochrony Danych, a także precyzuje zadania sekretariatu.

Artykuł 72 przedstawia przepisy dotyczące poufności.

3.4.8. ROZDZIAŁ VIII – ŚRODKI OCHRONY PRAWNEJ, ODPOWIEDZIALNOŚĆ I SANKCJE

Artykuł 73 przewiduje prawo każdego podmiotu danych do złożenia skargi do organu nadzorczego, na podstawie art. 28 ust. 4 dyrektywy 95/46/WE. Wymienia on ponadto organy, organizacje lub zrzeszenia, które mogą składać skargi w imieniu podmiotu danych lub, w przypadku naruszenia ochrony danych osobowych, niezależnie od skargi podmiotu danych.

Artykuł 74 dotyczy prawa do skorzystania z sądowego środka ochrony prawnej przeciwko organowi nadzorczemu. Opiera się on na przepisie ogólnym art. 28 ust. 3 dyrektywy 95/46/WE. Artykuł ten ustanawia w szczególności sądowy środek ochrony prawnej zobowiązujący organ nadzorczy do podjęcia działania w odpowiedzi na skargę oraz wyjaśnia kompetencje sądów państwa członkowskiego, w którym organ nadzorczy ma siedzibę. Przewiduje ponadto możliwość wszczęcia przez organ nadzorczy państwa członkowskiego, w którym podmiot danych ma miejsce zamieszkania, postępowania sądowego w imieniu podmiotu danych przed sądami innego państwa członkowskiego, w którym ma siedzibę właściwy organ nadzorczy.

Artykuł 75 dotyczy prawa do sądowego środka ochrony prawnej przeciwko administratorowi lub podmiotowi przetwarzającemu, w oparciu o art. 22 dyrektywy 95/46/WE, i umożliwia skierowanie sprawy do sądu bądź w państwie członkowskim, w którym ma siedzibę pozwany, bądź w tym, w którym ma miejsce zamieszkania podmiot danych. Jeśli postępowanie w ten samej sprawie czeka na rozstrzygnięcie w ramach mechanizmu zgodności, sąd może zawiesić swoje postępowanie, z wyjątkiem sytuacji nadzwyczajnych.

Artykuł 76 przedstawia wspólne zasady postępowań sądowych, w tym prawa organów, organizacji lub zrzeszeń do reprezentowania podmiotów danych przed sądami, prawo organu nadzorczego do udziału w postępowaniach prawnych oraz uzyskiwania przez sądy informacji na temat postępowań prowadzonych równolegle w innym państwie członkowskim, a także możliwość zawieszania przez sądy postępowań w takich przypadkach[38]. Na państwie członkowskim ciąży obowiązek zapewnienia sprawnego przebiegu postępowań sądowych[39].

Artykuł 77 ustanawia prawo do odszkodowania i zasady odpowiedzialności. Opiera się on na art. 23 dyrektywy 95/46/WE, rozszerza to prawo na szkody spowodowane przez podmioty przetwarzające i wyjaśnia zasady odpowiedzialności współadministratorów i podmiotów współprzetwarzających.

Artykuł 78 zobowiązuje państwa członkowskie do ustanowienia przepisów dotyczących kar, nakładania kar za naruszenia rozporządzenia oraz zapewnienia wdrożenia jego przepisów.

Artykuł 79 zobowiązuje każdy organ nadzorczy do nakładania sankcji administracyjnych wymienionych w katalogu zawartym w tym przepisie, w postaci grzywien do kwoty maksymalnej, z należytym uwzględnieniem każdego indywidualnego przypadku.

3.4.9. ROZDZIAŁ IX – PRZEPISY DOTYCZĄCE SZCZEGÓLNYCH SYTUACJI PRZETWARZANIA DANYCH

Artykuł 80 zobowiązuje państwa członkowskie do stosowania wyłączeń i odstępstw od przepisów szczególnych rozporządzenia, o ile jest to konieczne w celu pogodzenia prawa do ochrony danych osobowych z prawem wolności wypowiedzi. Opiera się on na art. 9 dyrektywy 95/46/WE zgodnie z wykładnią Trybunału Sprawiedliwości UE[40].

Artykuł 81 zobowiązuje państwa członkowskie, z zastrzeżeniem warunków dla szczególnych kategorii danych, do zapewnienia konkretnych gwarancji przy przetwarzaniu na potrzeby świadczenia opieki zdrowotnej.

Artykuł 82 przewiduje uprawnienie państw członkowskich do przyjmowania przepisów szczególnych dotyczących przetwarzania danych osobowych w kontekście zatrudnienia.

---

38 Na podstawie art. 5 ust. 1 decyzji ramowej Rady 2009/948/WSiSW z dnia 30 listopada 2009 r. w sprawie zapobiegania konfliktom jurysdykcji w postępowaniu karnym, Dz.U. L 328 z 15.12.2009, s. 42 oraz art. 13 ust. 1 rozporządzenia Rady (WE) nr 1/2003 z dnia 16 grudnia 2002 r. w sprawie wprowadzenia w życie reguł konkurencji ustanowionych w art. 81 i 82 Traktatu, Dz.U. L 1 z 4.1.2003, s. 1.

39 Na podstawie art. 18 ust. 1 dyrektywy 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym), Dz.U. L 178 z 17.7.2000, s. 1.

40 Por. w zakresie interpretacji np. wyrok Trybunału Sprawiedliwości UE z dnia 16 grudnia 2008 r., Satakunnan Markkinapörssi i Satamedia (C-73/07, Zb.Orz. z 2008 r., s. I-9831)

Artykuł 83 określa szczególne warunki przetwarzania danych osobowych do celów dokumentacji, statystyki i badań naukowych.

Artykuł 84 upoważnia państw członkowskie do przyjmowania przepisów szczególnych dotyczących dostępu organów nadzorczych do danych osobowych i pomieszczeń, w których administratorzy podlegają obowiązkowi zachowania tajemnicy.

Artykuł 85 umożliwia, w świetle art. 17 Traktatu o funkcjonowaniu Unii Europejskiej, nieprzerwane stosowanie obowiązujących kompleksowych przepisów dotyczących ochrony danych kościołów, jeśli zostały one ujednolicone z przepisami rozporządzenia.

3.4.10. ROZDZIAŁ X – AKTY DELEGOWANE I AKTY WYKONAWCZE

Artykuł 86 zawiera standardowe przepisy dotyczące wykonywania przekazanych uprawnień zgodnie z art. 290 TFUE. Dzięki temu prawodawca może przekazywać Komisji uprawnienia do przyjęcia aktów o charakterze nieustawodawczym o powszechnym zakresie stosowania, które uzupełniają lub zmieniają niektóre, inne niż zasadnicze, elementy aktu ustawodawczego (akty quasi-ustawodawcze).

Artykuł 87 zawiera przepisy dotyczący procedury komitetowej niezbędnej do powierzenia Komisji uprawnień wykonawczych w przypadkach, gdy zgodnie z art. 291 TFUE konieczne są jednolite warunki wykonywania prawnie wiążących aktów Unii. Zastosowanie ma tu procedura sprawdzająca.

3.4.11. ROZDZIAŁ XI – PRZEPISY KOŃCOWE

Artykuł 88 uchyla dyrektywę 95/46/WE.

Artykuł 89 wyjaśnia stosunek niniejszego rozporządzenia do dyrektywy o e-prywatności 2002/58/WE i wprowadza do niej zmiany.

Artykuł 90 zobowiązuje Komisję do dokonania oceny rozporządzenia i przedstawienia stosownych sprawozdań.

Artykuł 91 określa datę wejścia w życie rozporządzenia oraz okres przejściowy przed datą rozpoczęcia jego stosowania.

4. WPŁYW NA BUDŻET

Konkretny wpływ wniosku na budżet dotyczy zadań powierzonych Europejskiemu Inspektorowi Ochrony Danych, zgodnie z oceną skutków finansowych regulacji towarzyszącą niniejszemu wnioskowi. Wpływ ten wymaga przeprogramowania w ramach działu 5 perspektywy finansowej.

Niniejszy wniosek nie ma wpływu na wydatki operacyjne.

Ocena finansowych skutków regulacji towarzysząca wnioskowi dotyczącemu rozporządzenia obejmuje wpływ na budżet zarówno samego rozporządzenia, jak i dyrektywy o ochronie danych w obszarze policji i wymiaru sprawiedliwości.

2012/0011 (COD)

Wniosek

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY

w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych)

(Tekst mający znaczenie dla EOG)

PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 16 ust. 2 i art. 114 ust. 1,

uwzględniając wniosek Komisji Europejskiej,

po przekazaniu projektu aktu ustawodawczego parlamentom narodowym,

uwzględniając opinię Europejskiego Komitetu Ekonomiczno-Społecznego[41],

po zasięgnięciu opinii Europejskiego Inspektora Ochrony Danych[42],

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą,

a także mając na uwadze, co następuje:

(1) Ochrona osób fizycznych w zakresie przetwarzania danych osobowych jest prawem podstawowym. Artykuł 8 ust. 1 Karty praw podstawowych i art. 16 ust. 1 Traktatu stanowią, iż każda osoba ma prawo do ochrony danych osobowych, które jej dotyczą.

(2) Przetwarzanie danych osobowych ma służyć człowiekowi, zaś zasady i przepisy dotyczące ochrony osób fizycznych w odniesieniu do przetwarzania ich danych osobowych powinny, niezależnie od obywatelstwa czy miejsca stałego zamieszkania osób fizycznych, szanować ich podstawowe prawa i wolności, szczególnie prawo do ochrony danych osobowych. Powinno ono również przyczyniać się do stworzenia obszaru wolności, bezpieczeństwa i sprawiedliwości oraz unii gospodarczej, osiągnięcia postępu gospodarczego i społecznego, wzmocnienia i konwergencji gospodarek na rynku wewnętrznym, a także do poprawy zamożności ludzi.

(3) Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i

---

41 Dz.U. C z [...], s. .

42 Dz.U. C z [...], s. .

swobodnego przepływu tych danych[43] ma na celu harmonizację ochrony podstawowych praw i wolności osób fizycznych w zakresie przetwarzania danych oraz zagwarantowanie swobodnego przepływu danych osobowych między państwami członkowskimi.

(4) Integracja gospodarcza i społeczna będąca wynikiem funkcjonowania rynku wewnętrznego doprowadziła do znacznego zwiększenia transgranicznego przepływu danych osobowych. Zwiększyła się także wymiana danych między podmiotami gospodarczymi i społecznymi oraz publicznymi i prywatnymi w całej Unii. Prawo Unii wymaga, by organy krajowe poszczególnych państw członkowskich współpracowały ze sobą i prowadziły wymianę danych osobowych w celu wykonywania swoich obowiązków lub realizacji zadań w imieniu organów innych państw członkowskich.

(5) Szybki rozwój technologiczny i globalizacja przyniosły nowe wyzwania w zakresie ochrony danych osobowych. Niezwykle wzrosła skala wymiany i zbierania danych. Technologia umożliwia zarówno przedsiębiorcom prywatnym, jak i organom publicznym wykorzystywanie danych osobowych do wykonywania powierzonych im zadań na niespotykaną dotąd skalę. Osoby fizyczne coraz częściej udostępniają informacje osobowe publicznie i globalnie. Technologia całkowicie zmieniła zarówno gospodarkę, jak i życie społeczne, i wymaga dalszego ułatwienia swobodnego przepływu danych w Unii oraz przekazywania ich do państw trzecich i organizacji międzynarodowych, przy równoczesnym zagwarantowaniu wysokiego poziomu ochrony danych osobowych.

(6) Przemiany te wymagają stworzenia stabilnych i bardziej spójnych ram ochrony danych w Unii, popartych zdecydowanym egzekwowaniem, uwzględniając wagę zbudowania zaufania, które umożliwi rozwój gospodarki cyfrowej na rynku wewnętrznym. Osoby fizyczne powinny mieć kontrolę nad własnymi danymi osobowymi. Należy ponadto wzmocnić poczucie pewności prawa i jego praktycznego stosowania u osób fizycznych, podmiotów gospodarczych i organów publicznych.

(7) Cele i zasady dyrektywy 45/96/WE nie zmieniły się, co jednak nie zapobiegło rozdrobnieniu wdrażania przepisów dotyczących ochrony danych w Unii, ugruntowaniu niepewności prawnej oraz upowszechnieniu istniejącego w społeczeństwie poglądu, zgodnie z którym z ochroną osób fizycznych wiążą się istotne zagrożenia, dotyczące w szczególności działalności w internecie. Różnice w zakresie poziomu ochrony praw i wolności osób fizycznych, w szczególności prawa do ochrony danych osobowych, w zakresie przetwarzania danych osobowych, udzielanej w państwach członkowskich mogą uniemożliwić swobodny przepływ danych osobowych w całej Unii. Różnice te mogą zatem stanowić przeszkodę w prowadzeniu działalności gospodarczej na szczeblu Unii, zakłócać konkurencję i utrudniać organom wykonywanie ich obowiązków wynikających z przepisów prawa unijnego. Ta różnica w poziomie ochrony wynika z istnienia różnic we wdrażaniu i stosowaniu dyrektywy 95/46/WE.

(8) Aby zapewnić spójny i wysoki poziom ochrony osób fizycznych oraz usunąć przeszkody w przepływie danych osobowych, należy zapewnić we wszystkich

---

[43] Dz.U. L 281 z 23.11.1995, s. 31.

państwach członkowskich równorzędny poziom ochrony praw i wolności osób fizycznych w zakresie przetwarzania tych danych. Spójne i jednolite stosowanie przepisów dotyczących ochrony podstawowych praw i wolności osób fizycznych w zakresie przetwarzania danych osobowych powinno być zagwarantowane w całej Unii.

(9) Skuteczna ochrona danych osobowych w całej Unii wymaga wzmocnienia i doprecyzowania praw podmiotów danych oraz obowiązków podmiotów, które przetwarzają dane osobowe i kierują tym procesem, lecz także równorzędnych uprawnień w zakresie monitorowania i zapewnienia zgodności z przepisami w zakresie ochrony danych osobowych oraz równorzędnych sankcji wobec osób naruszających te przepisy w państwach członkowskich.

(10) Artykuł 16 ust. 2 Traktatu powierza Parlamentowi Europejskiemu i Radzie ustanowienie przepisów dotyczących ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu takich danych.

(11) W celu zapewnienia spójnego poziomu ochrony osób fizycznych w całej Unii oraz zapobiegania różnicom, które hamowałyby swobodny przepływ danych w ramach rynku wewnętrznego, należy przyjąć rozporządzenie, które zagwarantuje przedsiębiorcom, w tym mikroprzedsiębiorcom oraz małym i średnim przedsiębiorcom pewność prawną i przejrzystość i które zapewni ten sam poziom prawnie egzekwowalnych uprawnień i obowiązków administratorów i podmiotów przetwarzających osobom fizycznym we wszystkich państwach członkowskich, umożliwi spójne monitorowanie przetwarzania danych osobowych, stosowanie równoważnych sankcji we wszystkich państwach członkowskich oraz skuteczną współpracę organów nadzorczych różnych państw członkowskich. W związku ze szczególną sytuacją mikroprzedsiębiorców oraz małych i średnich przedsiębiorców niniejsze rozporządzenia przewiduje szereg odstępstw. Ponadto zachęca się instytucje i organy Unii, państwa członkowskie i ich organy nadzorcze, by wzięły pod uwagę szczególne potrzeby mikroprzedsiębiorców oraz małych i średnich przedsiębiorców, jeśli chodzi o zastosowanie niniejszego rozporządzenia. Pojęcie mikroprzedsiębiorców oraz małych i średnich przedsiębiorców powinno opierać się na zaleceniu Komisji 2003/361/WE z dnia 6 maja 2003 r. dotyczącym przedsiębiorstw mikro, małych i średnich.

(12) Ochrona zapewniona na mocy niniejszego rozporządzenia dotyczy osób fizycznych, niezależnie od ich obywatelstwa lub miejsca zamieszkania, w zakresie przetwarzania danych osobowych. Jeśli chodzi o przetwarzanie danych, które dotyczą osób prawnych, w szczególności przedsiębiorstw będących osobami prawnymi, w tym danych dotyczących firmy, formy prawnej i danych kontaktowych osoby prawnej, nie podlegają one ochronie udzielanej na mocy niniejszego rozporządzenia. Przepis ten powinien mieć także zastosowanie wtedy, gdy firma osoby prawnej obejmuje nazwisko jednej lub większej liczby osób fizycznych.

(13) Ochrona osób fizycznych powinna być technologicznie neutralna i nie powinna zależeć od stosowanych technik, ponieważ w przeciwnym razie wystąpiłoby poważne ryzyko obchodzenia prawa. Ochrona osób fizycznych powinna mieć zastosowanie do przetwarzania danych osobowych w sposób zautomatyzowany, jak również ręcznego przetwarzania, jeśli dane znajdują się lub mają znajdować się w zbiorze danych. Zbiory lub zestawy zbiorów oraz ich strony tytułowe, które nie są zorganizowane

według określonych kryteriów, nie powinny wchodzić w zakres niniejszego rozporządzenia.

(14) Rozporządzenie nie odnosi się do kwestii ochrony podstawowych praw i wolności lub swobodnego przepływu danych dotyczących działalności, która nie wchodzi w zakres prawa unijnego, ani też nie obejmuje przetwarzania danych osobowych przez instytucje, organy i jednostki administracyjne Unii, które podlegają przepisom rozporządzenia (WE) nr 45/2001[44] lub przetwarzania danych osobowych przez państwa członkowskie podczas prowadzenia działalności związanej ze wspólną polityką zagraniczną i bezpieczeństwa Unii.

(15) Niniejsze rozporządzenie nie powinno mieć zastosowania do przetwarzania przez osobę fizyczną danych osobowych o charakterze wyłącznie osobistym lub domowym, takich jak korespondencja i przechowywanie adresów, które są przetwarzane w celach niezarobkowych, zatem bez związku z działalnością zawodową lub handlową. Wyjątek ten nie powinien mieć także zastosowania do administratorów lub podmiotów przetwarzających, którzy zapewniają środki na przetwarzanie danych osobowych w celach osobistych lub domowych.

(16) Ochrona osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy w celu zapobiegania przestępstwom, ich ścigania, wykrywania lub karania albo w celu wykonywania kar kryminalnych oraz swobodnym przepływem takich danych podlegają szczególnemu instrumentowi prawnemu na szczeblu Unii. Z tego względu niniejsze rozporządzenie nie powinno mieć zastosowania do przetwarzania do wyżej wspomnianych celów. Jednak dane przetwarzane przez organy publiczne na mocy niniejszego rozporządzenia, wykorzystywane w celu zapobiegania przestępstwom, ich ścigania, wykrywania lub karania albo w celu wykonywania kar kryminalnych, powinny podlegać bardziej szczegółowemu instrumentowi prawnemu na szczeblu Unii (dyrektywa XX/YYY).

(17) Przepisy niniejszego rozporządzenia pozostają bez uszczerbku dla stosowania dyrektywy 2000/31/WE, w szczególności zasad odpowiedzialności usługodawców będących pośrednikami, o których mowa w art. 12-15 tej dyrektywy.

(18) Niniejsze rozporządzenie pozwala na uwzględnienie zasady publicznego dostępu do dokumentów urzędowych przy stosowaniu przepisów tego rozporządzenia.

(19) Każde przetwarzanie danych osobowych w kontekście działalności prowadzonej w siedzibie administratora lub podmiotu przetwarzającego w Unii powinno odbywać się zgodnie z niniejszym rozporządzeniem, niezależnie od tego, czy samo przetwarzanie ma miejsce w Unii czy poza nią. Siedziba zakłada skuteczne i faktycznie prowadzenie działalności poprzez stabilne rozwiązania. Forma prawna takich rozwiązań, niezależnie od tego, czy chodzi o oddział czy spółkę zależną posiadającą osobowość prawną, nie jest w tym względzie czynnikiem decydującym.

(20) By nie dopuścić do pozbawienia osób fizycznych ochrony, która przysługuje im na mocy niniejszego rozporządzenia, przetwarzanie danych osobowych podmiotów danych, które mają miejsce zamieszkania w Unii, przez administratora niemającego

---

[44] Dz.U. L 8 z 12.1.2001, s. 1.

siedziby w Unii, powinno podlegać niniejszemu rozporządzeniu, w przypadku gdy przetwarzanie wiąże się z oferowaniem towarów lub usług podmiotom danych lub monitorowaniem zachowania tych osób.

(21) Aby stwierdzić, czy przetwarzanie można uznać za „monitorowanie zachowania" podmiotów danych, należy upewnić się, czy osoby fizyczne można wyszukać w internecie, korzystając z technik przetwarzania danych, które polegają na przypisaniu „profilu" danej osobie fizycznej, w szczególności w celu podejmowania decyzji dotyczących tej osoby, analizowania jej preferencji osobistych, zachowań i postaw lub ich przewidywania.

(22) W miejscu, w którym na mocy prawa międzynarodowego publicznego stosuje się prawo krajowe państwa członkowskiego, na przykład na terenie misji dyplomatycznej lub placówki konsularnej, niniejsze rozporządzenie powinno także mieć zastosowanie do administratora niemającego siedziby w Unii.

(23) Zasady ochrony należy stosować do wszelkich informacji dotyczących zidentyfikowanych lub możliwych do zidentyfikowania osób. Aby ustalić, czy można zidentyfikować daną osobę fizyczną, należy wziąć pod uwagę wszystkie sposoby, jakimi mogą posłużyć się administrator lub inna osoba w celu zidentyfikowania tej osoby. Zasady ochrony nie powinny być stosowane do danych zanonimizowanych w taki sposób, że podmiot danych nie może być już zidentyfikowany.

(24) Osoby fizyczne korzystające z usług internetowych można identyfikować na podstawie identyfikatorów internetowych, które znajdują się w urządzeniach, aplikacjach, narzędziach i protokołach, takich jak adresy IP lub identyfikatory plików *cookie*. Mogą one zostawiać ślady, które, w połączeniu z unikatowymi identyfikatorami i innymi informacjami uzyskanymi przez serwery, mogą być wykorzystywane do tworzenia profili poszczególnych osób i ich identyfikacji. W wyniku tego numery identyfikacyjne, dane dotyczące lokalizacji, identyfikatory internetowe lub inne szczególne czynniki jako takie niekonieczne muszą być uważane za dane osobowe w każdych okolicznościach.

(25) Zgoda powinna być wyraźnie wyrażona w dowolny właściwy sposób umożliwiający swobodne i świadome wyrażenie woli przez podmiot danych bądź w formie oświadczenia, bądź w drodze wyraźnego działania potwierdzającego podmiotu danych, przy jednoczesnym zagwarantowaniu, że osoby fizyczne są świadome, iż wyrażają zgodę na przetwarzanie danych osobowych, w tym poprzez zaznaczenie okna wyboru podczas przeglądania strony internetowej lub też inne oświadczenie bądź zachowanie, które w tym kontekście wyraźnie oznacza akceptację przez podmiot danych proponowanego przetwarzania jego danych osobowych. Milczenie lub bezczynność nie powinny zatem stanowić zgody. Zgoda powinna obejmować całość przetwarzania dokonanego w tym samym celu lub w tych samych celach. Jeśli zgoda podmiotu danych ma być wyrażona w następstwie elektronicznego wniosku, wniosek taki musi być jasny, zwięzły i nie powodować niepotrzebnego przerwania świadczenia usługi, której dotyczy.

(26) Dane osobowe dotyczące zdrowia powinny w szczególności obejmować wszelkie dane dotyczące stanu zdrowia podmiotu danych, informacje na temat rejestracji osoby fizycznej w celu świadczenia usług zdrowotnych; informacje o płatnościach danej osoby fizycznej za opiekę zdrowotną lub kwalifikowaniu się danej osoby do

korzystania z opieki zdrowotnej; numer, symbol lub oznaczenie przypisane danej osobie wyłącznie w celu identyfikowania jej dla potrzeb świadczenia opieki zdrowotnej; wszelkie informacje na temat tej osoby zebrane w okresie świadczenia opieki zdrowotnej na jej rzecz; informacje pochodzące z badań laboratoryjnych lub lekarskich dotyczących części ciała lub płynów ustrojowych, w tym próbek biologicznych; informacje umożliwiające identyfikację osoby świadczącej usługi opieki zdrowotnej na rzecz danego pacjenta oraz wszelkie informacje np. na temat choroby, niepełnosprawności, ryzyka choroby, historii medycznej, leczenia klinicznego lub aktualnego stanu fizjologicznego lub biomedycznego podmiotu danych, niezależnie od ich źródła, którym może być np. lekarz lub inny pracownik służby zdrowia, szpital, urządzenie medyczne, badanie diagnostyczne *in vitro*.

(27) Siedzibę administratora w Unii należy ustalić na podstawie obiektywnych kryteriów. Powinna ona zakładać skuteczne i faktycznie zarządzanie, polegające na podejmowaniu najważniejszych decyzji dotyczących celów, warunków i środków przetwarzania w drodze stabilnych rozwiązań. Takie kryterium nie powinno zależeć od tego, czy przetwarzanie danych osobowych jest faktycznie dokonywane w tej lokalizacji; obecność i wykorzystanie środków technicznych i technologii do celów przetwarzania danych osobowych lub działalności w zakresie przetwarzania nie stanowią, same w sobie, takiej siedziby, nie są więc kryteriami wyznaczającymi siedzibę. Siedzibą podmiotu przetwarzającego powinno być miejsce jego zarządu w Unii.

(28) Grupa przedsiębiorstw powinna obejmować przedsiębiorstwo sprawujące kontrolę oraz przedsiębiorstwa kontrolowane, przy czym przedsiębiorstwo sprawujące kontrolę powinno być przedsiębiorstwem, które wywiera dominujący wpływ na inne przedsiębiorstwa ze względu, między innymi, na strukturę właścicielską, udział finansowy lub przepisy regulujące jego działalność lub też uprawnienia do wdrożenia przepisów dotyczących ochrony danych osobowych.

(29) Na szczególną ochronę danych osobowych zasługują dzieci, które mogą być w mniejszym stopniu świadome zagrożeń, konsekwencji, gwarancji i swoich praw związanych z przetwarzaniem danych osobowych. Aby stwierdzić, czy dana osoba jest dzieckiem, w niniejszym rozporządzeniu należy przyjąć definicję określoną w Konwencji Narodów Zjednoczonych o prawach dziecka.

(30) Wszelkie operacje przetwarzania danych osobowych powinny być zgodne z prawem, prowadzone rzetelnie i uczciwie wobec zainteresowanych osób. W szczególności konkretne cele przetwarzania danych powinny być jednoznaczne, zgodne z prawem i określone w momencie zbierania danych. Dane powinny być ścisłe, właściwe i ograniczone do minimum niezbędnego do celów, dla których dane są przetwarzane, co wymaga w szczególności dopilnowania, by zebrane dane nie wykraczały poza określony zakres i by okres przechowywania danych był ograniczony do ścisłego minimum. Dane osobowe powinny być przetwarzane tylko wówczas, gdy celu przetwarzania nie można osiągnąć innymi środkami. Należy podjąć wszelkie stosowne kroki gwarantujące poprawienie lub usunięcie nieścisłych danych osobowych. Aby uniknąć przechowywania danych przez czas dłuższy niż jest to konieczne, administrator powinien ustalić termin usuwania danych lub okresowego przeglądu.

(31) Aby przetwarzanie danych osobowych było zgodne z prawem, powinno odbywać się na podstawie zgody osoby zainteresowanej lub na innej uzasadnionej podstawie

przewidzianej przez prawo: czy to przepisów niniejszego rozporządzenia czy to innych przepisów prawa Unii lub państw członkowskich, o których mowa w tym rozporządzeniu.

(32) Jeśli przetwarzanie odbywa się na podstawie zgody podmiotu danych, ciężar udowodnienia, że podmiot danych wyraził zgodę na operację przetwarzania, spoczywa na administratorze. W szczególności w przypadku pisemnego oświadczenia złożonego w innej sprawie odpowiednie gwarancje powinny zapewniać, iż podmiot danych jest świadomy wyrażenia zgody oraz jej zakresu.

(33) W celu zapewnienia dobrowolnej zgody należy wyjaśnić, że zgoda nie stanowi ważnej podstawy prawnej, jeśli dana osoba nie może dokonać rzeczywistego i wolnego wyboru, a następnie nie może odmówić ani odwołać zgody bez poniesienia szkody.

(34) Zgoda nie powinna stanowić ważnej podstawy prawnej przetwarzania danych osobowych w sytuacji wyraźnego braku równowagi między podmiotem danych a administratorem. Dotyczy to w szczególności przypadku, gdy między podmiotem danych a administratorem istnieje stosunek zależności, między innymi wtedy, gdy dane osobowe pracowników są przetwarzane przez pracodawcę w kontekście zatrudnienia Jeśli administrator jest organem publicznym, brak równowagi wystąpiłby wyłącznie w przypadku operacji przetwarzania szczególnych danych, gdy organ publiczny może nałożyć obowiązek na mocy odpowiednich uprawnień publicznych a zgody nie można uznać za wyrażoną dobrowolnie, uwzględniając interes podmiotu danych.

(35) Przetwarzanie powinno być zgodne z prawem tam, gdzie jest konieczne w kontekście umowy lub zamiaru zawarcia umowy.

(36) Jeśli przetwarzanie odbywa się w ramach wypełnienia przez administratora ciążącego na nim obowiązku prawnego lub jeśli przetwarzanie jest konieczne w celu wykonania zadania realizowanego w interesie publicznym lub wykonania władzy publicznej, podstawę prawną przetwarzania powinny stanowić przepisy prawa Unii lub państwa członkowskiego, które spełniają wymagania Karty praw podstawowych Unii Europejskiej w zakresie ograniczeń praw i wolności. Prawo Unii lub prawo krajowe powinno określić, czy administratorem wykonującym zadanie realizowane w interesie publicznym lub w celu wykonania władzy publicznej powinien być organ administracji publicznej czy inna osoba fizyczna lub prawna podlegająca prawu publicznemu lub prawu prywatnemu, jak np. zrzeszenie zawodowe.

(37) Przetwarzanie danych osobowych powinno być również uznawane za zgodne z prawem, jeśli jest konieczne w celu ochrony interesu, który ma istotne znaczenie dla życia podmiotu danych.

(38) Słuszny interes administratora może stanowić podstawę prawną przetwarzania, pod warunkiem że interesy lub podstawowe prawa i wolności podmiotu danych, nie mają charakteru nadrzędnego. Wymagałoby to przeprowadzenia rzetelnej oceny, w szczególności w sytuacji, gdy podmiotem danych jest dziecko, zważywszy że dzieci wymagają szczególnej ochrony. Podmiot danych powinien mieć prawo wniesienia sprzeciwu wobec przetwarzania ze względu na swoją szczególną sytuacją i w sposób wolny od opłat. Aby zapewnić przejrzystość, administrator powinien być zobowiązany do wyraźnego poinformowania podmiotu danych o słusznych interesach

realizowanych przez administratora, oraz o prawie wniesienia sprzeciwu, a także powinien być zobowiązany do udokumentowania tych słusznych interesów. Zważywszy, że ustawodawca określa w przepisach podstawę prawną przetwarzania danych przez organy publiczne, ta podstawa prawa nie powinna mieć zastosowania do przetwarzania danych przez organy publiczne w ramach wykonywania powierzonych im zadań.

(39) Przetwarzanie danych w zakresie bezwzględnie koniecznym do celów zapewnienia bezpieczeństwa sieci i informacji, tj. zapewnienia odporności sieci lub systemu informacyjnego, na danym poziomie ufności, na zdarzenia przypadkowe lub działania niezgodne z prawem albo podstępne, naruszające dostępność, autentyczność, integralność i poufność przechowywanych lub przesyłanych danych oraz związanych z nimi usług oferowanych lub dostępnych poprzez te sieci i systemy, przez organy publiczne, zespoły reagowania na incydenty komputerowe (CERT), zespoły reagowania na komputerowe incydenty naruszające bezpieczeństwo (CSIRT), dostawców sieci i usług łączności elektronicznej oraz dostawców technologii i usług w zakresie bezpieczeństwa, stanowi słuszny interes danego administratora. Mogłoby to na przykład obejmować zapobieganie nieupoważnionemu dostępowi do sieci łączności elektronicznej oraz rozprowadzaniu złośliwych kodów oraz przerywanie ataków wywołujących „blokadę usługi", a także przeciwdziałanie uszkodzeniu systemów komputerowych i łączności elektronicznej.

(40) Przetwarzanie danych osobowych do innych celów powinno być dozwolone jedynie wtedy, gdy jest ono zgodne z celami, dla których dane zostały pierwotnie zebrane, w szczególności jeśli przetwarzanie jest niezbędne do celów badań historycznych, statystycznych lub naukowych. Jeśli ten inny cel nie jest zgodny z celem pierwotnym, w którym dane zostały zebrane, administrator powinien uzyskać zgodę podmiotu danych na realizację tego celu lub powinien oprzeć przetwarzanie na innej uzasadnionej podstawie zgodnego z prawem przetwarzania, w szczególności przewidzianej przez prawo Unii lub prawo państwa członkowskiego, któremu podlega administrator. W każdym przypadku należy zapewnić stosowanie zasad wskazanych w niniejszym rozporządzeniu, w szczególności w zakresie poinformowania podmiotu danych o tych innych celach.

(41) Dane osobowe, które z racji swego charakteru są szczególnie wrażliwe i narażone na ryzyko w kontekście podstawowych praw lub prywatność, zasługują na szczególną ochronę. Dane te nie powinny być przetwarzane, chyba że podmiot danych wyraźnie wyrazi na to zgodę. Należy jednak wyraźnie wskazać odstępstwa od tego zakazu ze względu na szczególne potrzeby, zwłaszcza wtedy gdy przetwarzanie danych odbywa się w ramach zgodnych z prawem działań niektórych zrzeszeń lub fundacji, których celem jest umożliwienie realizacji podstawowych wolności.

(42) Należy także zezwolić na odstępstwa od zakazu przetwarzania wrażliwych kategorii danych, jeśli odbywa się ono na podstawie przepisów prawa i z zastrzeżeniem odpowiednich gwarancji, w celu ochrony danych osobowych i innych podstawowych praw, jeśli jest to uzasadnione interesem publicznym, w szczególności w celach związanych z opieką zdrowotną, w tym zdrowiem publicznym i ochroną socjalną oraz zarządzaniem usługami opieki zdrowotnej, zwłaszcza by zapewnić odpowiednią jakość i zasadność ekonomiczną procedur stosowanych do rozstrzygania roszczeń w sprawie świadczeń i usług w ramach systemu ubezpieczeń zdrowotnych, lub w celach badań historycznych, statystycznych i naukowych.

(43) Ponadto przetwarzanie danych osobowych przez organy publiczne dla osiągnięcia przez oficjalnie uznane związki religijne celów określonych w prawie konstytucyjnym lub prawie międzynarodowym publicznym, odbywa się ze względu na interes publiczny.

(44) W przypadku gdy w trakcie działań wyborczych funkcjonowanie systemu demokratycznego w niektórych państwach członkowskich wymaga zbierania przez partie polityczne danych na temat opinii politycznych obywateli, przetwarzanie tych danych może być dozwolone ze względu na interes publiczny, pod warunkiem ustanowienia odpowiednich gwarancji.

(45) Jeśli dane przetwarzane przez administratora nie pozwalają mu na zidentyfikowanie osoby fizycznej, nie ma on obowiązku uzyskania dodatkowych informacji w celu identyfikacji podmiotu danych wyłącznie ze względu na konieczność przestrzegania przepisu niniejszego rozporządzenia. W przypadku wniosku o dostęp, administrator powinien być upoważniony do zwracania się do podmiotu danych o udzielenie dalszych informacji, które umożliwią mu znalezienie danych osobowych, o które zwraca się wnioskodawca

(46) Zasada przejrzystości wymaga, by wszelkie informacje przekazywane zarówno opinii publicznej, jak i podmiotowi danych, były łatwo dostępne i zrozumiałe, oraz by napisano je jasnym i prostym językiem. Dotyczy to w szczególności takich sytuacji jak np. reklama w internecie, w których duża liczba podmiotów i złożoność technologiczna praktyki utrudnia podmiotowi danych uzyskanie wiadomości o tym, że dane osobowe go dotyczące są zbierane, kto je zbiera oraz w jakich celach, oraz zrozumienie tego. Zważywszy, że dzieci zasługują na szczególną ochronę, wszelkie informacje i komunikaty, których przetwarzanie jest adresowane konkretnie do dziecka, powinny być tworzone w jasnym i prostym języku, który jest zrozumiały dla dziecka.

(47) Należy opracować sposoby ułatwienia podmiotowi danych korzystania z praw przysługujących mu na mocy niniejszego rozporządzenia, włączając mechanizmy składania wniosków, wolnych od opłat, dotyczących w szczególności dostępu do danych, poprawiania ich, usuwania oraz wykonywania prawa wniesienia sprzeciwu. Administrator powinien być zobowiązany do udzielania odpowiedzi na wnioski podmiotów danych w określonym terminie oraz podania przyczyn ewentualnego braku zastosowania się do wniosku danego podmiotu danych.

(48) Zasady rzetelnego i przejrzystego przetwarzania wymagają, by podmiot danych był informowany w szczególności o prowadzeniu operacji przetwarzania i jej celach, okresie przechowywania danych, przysługującym mu prawie dostępu, poprawienia lub usunięcia danych oraz prawie do złożenia skargi. W przypadku konieczności uzyskania danych od podmiotu danych, należy go także poinformować o tym, że ma on obowiązek przekazać dane oraz o konsekwencjach braku przekazania takich danych

(49) Informacje dotyczące przetwarzania danych osobowych odnoszących się do podmiotu danych powinny być mu przekazane w momencie zbierania danych lub, jeśli dane nie są uzyskiwane od tego podmiotu, w rozsądnym terminie, zależnie od okoliczności sprawy. Jeśli dane można zgodnie z prawem ujawnić innemu odbiorcy, w momencie

pierwszorazowego ujawnienia danych temu odbiorcy należy przekazać stosowne informacje podmiotowi danych.

(50) Nakładanie tego obowiązku nie jest jednak konieczne, jeśli podmiot danych dysponuje już tymi informacjami lub jeśli rejestracja bądź ujawnienie danych są wyraźnie przewidziane przez przepisy prawa, lub jeśli przekazanie informacji podmiotowi danych okazuje się niemożliwe lub wiąże się z niewspółmiernie dużym wysiłkiem. Ten ostatni wariant dotyczy sytuacji, w której przetwarzanie odbywa się w celach związanych z dokumentacją, statystyką lub w celach badań naukowych – w takim przypadku można wziąć pod uwagę liczbę podmiotów danych, wiek danych oraz przyjęte środki wyrównawcze.

(51) Każdej osobie powinno przysługiwać prawo dostępu do danych zebranych na jej temat, a wykonanie tego prawa powinno być na tyle łatwe, by każda osoba była świadoma przetwarzania i mogła zweryfikować jego zgodność z prawem. Dlatego też każdy podmiot danych powinien mieć prawo do wiedzy i uzyskania wiadomości w szczególności o celach, dla których dane są przetwarzane, przez jaki okres, jacy odbiorcy otrzymują dane, o zasadach przetwarzania danych oraz ewentualnych skutkach tego przetwarzania, nawet tylko na podstawie profilowania. Prawo to nie powinno negatywnie wpływać na prawa i wolności innych osób, w tym tajemnice handlowe lub własność intelektualną, w szczególności na prawa autorskie chroniące oprogramowanie. Powyżej omówione względy nie powinny jednak powodować odmowy udzielenia podmiotowi danych wszystkich informacji.

(52) Administrator powinien skorzystać ze wszystkich uzasadnionych środków w celu weryfikacji tożsamości podmiotu danych, który żąda dostępu, w szczególności w kontekście usług internetowych i identyfikatorów internetowych. Administrator nie powinien zatrzymywać danych osobowych wyłącznie po to, by móc odpowiadać na potencjalne wnioski.

(53) Każda osoba powinna mieć prawo do poprawienia dotyczących jej danych osobowych oraz „prawo do bycia zapomnianym”, jeśli przechowywanie tych danych nie jest zgodne z niniejszym rozporządzeniem. W szczególności podmioty danych powinny mieć prawo do tego, by ich dane osobowe zostały usunięte i nie były dalej przetwarzane, jeśli dane te nie są już konieczne do celów, dla których dane są zbierane lub przetwarzane w inny sposób, jeśli podmioty danych odwołały zgodę na przetwarzanie lub jeśli wnoszą sprzeciw wobec przetwarzania danych osobowych ich dotyczących, lub jeśli przetwarzanie ich danych osobowych nie jest zgodne z niniejszym rozporządzeniem z innego powodu. Prawo to ma szczególne znaczenie wtedy, gdy podmiot danych wyraził zgodę jako dziecko, nie będąc w pełni świadomy ryzyk związanych z przetwarzaniem, a w późniejszym czasie chce usunąć takie dane osobowe, zwłaszcza z internetu. Dalsze przechowywanie danych powinno być jednak dopuszczalne, jeśli jest ono niezbędne do celów dokumentacji, statystyki i badań naukowych, realizacji interesu publicznego w dziedzinie zdrowia publicznego, wykonania prawa wolności wypowiedzi, jeśli wymagają tego przepisy prawa lub jeśli są powody ograniczenia przetwarzania danych zamiast ich usunięcia.

(54) Aby wzmocnić „prawo do bycia zapomnianym” w internecie, prawo do usunięcia danych powinno być także rozszerzone w taki sposób, by administrator, który upublicznił dane, miał obowiązek poinformować osoby trzecie, które przetwarzają te dane, że podmiot przetwarzający dane złożył wniosek o usunięcie wszelkich linków

do danych, kopii lub replikacji tych danych osobowych. Aby zapewnić przekazanie tych informacji, administrator powinien podjąć wszelkie racjonalne kroki, w tym środki techniczne, dotyczące danych, za których publikację odpowiada administrator. Jeśli chodzi o publikowanie danych osobowych przez osoby trzecie, administratora należy uznać za odpowiedzialnego za publikację tych danych, jeśli wyraził on zgodę na publikację tych danych przez osobę trzecią.

(55) W celu dalszego wzmocnienia kontroli nad własnymi danymi oraz prawa dostępu, podmioty danych powinny mieć prawo, w przypadku gdy dane osobowe są przetwarzane w sposób elektroniczny oraz w zorganizowanym i powszechnie używanym formacie, do otrzymania kopii dotyczących ich danych także w takim powszechnie używanym formacie elektronicznym. Podmiot danych powinien także móc przekazywać dane, które dostarczył, ze zautomatyzowanej aplikacji, takiej jak sieć społeczna, do innej. Powinno to mieć zastosowanie wtedy, gdy podmiot danych dostarczył dane do automatycznego systemu przetwarzania na podstawie swojej zgody lub w związku z wykonaniem umowy.

(56) W przypadkach, w których dane osobowe mogłyby być przetwarzane zgodnie z prawem w celu ochrony żywotnych interesów podmiotu danych lub gdy jest to uzasadnione interesem publicznym, wykonywaniem władzy publicznej lub słusznymi interesami administratora, każdemu podmiotowi danych powinno jednak przysługiwać prawo wniesienia sprzeciwu wobec przetwarzania danych go dotyczących. Ciężar dowodu w zakresie wykazania, że słuszne interesy administratora mogą mieć charakter nadrzędny wobec interesów lub podstawowych praw i wolności podmiotu danych, spoczywa na administratorze.

(57) Jeśli dane osobowe przetwarzane są do celów marketingu bezpośredniego, podmiot danych powinien mieć prawo wniesienia sprzeciwu wobec takiego przetwarzania w prosty, skuteczny i wolny od opłat sposób.

(58) Każda osoba fizyczna powinna mieć prawo niepodlegania środkowi opartemu na profilowaniu dokonywanym poprzez automatyczne przetwarzanie. Taki środek powinien być jednak dozwolony wtedy, gdy jest wyraźnie przewidziany przez przepisy prawa, stosowany w toku zawierania lub wykonywania umowy lub gdy podmiot danych wyraził na niego zgodę. W każdym przypadku takie przetwarzanie powinno stanowić przedmiot odpowiednich gwarancji, w tym konkretnych informacji podmiotu danych i prawa do interwencji ze strony człowieka, a środek ten nie powinien dotyczyć dzieci.

(59) Ograniczenia dotyczące szczególnych zasad i praw do informacji, dostępu, poprawiania i usuwania lub prawa przenoszenia danych, prawa wniesienia sprzeciwu, środków opartych na profilowaniu, a także informowania podmiotu danych o naruszeniu ochrony danych osobowych oraz pewnych powiązanych obowiązków administratorów mogą być nałożone przez prawo Unii lub państwa członkowskiego, w zakresie w jakim jest to konieczne i proporcjonalne w demokratycznym społeczeństwie, by zagwarantować bezpieczeństwo publiczne, w tym ochronę życia ludzkiego, zwłaszcza w ramach reagowania na klęski żywiołowe lub katastrofy wywołane przez człowieka, możliwość zapobiegania przestępstwom lub naruszeniom zasad etyki w przypadku zawodów regulowanych, ich ścigania i karania, inne publiczne interesy Unii lub państwa członkowskiego, w szczególności ważny interes gospodarczy lub finansowy Unii lub państwa członkowskiego, ochronę podmiotu

danych lub też prawa i wolności innych osób. Ograniczenia te powinny być zgodne z wymogami Karty praw podstawowych Unii Europejskiej oraz Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności.

(60) Należy obciążyć administratora całkowitą odpowiedzialnością za przetwarzanie danych osobowych prowadzone przez niego samego lub w jego imieniu. W szczególności administrator powinien zapewnić zgodność takiej operacji przetwarzania z niniejszym rozporządzeniem i mieć obowiązek wykazania tej zgodności.

(61) Ochrona praw i wolności podmiotów danych w zakresie przetwarzania danych osobowych wymaga podjęcia odpowiednich środków technicznych i organizacyjnych, zarówno przy przygotowywaniu przetwarzania, jak i podczas samego przetwarzania, w celu zagwarantowania spełnienia wymogów niniejszego rozporządzenia. By zapewnić i wykazać zgodność z niniejszym rozporządzeniem, administrator powinien przyjąć wewnętrzne polityki i wdrożyć odpowiednie środki, które są w szczególności zgodne z zasadą uwzględnienia ochrony danych już w fazie projektowania oraz zasadą domyślnej ochrony danych.

(62) Ochrona praw i wolności podmiotów danych, a także zobowiązania i odpowiedzialność administratorów i podmiotów przetwarzających, także w odniesieniu do monitorowania przez organy nadzorcze i środków przez nie stosowanych, wymaga dokonania w niniejszym rozporządzeniu jasnego przydziału obowiązków, w tym w przypadku gdy administrator określa cele, warunki i sposoby przetwarzania wspólnie z innymi administratorami oraz gdy operacja przetwarzania jest dokonywana w imieniu administratora.

(63) Jeśli administrator niemający siedziby w Unii przetwarza dane osobowe podmiotów danych mających miejsce zamieszkania w Unii, a jego działalność w zakresie przetwarzania wiąże się z oferowaniem towarów lub usług tym podmiotom lub monitorowaniem ich zachowania, powinien on wyznaczyć przedstawiciela, chyba że administrator ma siedzibę w państwie trzecim zapewniającym odpowiedni poziom ochrony, jest małym lub średnim przedsiębiorcą, organem lub podmiotem publicznym, lub chyba że jedynie okazjonalnie oferuje towary lub usługi tym podmiotom. Przedstawiciel powinien działać w imieniu administratora, a organ nadzorczy może się do niego zwracać.

(64) By stwierdzić, czy administrator jedynie okazjonalnie oferuje towary i usługi podmiotom danych mającym miejsce zamieszkania w Unii, należy się upewnić, czy z całości działalności administratora wynika, że oferowanie towarów i usług tym osobom, stanowi działalność dodatkową do działalności głównej.

(65) By wykazać zgodność z niniejszym rozporządzeniem, administrator lub podmiot przetwarzający powinni dokumentować każdą operację przetwarzania. Każdy administrator i podmiot przetwarzający powinni być zobowiązani do współpracy z organem nadzorczym oraz do udostępniania mu, na żądanie, dokumentacji, tak by mogła ona służyć do monitorowania tych operacji przetwarzania.

(66) W celu utrzymania bezpieczeństwa i zapobiegania naruszaniu przepisów niniejszego rozporządzenia administrator i podmiot przetwarzający powinni ocenić ryzyko związane z przetwarzaniem oraz wdrożyć środki mające na celu ograniczenie tego

ryzyka. Środki te powinny zapewnić odpowiedni poziom bezpieczeństwa, uwzględniając stan wiedzy naukowej oraz koszty wdrożenia środków w odniesieniu do ryzyka oraz charakteru danych osobowych podlegających ochronie. Ustanawiając standardy techniczne i środki organizacyjne, by zapewnić bezpieczeństwo przetwarzania, Komisja powinna promować neutralność technologiczną, interoperacyjność i innowacyjność oraz, w razie potrzeby, współpracować z państwami trzecimi.

(67) Naruszenie ochrony danych osobowych, w braku odpowiedniej i szybkiej reakcji, może prowadzić do znacznej straty ekonomicznej i szkód społecznych u danej osoby, w tym oszustwa dotyczącego tożsamości. Z tego względu administrator, niezwłocznie po powzięciu wiadomości o naruszeniu, jeśli to możliwe, w ciągu 24 godzin powinien zawiadomić organ nadzorczy o naruszeniu. Jeśli nie jest to możliwe w ciągu 24 godzin, do zawiadomienia należy dołączyć stosowne wyjaśnienie powodów opóźnienia. Osoby, których dane osobowe mogłyby ucierpieć wskutek takiego naruszenia, powinny być niezwłocznie zawiadamiane, aby umożliwić im podjęcie niezbędnych środków ostrożności. Naruszenie powinno być uznawane za wywierające niekorzystny wpływ na dane osobowe lub prywatność podmiotu danych, jeżeli jego skutkiem mogą być np. kradzież lub oszustwo dotyczące tożsamości, uszkodzenie ciała, poważne upokorzenie lub naruszenie dobrego imienia. Zawiadomienie powinno zawierać opis charakteru naruszenia ochrony danych osobowych oraz zalecenia dla osoby zainteresowanej dotyczące ograniczenia potencjalnych niekorzystnych skutków naruszenia. Zawiadomienia powinny być przekazywane podmiotom danych tak szybko jak to racjonalnie możliwe, w ścisłej współpracy z organem nadzorczym oraz z poszanowaniem wytycznych przekazanych przez ten organ lub inne właściwe organy (np. organy ścigania). Na przykład szansa ograniczenia przez podmioty danych bezpośredniego ryzyka szkody wymagałaby szybkiego zawiadomienia podmiotów danych, zaś potrzeba wdrożenia właściwych środków w przypadku powtarzających się lub podobnych naruszeń ochrony danych może usprawiedliwiać dłuższe opóźnienie.

(68) By ustalić, czy organ nadzorczy i podmiot danych zostali niezwłocznie zawiadomieni o naruszeniu ochrony danych osobowych, należy sprawdzić, czy administrator wdrożył i zastosował odpowiednią ochronę technologiczną i środki organizacyjne pozwalające od razu stwierdzić, czy wystąpiło naruszenie ochrony danych osobowych, oraz niezwłocznie poinformować organ nadzorczy i podmiot danych, przed narażeniem na szwank interesu osobistego lub gospodarczego, uwzględniając zwłaszcza charakter i wagę naruszenia ochrony danych osobowych i jego konsekwencje oraz niekorzystne skutki dla podmiotu danych.

(69) Przy określaniu szczegółowych przepisów dotyczących formy i procedur mających zastosowanie przy zawiadamianiu o naruszeniach ochrony danych osobowych należy odpowiednio uwzględnić okoliczności naruszenia, w tym zbadać, czy dane osobowe były zabezpieczone właściwymi technicznymi środkami ochrony, skutecznie ograniczającymi prawdopodobieństwo oszustwa dotyczącego tożsamości lub innych form nadużycia danych. W tych przepisach i procedurach należy ponadto uwzględnić słuszne interesy organów ścigania, w przypadkach gdy przedwczesne ujawnienie mogłoby niepotrzebnie utrudnić badanie okoliczności naruszenia.

(70) Dyrektywa 95/46/WE przewidziała ogólny obowiązek zawiadamiania organów nadzorczych o przetwarzaniu danych osobowych. Obowiązek ten powoduje jednak

obciążenia administracyjne i finansowe i nie w każdym przypadku przyczynia się do ochrony danych osobowych. Z tego względu należałoby znieść ten ogólny obowiązek zawiadomienia i zastąpić go skutecznymi procedurami i mechanizmami, które zamiast tego koncentrowałyby się na operacjach przetwarzania, które mogą stwarzać określone ryzyko dla praw i wolności podmiotów danych, ze względu na swój charakter, zakres lub cele. W takich przypadkach administrator lub podmiot przetwarzający powinni przeprowadzić ocenę skutków w zakresie ochrony danych przed przetwarzaniem, która powinna w szczególności obejmować przewidywane środki, gwarancje i mechanizmy mające na celu zapewnienie ochrony danych osobowych oraz wykazanie zgodności z niniejszym rozporządzeniem.

(71) Powinno to w szczególności mieć zastosowanie do nowo ustanowionych wielkoskalowych zbiorów danych, które mają na celu przetwarzanie znacznej ilości danych osobowych na szczeblu regionalnym, krajowym lub ponadnarodowym i które mogłyby mieć wpływ na dużą liczbę podmiotów danych.

(72) W niektórych okolicznościach może być rozsądne i korzystne, by temat oceny skutków w zakresie ochrony danych był szerszy niż tylko pojedynczy projekt, na przykład gdy organy lub podmioty publiczne zamierzają ustanowić wspólną aplikację lub platformę służącą do przetwarzania lub gdy kilku administratorów planuje wprowadzić wspólną aplikację lub środowisko przetwarzania obejmujące sektor lub segment przemysłu lub do celów powszechnie stosowanej działalności międzysektorowej.

(73) Ocenę skutków w zakresie ochrony danych powinien przeprowadzić organ publiczny lub podmiot publiczny, o ile takiej oceny nie dokonano do tej pory w kontekście przyjęcia przepisów prawa krajowego, na których opiera się wykonanie zadań organu publicznego lub podmiotu publicznego i które regulują szczególną operację przetwarzania lub zestaw omawianych operacji.

(74) Jeśli ocena skutków w zakresie ochrony danych wykaże, że operacje przetwarzania wiążą się z wysokim poziomem konkretnych ryzyk dla praw i wolności podmiotów danych, takich jak pozbawienie osób fizycznych przysługującego im prawa lub korzystanie z konkretnych nowych technologii, przed rozpoczęciem operacji należy zasięgnąć opinii organu nadzorczego na temat ryzykownego przetwarzania, które mogłoby być niezgodne z niniejszym rozporządzeniem oraz przedstawić propozycje naprawienia tej sytuacji. Opinii należy zasięgnąć również w trakcie przygotowywania środka ustawodawczego przez parlament narodowy lub środka opartego na takim środku prawnym, który określa charakter przetwarzania danych oraz daje odpowiednie gwarancje.

(75) Jeśli przetwarzanie odbywa się w sektorze publicznym lub jeśli przetwarzanie w sektorze prywatnym prowadzi duże przedsiębiorstwo, lub jeśli główna działalność przedsiębiorstwa, niezależnie od jego wielkości, obejmuje operacje przetwarzania, które wymagają regularnego i systematycznego monitorowania, osoba trzecia powinna wspomagać administratora lub podmiot przetwarzający w monitorowaniu zgodności, na poziomie wewnętrznym, z niniejszym rozporządzeniem. Taki inspektor ochrony danych, który może być pracownikiem administratora, powinien być w stanie niezależnie wykonywać swoje obowiązki i zadania.

(76) Zrzeszenia lub inne organy reprezentujące różne kategorie administratorów należy zachęcać do sporządzenia kodeksów postępowania, w granicach niniejszego rozporządzenia, by ułatwiać skuteczne stosowanie niniejszego rozporządzenia, uwzględniając szczególny charakter przetwarzania prowadzonego w niektórych sektorach.

(77) By zwiększyć przejrzystość i zgodność z niniejszym rozporządzeniem, należy zachęcać do ustanowienia mechanizmów certyfikacji oraz wprowadzenia pieczęci i oznaczeń w zakresie ochrony danych, umożliwiając w ten sposób podmiotom danych szybką ocenę poziomu ochrony danych odnośnych produktów i usług.

(78) Transgraniczny przepływ danych osobowych jest koniecznym warunkiem rozwoju handlu międzynarodowego i współpracy międzynarodowej. Zwiększenie tego przepływu wiąże się z nowymi wyzwaniami i problemami w zakresie ochrony danych osobowych. Przekazując dane osobowe z Unii do państw trzecich lub organizacji międzynarodowych, nie należy jednak zmniejszać poziomu ochrony osób fizycznych gwarantowanego w Unii na mocy niniejszego rozporządzenia. W każdym razie przekazywanie danych do państw trzecich może odbywać się jedynie w pełnej zgodności z niniejszym rozporządzeniem.

(79) Niniejsze rozporządzenie nie narusza postanowień umów międzynarodowych zawartych między Unią a państwami trzecimi, regulujących przekazywanie danych osobowych, przewidujących odpowiednie gwarancje dla podmiotów danych.

(80) Komisja może podjąć decyzję, która będzie obowiązywać w całej Unii, że niektóre państwa trzecie lub też jakieś terytorium lub sektor, w którym odbywa się przetwarzanie danych w państwie trzecim, bądź organizacja międzynarodowa oferują odpowiedni poziom ochrony danych, gwarantując tym samym pewność prawną i jednolitość w całej Unii, jeśli chodzi o państwa trzecie lub organizacje międzynarodowe uważane za zapewniające taki poziom ochrony. W takich przypadkach przekazywanie danych osobowych do tych państw może odbywać się bez potrzeby uzyskania dalszego zezwolenia.

(81) Zgodnie z podstawowymi wartościami, na których opiera się Unia, w szczególności ochroną praw człowieka, w swej ocenie państwa trzeciego Komisja powinna wziąć pod uwagę sposób, w jaki dane państwo trzecie przestrzega zasad praworządności, dostępu do wymiaru sprawiedliwości, a także międzynarodowych norm i standardów ochrony praw człowieka.

(82) Komisja może również uznać, że państwo trzecie lub terytorium bądź sektor, w którym odbywa się przetwarzanie danych w państwie trzecim, albo organizacja międzynarodowa nie oferują odpowiedniego poziomu ochrony danych. W związku z tym przekazywanie danych osobowych do tego państwa trzeciego powinno być zakazane. W takim przypadku należałoby przewidzieć możliwość odbywania konsultacji między Komisją a tymi państwami trzecimi lub organizacjami międzynarodowymi.

(83) W braku decyzji stwierdzającej odpowiedni poziom ochrony administrator lub podmiot przetwarzający powinni podjąć środki mające na celu zrekompensowanie braku ochrony w państwie trzecim poprzez zaoferowanie podmiotowi danych odpowiednich gwarancji. Takie odpowiednie gwarancje mogą polegać na skorzystaniu

z wiążących reguł korporacyjnych, standardowych klauzul ochrony danych przyjętych przez Komisję, standardowych klauzul ochrony danych przyjętych przez organ nadzorczy, klauzul umownych dopuszczonych przez organ nadzorczy lub innych właściwych i proporcjonalnych środków uzasadnionych w świetle wszystkich okoliczności związanych z jedną operacją przekazania danych lub zestawem takich operacji przekazania, o ile zezwoli na to organ nadzorczy.

(84) Możliwość korzystania przez administratora lub podmiot przetwarzający ze standardowych klauzul ochrony danych przyjętych przez Komisję lub organ nadzorczy nie powinna uniemożliwiać włączenia przez nich standardowych klauzul ochrony danych do szerszej umowy ani dodania innych klauzul, pod warunkiem że nie są one sprzeczne, bezpośrednio lub pośrednio, ze standardowymi klauzulami umownymi przyjętymi przez Komisję lub organ nadzorczy lub też nie naruszają podstawowych praw lub wolności podmiotów danych.

(85) Grupa korporacyjna powinna móc korzystać z zatwierdzonych wiążących reguł korporacyjnych do międzynarodowego przekazywania danych z Unii do organizacji w ramach tej samej korporacyjnej grupy przedsiębiorstw, o ile takie reguły korporacyjne obejmują istotne zasady i egzekwowalne prawa mające na celu zapewnienie odpowiednich standardów przekazywania lub kategorii przekazywania danych osobowych.

(86) Należy przewidzieć możliwość przekazywania danych w niektórych okolicznościach, jeżeli podmiot danych wyraził na to zgodę, jeżeli przekazanie danych jest konieczne w związku z umową lub roszczeniem prawnym, jeżeli wymagać tego będzie ochrona ważnego interesu publicznego wskazanego przez Unię lub państwo członkowskie lub w przypadku przekazania danych z rejestru utworzonego na mocy przepisów prawa i przeznaczonego do wglądu dla ogółu społeczeństwa lub osób wykazujących słuszny interes. W tym ostatnim przypadku przekazanie nie powinno obejmować całości danych lub całych kategorii danych z rejestru oraz, jeżeli rejestr jest przeznaczony do wglądu dla osób wykazujących słuszny interes, przekazanie danych powinno nastąpić jedynie na wniosek tych osób lub wówczas, gdy osoby te mają być odbiorcami.

(87) Odstępstwa te powinny mieć w szczególności zastosowanie do przekazywania danych wymaganego i niezbędnego do ochrony istotnego interesu publicznego, na przykład w przypadkach przesyłania danych za granicę między organami ds. konkurencji, organami podatkowymi lub administracją celną, finansowymi organami nadzorczymi, między służbami odpowiedzialnymi za sprawy ubezpieczeń społecznych lub do organów odpowiedzialnych za zapobieganie przestępstwom, ich ściganie, wykrywanie lub karanie.

(88) Przekazywanie, którego nie można określić jako częste lub masowe, mogłoby także być możliwe ze względu na słuszne interesy administratora lub podmiotu przetwarzającego, przy założeniu, że dokonali oni oceny wszystkich okoliczności związanych z przekazaniem danych. W przypadku przetwarzania do celów dokumentacji, statystyki i badań naukowych należy wziąć pod uwagę słuszne oczekiwania społeczeństwa w zakresie zwiększenia wiedzy.

(89) W każdym przypadku, jeśli Komicja nie podjęła decyzji stwierdzającej odpowiedni poziomu ochrony danych w państwie trzecim, administrator lub podmiot przetwarzający powinni skorzystać z rozwiązań, które dają podmiotom danych

gwarancję, że będą one nadal podlegać podstawowym prawom i gwarancjom w zakresie przetwarzania ich danych w Unii, także po przekazaniu danych.

(90) Niektóre państwa trzecie uchwalają ustawy, rozporządzenia i inne instrumenty prawne, które mają bezpośrednio regulować działalność w zakresie przetwarzania danych osób fizycznych i prawnych podlegających jurysdykcji państw członkowskich. Ekstraterytorialne stosowanie tych ustaw, rozporządzeń i innych instrumentów prawnych może naruszać prawo międzynarodowe i uniemożliwiać osiągnięcie celu ochrony osób fizycznych zagwarantowanej przez Unię w niniejszym rozporządzeniu. Przekazywanie nie powinno być dopuszczalne, jeśli nie są spełnione warunki przekazywania danych do państw trzecich wskazane w niniejszym rozporządzeniu. Może to może między innymi dotyczyć sytuacji, w której ujawnienie jest niezbędne ze względu na ważny interes publiczny uznany w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator. Warunki istnienia ważnego interesu publicznego powinny zostać następnie określone przez Komisję w akcie delegowanym.

(91) Przenoszenie danych osobowych ponad granicami może wiązać się z jeszcze większym ryzykiem niemożności wykonywania przez osoby fizyczne praw do ochrony danych osobowych, w szczególności by chronić się przed niezgodnym z prawem wykorzystaniem lub ujawnieniem tych informacji. Organy nadzorcze mogą jednocześnie uznać, że nie są w stanie rozpatrywać skarg lub prowadzić dochodzeń związanych z działalnością, która ma miejsce poza granicami ich państwa. Ich wysiłki zmierzające do wspólnej pracy w kontekście transgranicznym mogą także być hamowane przez niewystarczające uprawnienia w zakresie zapobiegania powyżej opisanym zjawiskom lub zaradzenia im, niespójne systemy prawne oraz przeszkody praktyczne, takie jak ograniczone środki. Z tego względu należy promować ściślejszą współpracę między organami nadzorującymi ochronę danych, by pomagać im w wymianie informacji i prowadzeniu dochodzeń z ich międzynarodowymi odpowiednikami.

(92) Utworzenie w państwach członkowskich organów nadzorczych, wykonujących swoje funkcje w sposób całkowicie niezależny, jest zasadniczym elementem ochrony osób fizycznych w zakresie przetwarzania danych osobowych. Państwa członkowskie mogą ustanowić więcej niż jeden organu nadzorczy, by odzwierciedlić swoją strukturę konstytucyjną, organizacyjną i administracyjną.

(93) Jeśli państwo członkowskie ustanowi kilka organów nadzorczych, powinno także w swoich przepisach ustanowić mechanizmy zapewnienia skutecznego udziału tych organów nadzorczych w mechanizmie zgodności. Takie państwo członkowskie powinno w szczególności wskazać organ nadzorczy, który działa jako pojedynczy punkt kontaktowy do celów skutecznego udziału tych organów w omawianym mechanizmie, by zapewnić sprawną i płynną współpracę z innymi organami nadzorczymi, Europejską Radą Ochrony Danych i Komisją.

(94) Każdy organ nadzorczy powinien zostać wyposażony w odpowiednie zasoby finansowe i ludzkie, pomieszczenia i infrastrukturę, niezbędne do skutecznego wykonywania swoich zadań, w tym zadań związanych ze wzajemną pomocą i współpracą z innymi organami nadzorczymi w całej Unii.

(95) Warunki ogólne członkostwa w organie nadzorczym powinny być określone w przepisach prawa każdego państwa członkowskiego i powinny w szczególności przewidywać, iż członkowie tego organu powinni być wyznaczeni przez parlament albo przez rząd państwa członkowskiego oraz obejmować zasady dotyczące kwalifikacji i stanowiska tych członków.

(96) Organy nadzorcze powinny monitorować stosowanie przepisów w sposób zgodny z niniejszym rozporządzeniem oraz przyczyniać się do jego spójnego stosowania w całej Unii, w celu ochrony osób fizycznych w zakresie przetwarzania ich danych osobowych oraz ułatwienia swobodnego przepływu danych osobowych w ramach rynku wewnętrznego. W tym celu organy nadzorcze powinny współpracować ze sobą oraz z Komisją.

(97) Jeśli przetwarzanie danych osobowych w kontekście działalności prowadzonej w siedzibie administratora lub podmiotu przetwarzającego w Unii odbywa się w kilku państwach, jeden organ nadzorczy powinien być właściwy w zakresie monitorowania działalności administratora lub podmiotu przetwarzającego w całej Unii oraz podejmowania odnośnych decyzji, by zwiększyć spójne stosowanie, zagwarantować pewność prawną oraz ograniczyć obciążenie administracyjne administratorów i podmiotów przetwarzających.

(98) Właściwym organem, zapewniającym taki punkt kompleksowej obsługi, powinien być organ nadzorczy państwa członkowskiego, w którym administrator lub podmiot przetwarzający ma siedzibę główną.

(99) Niniejsze rozporządzenie ma zastosowanie także do działalności sądów krajowych, natomiast właściwość organów nadzorczych nie powinna obejmować przetwarzania danych osobowych wykorzystywanych przez sądy w ramach sprawowania wymiaru sprawiedliwości, by chronić niezawisłość sędziów podczas wykonywania przez nich zadań sądowych. Wyjątek ten powinien być jednak ściśle ograniczony do rzeczywistych działań sądowych w sprawach sądowych i nie powinien mieć zastosowania do innych działań, w których sędziowie mogą brać udział, zgodnie z prawem krajowym.

(100) By zapewnić spójne monitorowanie i wykonanie niniejszego rozporządzenia w całej Unii, organy nadzorcze powinny mieć w każdym państwie członkowskim te same obowiązki i faktyczne uprawnienia, w tym uprawnienie do przeprowadzania dochodzenia i prawnie wiążącej interwencji, podejmowania decyzji i nakładania sankcji, w szczególności w sprawach skarg od osób fizycznych oraz do udziału w postępowaniu sądowym. Uprawnienia dochodzeniowe organów nadzorczych, jeśli chodzi o dostęp do pomieszczeń, powinny być wykonywane zgodnie z prawem unijnym i prawem krajowym. W szczególności dotyczy to wymogu uprzedniego uzyskania zezwolenia sądu.

(101) Każdy organ nadzorczy powinien rozpatrywać skargi złożone przez podmiot danych oraz przeprowadzić stosowne dochodzenie. Dochodzenie na podstawie skargi powinno być prowadzone, z zastrzeżeniem kontroli sądowej, w zakresie odpowiednim do konkretnej sprawy. Organ nadzorczy powinien poinformować podmiot danych o postępach i wyniku skargi w rozsądnym terminie. Jeśli dana sprawa wymaga prowadzenia dalszego dochodzenia lub koordynacji z innym organem nadzorczym, podmiot danych powinien być o tym poinformowany.

(102) Działania w zakresie podnoszenia świadomości prowadzone przez organy nadzorcze i skierowane do opinii publicznej powinny obejmować szczególne środki adresowane do administratorów i podmiotów przetwarzających, w tym mikroprzedsiębiorców oraz małych i średnich przedsiębiorców, a także podmiotów danych.

(103) Organy nadzorcze powinny wspierać się wzajemnie w wykonywaniu swoich zadań oraz świadczyć sobie wzajemną pomoc, by zapewnić spójne stosowanie i egzekwowanie przepisów niniejszego rozporządzenia na rynku wewnętrznym.

(104) Każdy organ nadzorczy powinien mieć prawo udziału w operacjach prowadzonych wspólnie przez organy nadzorcze. Organ nadzoru, który otrzyma stosowny wniosek, powinien mieć obowiązek udzielenia odpowiedzi w ściśle określonym terminie.

(105) By zapewnić spójne stosowanie przepisów niniejszego rozporządzenia w całej Unii, należy ustanowić mechanizm zgodności w zakresie współpracy między organami nadzorczymi i Komisją. Mechanizm ten powinien mieć w szczególności zastosowanie tam, gdzie organ nadzorczy zamierza podjąć środek w zakresie operacji przetwarzania powiązanych z oferowaniem towarów lub usług podmiotom danych w kilku państwach członkowskich, lub też monitorowaniem podmiotów danych, lub który mógłby mieć istotny wpływ na swobodny przepływ danych. Powinien także mieć zastosowanie wtedy, gdy organ nadzorczy lub Komisja wnioskują o rozwiązanie danej kwestii w ramach mechanizmu zgodności. Mechanizm ten powinien pozostawać bez uszczerbku dla środków, które Komisja może podjąć w ramach wykonywania swoich uprawnień na mocy Traktatu.

(106) W ramach stosowania mechanizmu zgodności Europejska Rada Ochrony Danych powinna, w określonym terminie, wydać opinię, o ile tak postanowią jej członkowie w głosowaniu zwykłą większością głosów lub jeśli zażądają tego organ nadzorczy lub Komisja.

(107) By zapewnić zgodność z przepisami niniejszego rozporządzenia, Komisja może przyjąć opinię lub podjąć decyzję w tej sprawie, żądając od organu nadzorczego zawieszenia tego projektu środka.

(108) Może zaistnieć nagła potrzeba działania w celu ochrony interesów podmiotów danych, w szczególności gdy istnieje niebezpieczeństwo, że egzekwowanie prawa przysługującego podmiotowi danych może być istotnie utrudnione. Z tego względu organ nadzorczy, stosując mechanizm zgodności, powinien być w stanie przyjąć środki tymczasowe o określonym czasie obowiązywania.

(109) Stosowanie tego mechanizmu powinno być warunkiem ważności prawnej i egzekwowania odnośnej decyzji przez organ nadzorczy. W innych przypadkach o charakterze transgranicznym wzajemna współpraca i wspólne dochodzenia mogą być prowadzone przez zainteresowane organy nadzorcze na zasadzie dwustronnej lub wielostronnej bez stosowania mechanizmu zgodności.

(110) Na szczeblu Unii należy ustanowić Europejską Radę Ochrony Danych. Powinna ona zastąpić Grupę Roboczą ds. Ochrony Osób Fizycznych w zakresie Przetwarzania Danych Osobowych powołaną na mocy dyrektywy 95/46/WE. W jej skład powinni wchodzić szefowie organów nadzorczych wszystkich państw członkowskich oraz Europejski Inspektor Ochrony Danych. Komisja powinna uczestniczyć w jej

działaniach. Europejska Rada Ochrony Danych powinna przyczyniać się do spójnego stosowania przepisów niniejszego rozporządzenia na terytorium całej Unii, w tym poprzez doradzanie Komisji i promowanie współpracy organów nadzorczych na terytorium całej Unii. Wypełniając swoje zadania, Europejska Rada Ochrony Danych powinna działać niezależnie.

(111) Każdy podmiot danych powinien mieć prawo do złożenia skargi do organu nadzorczego w dowolnym państwie członkowskim oraz prawo do sądowego środka ochrony prawnej, jeśli uzna, że jego prawa wynikające z niniejszego rozporządzenia są naruszane lub jeśli organ nadzorczy nie reaguje na skargę lub nie podejmuje działania, pomimo iż jest ono niezbędne w celu ochrony praw podmiotu danych.

(112) Każdy organ, organizacja lub zrzeszenie, które ma na celu ochronę praw i interesów podmiotów danych w zakresie ochrony ich danych i które zostało utworzone zgodnie z prawem państwa członkowskiego, powinno mieć prawo do złożenia skargi do organu nadzorczego lub wykonania prawa do sądowego środka ochrony prawnej w imieniu podmiotów danych, lub też złożenia, niezależnie od skargi podmiotu danych, własnej skargi, jeśli uzna, iż doszło do naruszenia ochrony danych osobowych.

(113) Każda osoba fizyczna lub prawna powinna mieć prawo do sądowego środka ochrony prawnej przeciwko dotyczącej jej decyzji organu nadzorczego. Postępowanie przeciwko organowi nadzorczemu należy wszcząć przed sądem państwa członkowskiego, w którym organ nadzorczy ma siedzibę.

(114) By wzmocnić ochronę sądową podmiotu danych w sytuacjach, w których właściwy organ nadzorczy ma siedzibę w innym państwie członkowskim niż to, w którym mieszka podmiot danych, podmiot danych może zwrócić się do podmiotu, organizacji lub zrzeszenia mającego na celu ochronę praw i interesów podmiotu danych w zakresie ochrony jego danych z wnioskiem o wszczęcie w jego imieniu postępowania przeciwko temu organowi nadzorczemu we właściwym sądzie innego państwa członkowskiego.

(115) W sytuacji, w której właściwy organ nadzorczy mający siedzibę w innym państwie członkowskim nie podejmuje działania lub podjął niewystarczające środki w odniesieniu do skargi, podmiot danych może zwrócić się do organu nadzorczego w państwie członkowskim, w którym ma miejsce zwykłego pobytu, o wszczęcie postępowania przeciwko temu organowi nadzorczemu we właściwym sądzie innego państwa członkowskiego. Organ nadzorczy, do którego złożono wniosek, może podjąć decyzję, z zastrzeżeniem kontroli sądowej, czy przyjęcie wniosku jest właściwe.

(116) W przypadku postępowania przeciwko administratorowi lub podmiotowi przetwarzającemu, powód powinien mieć możliwość wniesienia pozwu do sądu w państwie członkowskim, w którym administrator lub podmiot przetwarzający mają siedzibę lub w którym mieszka podmiot danych, chyba że administrator jest organem publicznym działającym w ramach wykonywania swoich uprawnień publicznych.

(117) Jeśli istnieją przesłanki, by sądzić, że w sądach w różnych państwach członkowskich toczą się równoległe postępowania, sądy powinny być zobowiązane do kontaktowania się ze sobą. Sądy powinny mieć możliwość zawieszenia postępowania, w sytuacji gdy w innym państwie członkowskim toczy się postępowanie równoległe. W celu zapewnienia skuteczności postępowań sądowych państwa członkowskie powinny

zagwarantować szybkie przyjmowanie środków mających zaradzić lub zapobiec naruszeniom niniejszego rozporządzenia.

(118) Szkoda, jaką dana osoba może ponieść wskutek niezgodnego z prawem przetwarzania danych, powinna zostać naprawiona przez administratora lub podmiot przetwarzający, który może być zwolniony z odpowiedzialności w przypadku dowiedzenia, że szkoda nie powstała z jego winy, szczególnie wówczas gdy udowodni winę podmiotu danych lub w przypadku siły wyższej.

(119) Na wszystkie osoby fizyczne i prawne, która nie przestrzegają niniejszego rozporządzenia, niezależnie od tego czy działają na podstawie prawa prywatnego czy publicznego, powinny zostać nałożone kary. Państwa członkowskie powinny dopilnować, by kary były skuteczne, proporcjonalne i odstraszające, oraz podjąć wszelkie środki mające na celu wykonanie tych kar.

(120) W celu wzmocnienia i zharmonizowania sankcji administracyjnych za naruszenia przepisów niniejszego rozporządzenia, każdy organ nadzorczy powinien być uprawniony do nakładania sankcji administracyjnych. Niniejsze rozporządzenie powinno wymieniać te przestępstwa oraz wskazywać górną granicę wysokości grzywien administracyjnych, którą należy ustalić oddzielnie dla każdego przypadku, odpowiednio do danej sytuacji, ze szczególnym uwzględnieniem charakteru, wagi i czasu trwania naruszenia. Z mechanizmu zgodności można także korzystać do zniesienia różnic w stosowaniu sankcji administracyjnych.

(121) Przetwarzanie danych osobowych wyłącznie w celach dziennikarskich lub w celu uzyskania wyrazu artystycznego lub literackiego powinno kwalifikować się do zwolnienia z wymogów niektórych przepisów niniejszego rozporządzenia, by pogodzić prawo do ochrony danych osobowych z prawem do wolności wypowiedzi, a zwłaszcza prawem do uzyskiwania i udzielania informacji, co gwarantuje w szczególności art. 11 Karty praw podstawowych Unii Europejskiej. Powinno mieć to w szczególności zastosowanie do przetwarzania danych osobowych w dziedzinie techniki audiowizualnej oraz w archiwach danych i bibliotekach prasowych. Z tego względu państwa członkowskie powinny przyjąć środki ustawodawcze, które powinny określać wyjątki i odstępstwa konieczne do zapewnienia równowagi pomiędzy prawami podstawowymi. Państwa członkowskie powinny przyjąć takie wyjątki i odstępstwa, jeśli chodzi o zasady ogólne, prawa podmiotów danych, administratora i podmiot przetwarzający, przekazywanie danych do państw trzecich lub organizacji międzynarodowych, organy nadzorcze oraz współpracę i zgodność. Nie powinno to jednak powodować wprowadzenia przez państwa członkowskie wyjątków od innych przepisów rozporządzenia. W celu uwzględnienia znaczenia prawa do wolności wypowiedzi w każdym demokratycznym społeczeństwie, należy dokonać wykładni pojęć dotyczących tej wolności, takich jak szeroko rozumiane dziennikarstwo. Państwa członkowskie powinny zatem zaklasyfikować jako działalność „dziennikarską” do celów wyjątków i odstępstw określonych w niniejszym rozporządzeniu, działalność której przedmiotem jest ujawnianie opinii publicznej informacji, opinii lub pomysłów, niezależnie od nośnika wykorzystanego do ich przekazania. Działalność ta nie powinna być ograniczona do agencji medialnych i może być podejmowana zarówno w celach dochodowych, jak i w celach niedochodowych.

(122) Przetwarzanie danych osobowych dotyczących zdrowia, jako szczególnej kategorii danych, które zasługują na wyższy poziom ochrony, może być często uzasadnione wieloma względami przemawiającymi na korzyść poszczególnych osób i społeczeństwa jako całości, zwłaszcza w kontekście zapewnienia ciągłości transgranicznej opieki zdrowotnej. Z tego względu niniejsze rozporządzenie powinno przewidywać zharmonizowane warunki przetwarzania danych dotyczących zdrowia, z zastrzeżeniem szczególnych i odpowiednich gwarancji w celu ochrony podstawowych praw i danych osobowych osób fizycznych. Obejmuje to prawo osób fizycznych do dostępu do ich danych osobowych dotyczących zdrowia, na przykład danych w dokumentacji medycznej zawierających takie informacje, jak diagnoza, wyniki badań, oceny dokonywane przez lekarzy prowadzących leczenie oraz informacje na temat wszelkich stosowanych terapii lub przeprowadzonych zabiegów.

(123) Przetwarzanie danych osobowych dotyczących zdrowia bez zgody podmiotu danych może być konieczne ze względu na interes publiczny w dziedzinie zdrowia publicznego. W tym kontekście „zdrowie publiczne" należy interpretować zgodnie z definicją w rozporządzeniu (WE) nr 1338/2008 Parlamentu Europejskiego i Rady z dnia 16 grudnia 2008 r. w sprawie statystyk Wspólnoty w zakresie zdrowia publicznego oraz zdrowia i bezpieczeństwa w pracy, według której oznacza ono 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, opiekę zdrowotną, wydatki na opiekę zdrowotną i sposób jej finansowania oraz przyczyny zgonów. Takie przetwarzanie danych osobowych dotyczących zdrowia w celu realizacji interesu publicznego nie powinno skutkować przetwarzaniem danych do innych celów przez osoby trzecie, takie jak pracownicy, zakłady ubezpieczeń i banki.

(124) Zasady ogólne ochrony osób fizycznych w zakresie przetwarzania danych osobowych powinny mieć także zastosowanie w kontekście zatrudnienia. Zatem w celu regulacji przetwarzania danych osobowych pracowników w kontekście zatrudnienia państwa członkowskie powinny mieć możliwość, w granicach niniejszego rozporządzenia, przyjmowania w drodze ustawy przepisów szczególnych dotyczących przetwarzania danych osobowych w sektorze zatrudnienia.

(125) Zgodne z prawem przetwarzanie danych osobowych do celów dokumentacji, statystyki lub badań naukowych powinno także respektować inne odnośne przepisy, takie jak dotyczące prób klinicznych.

(126) Do celów niniejszego rozporządzenia badania naukowe powinny obejmować badania podstawowe, badania stosowane oraz badania finansowane ze środków prywatnych, a ponadto powinny uwzględniać cel Unii określony w art. 179 ust. 1 Traktatu o funkcjonowaniu Unii Europejskiej polegający na ustanowieniu Europejskiej Przestrzeni Badawczej.

(127) Jeśli chodzi o uprawnienia organów nadzorczych w zakresie uzyskania od administratora lub podmiotu przetwarzającego dostępu do danych osobowych oraz dostępu do ich pomieszczeń, państwa członkowskie mogą przyjąć w drodze ustawy, w granicach niniejszego rozporządzenia, przepisy szczególne mające na celu ochronę obowiązku zachowania tajemnicy służbowej lub innej równoważnej tajemnicy, w

zakresie w jakim jest to konieczne, by pogodzić prawo do ochrony danych osobowych z obowiązkiem zachowania tajemnicy służbowej.

(128) Niniejsze rozporządzenie szanuje status przyznany na mocy prawa krajowego kościołom i stowarzyszeniom lub wspólnotom religijnym w państwach członkowskich i nie narusza tego statusu, jak uznano w art. 17 Traktatu o funkcjonowaniu Unii Europejskiej. W związku z tym, jeśli kościół w państwie członkowskim stosuje, w momencie wejścia w życie niniejszego rozporządzenia, kompleksowe przepisy dotyczące ochrony osób fizycznych w zakresie przetwarzania danych osobowych, te obowiązujące przepisy powinny mieć zastosowanie, jeżeli zostaną dostosowane do niniejszego rozporządzenia. Kościoły i stowarzyszenia religijne powinny być zobowiązane do ustanowienia całkowicie niezależnego organu nadzorczego.

(129) By spełnić cele niniejszego rozporządzenia, mianowicie chronić podstawowe prawa i wolności osób fizycznych, w szczególności ich prawo do ochrony danych osobowych, oraz by zagwarantować swobodny przepływ danych osobowych w Unii, należy przekazać Komisji uprawnienie do przyjmowania aktów zgodnie z art. 290 Traktatu o funkcjonowaniu Unii Europejskiej. Akty delegowane powinny być w szczególności przyjmowane z poszanowaniem zgodności przetwarzania z prawem; określania kryteriów i warunków zgody dziecka, przetwarzania szczególnych kategorii danych; określania kryteriów i warunków wyraźnie przesadnych wniosków i nadmiernych opłat za wykonanie prawa podmiotu danych; kryteriów i wymogów dotyczących informacji przekazywanych podmiotowi danych oraz w zakresie prawa dostępu; prawa do bycia zapomnianym i do usunięcia danych; środków opartych na profilowaniu; kryteriów i wymogów w zakresie odpowiedzialności administratora, uwzględnienia danych już w fazie projektowania oraz ochrony danych jako opcji domyślnej; podmiotu przetwarzającego; kryteriów i wymogów w zakresie dokumentacji oraz bezpieczeństwa przetwarzania; kryteriów i wymogów w zakresie stwierdzenia naruszenia ochrony danych osobowych i zawiadomienia organu nadzorczego oraz warunków, w których naruszenie danych osobowych może niekorzystnie wpłynąć na podmiot danych; kryteriów i warunków operacji przetwarzania wymagających przeprowadzenia oceny skutków w zakresie ochrony danych; kryteriów i wymogów określenia wysokiego stopnia szczególnych zagrożeń, które wymagają uprzedniej konsultacji; wskazania i określenia zadań inspektora ochrony danych; kodeksów postępowania; kryteriów i wymogów w zakresie mechanizmów certyfikacji; kryteriów i wymogów w zakresie przekazywania danych na podstawie wiążących reguł korporacyjnych; odstępstw dotyczących przetwarzania; sankcji administracyjnych; przetwarzania w celach zdrowotnych; przetwarzania w kontekście zatrudnienia oraz przetwarzania do celów badań historycznych, statystycznych i naukowych. Szczególnie ważne jest, aby w czasie swoich prac przygotowawczych Komisja prowadziła stosowne konsultacje, w tym na poziomie ekspertów. W trakcie przygotowywania i opracowywania aktów delegowanych Komisja powinna zapewnić jednoczesne, terminowe i odpowiednie przekazanie stosownych dokumentów Parlamentowi Europejskiemu i Radzie.

(130) Aby zagwarantować jednolite warunki wdrażania niniejszego rozporządzenia, należy powierzyć Komisji uprawnienia wykonawcze w zakresie: opracowania standardowych formularzy w zakresie przetwarzania danych osobowych dziecka; standardowych procedur i formularzy w zakresie wykonywania praw przez podmioty danych; standardowych formularzy służących przekazywaniu informacji podmiotowi danych; standardowych formularzy i procedur dotyczących prawa dostępu; prawa przenoszenia

danych; standardowych formularzy dotyczących odpowiedzialności administratora za uwzględnienie ochrony danych już w fazie projektowania, domyślną ochronę danych oraz dokumentację; szczególnych wymogów w zakresie bezpieczeństwa przetwarzania; standardowego formatu i procedur dotyczących zawiadomienia organu nadzorczego o naruszeniu ochrony danych osobowych oraz przekazywania informacji o naruszeniu ochrony danych osobowych podmiotowi danych; standardów i procedur w zakresie oceny skutków w zakresie ochrony danych; formularzy i procedur dotyczących uprzedniego zezwolenia i uprzedniej konsultacji; technicznych standardów i mechanizmów certyfikacji; odpowiedniego poziomu ochrony przyznanej przez państwo trzecie, na jego terytorium bądź przez sektor, w którym odbywa się przetwarzanie danych w tym państwie trzecim bądź też organizację międzynarodową; ujawnień, na które Unia nie wyraziła zgody; wzajemnej pomocy, wspólnych operacji; decyzji podejmowanych na mocy mechanizmu współpracy. Uprawnienia te powinny być wykonywane zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 182/2011 z dnia 16 lutego 2011 r. ustanawiającym przepisy i zasady ogólne dotyczące trybu kontroli przez państwa członkowskie wykonywania uprawnień wykonawczych przez Komisję[45]. W tym kontekście Komisja powinna rozważyć wprowadzenie szczególnych środków dla mikroprzedsiębiorców oraz małych i średnich przedsiębiorców.

(131) Procedurę sprawdzającą należy stosować w przypadku przyjmowania standardowych formularzy dotyczących zgody dziecka; standardowych procedur i formularzy w zakresie wykonywania praw przez podmioty danych; standardowych formularzy służących przekazywaniu informacji podmiotowi danych; standardowych formularzy i procedur dotyczących prawa dostępu; prawa przenoszenia danych; standardowych formularzy dotyczących odpowiedzialności administratora za uwzględnienie ochrony danych już w fazie projektowania, domyślną ochronę danych oraz dokumentację; szczególnych wymogów w zakresie bezpieczeństwa przetwarzania; standardowego formatu i procedur dotyczących zawiadamiania organu nadzorczego o naruszeniu ochrony danych osobowych oraz przekazywania informacji o naruszeniu ochrony danych osobowych podmiotowi danych; standardów i procedur dotyczących oceny skutków w zakresie ochrony danych; formularzy i procedur dotyczących uprzedniego zezwolenia i uprzedniej konsultacji; technicznych standardów i mechanizmów certyfikacji; odpowiedniego poziomu ochrony przyznanej przez państwo trzecie, terytorium bądź sektor, w którym odbywa się przetwarzanie danych w tym państwie trzecim bądź też organizację międzynarodową; ujawnień, na które Unia nie wyraziła zgody; wzajemnej pomocy; wspólnych operacji; decyzji podejmowanych w ramach mechanizmu zgodności, zważywszy że akty te mają charakter ogólny.

(132) Komisja powinna przyjąć akty wykonawcze mające natychmiastowe zastosowanie, jeśli, w uzasadnionych przypadkach dotyczących państwa trzeciego, terytorium lub sektora, w którym przetwarzane są dane w tym państwie trzecim lub w organizacji międzynarodowej, które nie zapewniają odpowiedniego poziomu ochrony, oraz w odniesieniu do kwestii, o których poinformowały organy nadzorcze w ramach mechanizmu zgodności, jest to uzasadnione szczególnie pilną potrzebą.

---

[45] 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.

(133) Ponieważ cele niniejszego rozporządzenia, mianowicie zapewnienie odpowiedniego poziomu ochrony osób fizycznych i swobodnego przepływu danych w ramach całej Unii, nie mogą zostać osiągnięte w wystarczającym stopniu przez państwa członkowskie, natomiast z uwagi na skalę i skutki proponowanego działania możliwe jest lepsze ich osiągnięcie na szczeblu unijnym, Unia może przyjąć środki zgodnie z zasadą pomocniczości, o której mowa w art. 5 Traktatu o Unii Europejskiej. Zgodnie z zasadą proporcjonalności określoną w tym artykule niniejsze rozporządzenie nie wychodzi poza zakres niezbędny do osiągnięcia tego celu.

(134) Dyrektywa 95/46/WE powinna zostać uchylona niniejszym rozporządzeniem. Decyzje przyjęte przez Komisję oraz zezwolenia wydane przez organy nadzorcze na podstawie dyrektywy 95/46/WE powinny jednak pozostać w mocy.

(135) Niniejsze rozporządzenie powinno mieć zastosowanie do wszystkich kwestii dotyczących ochrony podstawowych praw i wolności w zakresie przetwarzania danych osobowych, które nie podlegają szczególnym obowiązkom służącym realizacji tego samego celu określonego w dyrektywie 2002/58/WE, włączając obowiązki nałożone na administratora oraz prawa osób fizycznych. W celu wyjaśnienia związku między niniejszym rozporządzeniem a dyrektywą 2002/58/WE należy odpowiednio zmienić tę dyrektywę.

(136) W odniesieniu do Islandii i Norwegii, niniejsze rozporządzenie stanowi rozwinięcie przepisów dorobku Schengen w zakresie w jakim ma ono zastosowanie do przetwarzania danych osobowych przez organy zaangażowane we wdrożenie tych przepisów, w rozumieniu Umowy zawartej przez Radę Unii Europejskiej i Republikę Islandii oraz Królestwo Norwegii dotyczącej włączenia tych dwóch państw we wprowadzanie w życie, stosowanie i rozwój dorobku Schengen[46].

(137) W odniesieniu do Szwajcarii, niniejsze rozporządzenie stanowi rozwinięcie przepisów dorobku Schengen w zakresie w jakim ma ono zastosowanie do przetwarzania danych osobowych przez organy zaangażowane we wdrożenie tych przepisów, w rozumieniu Umowy zawartej między Unią Europejską, Wspólnotą Europejską a Konfederacją Szwajcarską w sprawie włączenia Konfederacji Szwajcarskiej we wprowadzanie w życie, stosowanie i rozwój dorobku Schengen[47].

(138) W odniesieniu do Lichtensteinu, niniejsze rozporządzenie stanowi rozwinięcie przepisów dorobku Schengen w zakresie w jakim ma ono zastosowanie do przetwarzania danych osobowych przez organy zaangażowane we wdrożenie tych przepisów, w rozumieniu Protokołu między Unią Europejską, Wspólnotą Europejską, Konfederacją Szwajcarską i Księstwem Liechtensteinu w sprawie przystąpienia Księstwa Liechtensteinu do Umowy między Unią Europejską, Wspólnotą Europejską i Konfederacją Szwajcarską dotyczącej włączenia Konfederacji Szwajcarskiej we wprowadzanie w życie, stosowanie i rozwój dorobku Schengen[48].

(139) Biorąc pod uwagę, jak podkreślił Trybunał Sprawiedliwości Unii Europejskiej, iż prawo do ochrony danych osobowych nie jest prawem bezwzględnym, lecz musi być rozpatrywane w odniesieniu do funkcji, jaką pełni w społeczeństwie i równoważone

---

[46] Dz.U. L 176 z 10.7.1999, s. 36.
[47] Dz.U. L 53 z 27.2.2008, s. 52.
[48] Dz.U. L 160 z 18.6.2011, s. 19.

innymi podstawowymi prawami, zgodnie z zasadą proporcjonalności, niniejsze rozporządzenie respektuje podstawowe prawa i przestrzega zasad uznanych w Karcie praw podstawowych Unii Europejskiej zapisanych w Traktacie, zwłaszcza prawa do poszanowania życia prywatnego i rodzinnego, domu i komunikowania się, prawa do ochrony danych osobowych, wolności myśli, sumienia i religii, wolności wypowiedzi i informacji, wolności prowadzenia działalności gospodarczej, prawa do skutecznego środka ochrony prawnej, rzetelnego procesu sądowego oraz różnorodności kulturowej, religijnej i językowej.

PRZYJMUJĄ NINIEJSZE ROZPORZĄDZENIE:

ROZDZIAŁ I
PRZEPISY OGÓLNE

Artykuł 1
Przedmiot i cele

1. Niniejsze rozporządzenie ustanawia przepisy dotyczące ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz przepisy dotyczące swobodnego przepływu danych osobowych.

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

3. Nie ogranicza się ani nie zakazuje swobodnego przepływu danych osobowych w Unii z powodów związanych z ochroną osób fizycznych w zakresie przetwarzania danych osobowych.

Artykuł 2
Zakres materialny

1. Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych w sposób w całości lub w części zautomatyzowany oraz innych rodzajów przetwarzania danych osobowych, stanowiących część zbioru danych lub mających stanowić część zbioru danych.

2. Niniejsze rozporządzenie nie ma zastosowania do przetwarzania danych osobowych:

   a) w ramach działalności wykraczającej poza zakres prawa Unii, w szczególności dotyczącej bezpieczeństwa narodowego;

   b) przez instytucje, organy i jednostki organizacyjne Unii;

   c) przez państwa członkowskie w wykonywaniu działań wchodzących w zakres rozdziału 2 Traktatu o funkcjonowaniu Unii Europejskiej;

   d) przez osobę fizyczną w celach innych niż zarobkowe w ramach własnych działań o charakterze czysto osobistym lub domowym;

e) przez właściwe organy do celów zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich lub ścigania, albo wykonywania kar kryminalnych.

3. Niniejsze rozporządzenie pozostaje bez uszczerbku dla stosowania dyrektywy 2000/31/WE, w szczególności zasad odpowiedzialności usługodawców będących pośrednikami, o których mowa w art. 12-15 tej dyrektywy.

Artykuł 3
Zakres terytorialny

1. Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych w kontekście działalności prowadzonej w zakładzie administratora lub podmiotu przetwarzającego na terytorium Unii.

2. Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych podmiotów danych mających miejsce zamieszkania w Unii przez administratora niemającego siedziby w Unii, gdy przetwarzanie wiąże się z:

   a) oferowaniem towarów lub usług takim podmiotom danych w Unii, lub

   b) monitorowaniem ich zachowania.

3. Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych przez administratora, który nie ma siedziby na terytorium Unii, lecz w miejscu, w którym na mocy prawa międzynarodowego publicznego ma zastosowanie prawo krajowe państwa członkowskiego.

Artykuł 4
Definicje

Do celów niniejszego rozporządzenia:

(1) „podmiot danych” oznacza zidentyfikowaną osobę fizyczną lub osobę fizyczną, którą można zidentyfikować, bezpośrednio lub pośrednio, za pomocą wszelkich środków, które z rozsądnym prawdopodobieństwem mogą być użyte przez administratora lub inną osobę fizyczną bądź prawną, szczególnie przez odniesienie do numeru identyfikacyjnego, danych dotyczących lokalizacji, identyfikatora online lub przynajmniej jednego czynnika charakterystycznego dla fizycznej, fizjologicznej, genetycznej, umysłowej, ekonomicznej, kulturowej lub społecznej tożsamości tej osoby;

(2) „dane osobowe” oznaczają wszelkie informacje dotyczące podmiotu danych;

(3) „przetwarzanie” oznacza każdą operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych przy pomocy środków zautomatyzowanych lub innych, jak np. zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptacja lub modyfikacja, pobieranie, uzyskiwanie wglądu, wykorzystywanie, ujawnianie poprzez przekazanie,

rozpowszechnianie lub udostępnianie w inny sposób, dopasowywanie lub łączenie, usuwanie lub niszczenie;

(4) „zbiór danych” oznacza każdy zorganizowany zestaw danych osobowych, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany lub rozproszony funkcjonalnie lub geograficznie;

(5) „administrator” oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę organizacyjną lub inny podmiot, który samodzielnie lub wspólnie z innymi organami ustala cele, warunki i sposoby przetwarzania danych osobowych; w przypadkach, w których cele, warunki i sposoby ustalane są prawem Unii lub państwa członkowskiego, administrator lub szczególne kryteria jego wyznaczania mogą zostać określone w prawie Unii lub państwa członkowskiego;

(6) „podmiot przetwarzający” oznacza osobę fizyczną lub prawną, organ publiczny, agencję lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;

(7) „odbiorca” oznacza osobę fizyczną lub prawną, organ publiczny, agencję lub inny podmiot, któremu ujawnia się dane osobowe;

(8) „zgoda podmiotu danych” oznacza dobrowolne, szczególne, świadome i wyraźne oświadczenie woli, przez które podmiot danych, w drodze oświadczenia lub wyraźnego działania potwierdzającego, wyraża zgodę na przetwarzanie dotyczących go danych osobowych;

(9) „naruszenie ochrony danych osobowych” oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub dostępu do danych osobowych przesyłanych, przechowywanych lub przetwarzanych w inny sposób;

(10) „dane genetyczne” oznaczają wszelkie dane dowolnego rodzaju dotyczące charakterystycznych cech osoby fizycznej, odziedziczonych lub nabytych na etapie wczesnego rozwoju prenatalnego;

(11) „dane biometryczne” oznaczają wszelkie dane dotyczące cech fizycznych, fizjologicznych i behawioralnych danej osoby, które umożliwiają jej precyzyjną identyfikację, takie jak wizerunek twarzy lub dane daktyloskopijne;

(12) „dane dotyczące zdrowia” oznaczają wszelkie informacje związane ze zdrowiem fizycznym lub psychicznym danej osoby lub ze świadczeniem usług zdrowotnych na jej rzecz;

(13) „główna siedziba” oznacza, jeśli chodzi o administratora, jego siedzibę w Unii, w której podejmowane są najważniejsze decyzje dotyczące celów, warunków i sposobów przetwarzania danych; jeśli decyzji dotyczących celów, warunków i sposobów przetwarzania danych osobowych nie podejmuje się w Unii, główną siedzibą jest miejsce, w którym odbywa się główna działalność w zakresie przetwarzania w kontekście działalności zakładu administratora w Unii. Jeśli chodzi o podmiot przetwarzający, „główna siedziba” oznacza miejsce, w którym znajduje się jego zarząd w Unii;

(14) „przedstawiciel” oznacza każdą osobę fizyczną lub prawną mającą miejsce zamieszkania lub siedzibę w Unii, wyraźnie wyznaczoną przez administratora, która działa w miejsce administratora i do której organ nadzorczy lub inny podmiot w Unii mogą się zwrócić zamiast do administratora w kwestiach dotyczących obowiązków administratora wynikających z niniejszego rozporządzenia;

(15) „przedsiębiorstwo” oznacza każdy podmiot prowadzący działalność gospodarczą, niezależne od jego formy prawnej, w tym w szczególności osoby fizyczne i prawne, partnerstwa lub zrzeszenia prowadzące regularną działalność gospodarczą;

(16) „grupa przedsiębiorstw” oznacza przedsiębiorstwo sprawujące kontrolę oraz przedsiębiorstwa kontrolowane;

(17) „wiążące reguły korporacyjne” oznaczają polityki ochrony danych osobowych, których przestrzegają administrator lub podmiot przetwarzający mający siedzibę na terytorium państwa członkowskiego Unii do celów przekazywania danych osobowych do administratora lub podmiotu przetwarzającego w przynajmniej jednym państwie trzecim w ramach grupy przedsiębiorstw;

(18) „dziecko” oznacza każdą osobę w wieku poniżej 18 lat;

(19) „organ nadzorczy” oznacza organ publiczny ustanowiony przez państwo członkowskie zgodnie z art. 46.

ROZDZIAŁ II
ZASADY

Artykuł 5
Zasady dotyczące przetwarzania danych osobowych

Dane osobowe muszą być:

a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty w odniesieniu do podmiotu danych;

b) zbierane w konkretnych, bezpośrednich i zgodnych z prawem celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami;

c) prawidłowe, właściwe i ograniczone do minimum niezbędnego w odniesieniu do celów, do których dane są przetwarzane; dane te są przetwarzane jedynie wtedy gdy i tylko przez okres w którym tych celów nie można spełnić przetwarzając informacje, które nie obejmują danych osobowych;

d) ścisłe i, w razie potrzeby, aktualne; należy podjąć wszelkie zasadne działania, by zapewnić niezwłoczne usunięcie lub poprawienie nieścisłych danych osobowych, z uwzględnieniem celów ich przetwarzania;

e) przechowywane w formie umożliwiającej identyfikację podmiotów danych przez czas nie dłuższy niż jest to konieczne do celów, dla których dane są

przetwarzane; dane osobowe mogą być przechowywane przez czas dłuższy pod warunkiem, że będą przetwarzane wyłącznie do celów dokumentacji, statystyki lub badań naukowych zgodnie z przepisami i warunkami, o których mowa w art. 83 oraz pod warunkiem prowadzania okresowej kontroli konieczności dalszego ich przechowywania;

f) przetwarzane pod nadzorem i na odpowiedzialność administratora, który zapewnia i wykazuje zgodność każdej operacji przetwarzania z przepisami niniejszego rozporządzenia.

Artykuł 6
Zgodność z prawem przetwarzania

1. Przetwarzanie danych osobowych jest zgodne z prawem, o ile ma zastosowanie co najmniej jeden z poniższych elementów:

   a) podmiot danych wyraził zgodę na przetwarzanie swoich danych osobowych do jednego lub większej liczby konkretnych celów;

   b) przetwarzanie danych jest konieczne do wykonania umowy, której stroną jest podmiot danych, lub w celu podjęcia działań na żądanie podmiotu danych przed zawarciem umowy;

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

   d) przetwarzanie jest konieczne w celu ochrony żywotnych interesów podmiotów danych;

   e) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub wykonania władzy publicznej powierzonej administratorowi;

   f) przetwarzanie jest konieczne dla celów wynikających ze słusznych interesów realizowanych przez administratora, z wyjątkiem sytuacji, kiedy nadrzędny charakter ma interes podstawowych praw i wolności podmiotu danych, które wymagają ochrony danych osobowych, w szczególności gdy podmiotem danych jest dziecko. Przepisu tego nie stosuje się do przetwarzania realizowanego przez organy publiczne w wykonaniu ich zadań.

2. Przetwarzanie danych osobowych, konieczne do celów dokumentacji, statystyki lub badań naukowych, jest zgodne z prawem, z zastrzeżeniem warunków i gwarancji, o których mowa w art. 83.

3. Podstawa przetwarzania, o której mowa w ust. 1 lit. c) i e), musi być przewidziana w:

   a) prawie Unii; lub

   b) prawie państwa członkowskiego, któremu podlega administrator.

   Prawo państwa członkowskiego musi realizować cel leżący w interesie publicznym lub musi być konieczne do ochrony praw i wolności innych osób, respektować istotę

prawa do ochrony danych osobowych i być proporcjonalne do wyznaczonego słusznego celu.

4. Jeśli cel dalszego przetwarzania nie jest zgodny z celem, dla którego zebrano dane osobowe, przetwarzanie musi opierać się na co najmniej jednej z podstaw prawnych przewidzianych w ust. 1 lit. a)-e). Ma to w szczególności zastosowanie do każdej zmiany ogólnych warunków umowy.

5. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 86 w celu doprecyzowania warunków, o których mowa w ust. 1 lit. f), dla różnych sektorów i sytuacji, w których przetwarza się dane, w tym jeśli chodzi o przetwarzanie danych osobowych dotyczących dziecka.

Artykuł 7
Warunki udzielenia zgody

1. Ciężar udowodnienia zgody podmiotu danych na przetwarzanie jego danych osobowych w określonych celach spoczywa na administratorze.

2. Jeśli zgoda podmiotu danych ma być udzielona w kontekście pisemnego oświadczenia, które dotyczy także innej kwestii, wymóg udzielenia zgody musi zostać przedstawiony w sposób pozwalający wyraźnie odróżnić go od tej innej kwestii.

3. Podmiot danych ma prawo odwołać swoją zgodę w dowolnym momencie. Odwołanie zgody nie ma wpływu na zgodność z prawem przetwarzania opartego na zgodzie przed jej odwołaniem.

4. Zgoda nie stanowi podstawy prawnej przetwarzania w sytuacji poważnej nierówności między podmiotem danych a administratorem.

Artykuł 8
Przetwarzanie danych osobowych dziecka

1. Do celów niniejszego rozporządzenia, w odniesieniu do oferowania usług społeczeństwa informacyjnego bezpośrednio dziecku, przetwarzanie danych osobowych dziecka w wieku poniżej 13 lat jest zgodne z prawem, o ile zgodę na nie wydał lub pozwolił na nie rodzic lub opiekun dziecka. Administrator podejmuje racjonalne starania w celu uzyskania możliwej do zweryfikowania zgody, uwzględniając dostępną technologię.

2. Ustęp 1 nie wpływa na ogólne przepisy prawa umów państw członkowskich, takie jak przepisy dotyczące ważności, zawierania lub skutków umowy wobec dziecka.

3. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 86 w celu doprecyzowania kryteriów i wymogów dotyczących sposobów uzyskania do zweryfikowania zgody, o której mowa w ust. 1. Wykonując to uprawnienie, Komisja rozważa szczególne środki dla mikroprzedsiębiorców oraz małych i średnich przedsiębiorców.

4. Komisja może ustanowić standardowe formularze dotyczące szczególnych form uzyskiwania możliwej do zweryfikowania zgody, o której mowa w ust. 1. Te akty wykonawcze są przyjmowane zgodnie z procedurą sprawdzającą, o której mowa w art. 87 ust. 2.

Artykuł 9

Przetwarzanie szczególnych kategorii danych osobowych

1. Zakazuje się przetwarzania danych osobowych ujawniających rasę lub pochodzenie etniczne, poglądy polityczne, religię lub przekonania, przynależność do związków zawodowych oraz przetwarzania danych genetycznych lub danych dotyczących zdrowia lub seksualności, wyroków skazujących lub powiązanych środków zabezpieczających.

2. Ustęp 1 nie ma zastosowania, w przypadku gdy:

   a) podmiot danych udzielił zgody na przetwarzanie tych danych osobowych, z zastrzeżeniem warunków określonych w art. 7 i 8, z wyjątkiem sytuacji, gdy prawo Unii lub prawo państwa członkowskiego przewiduje, że zakaz, o którym mowa w ust. 1, nie może być uchylony przez podmiot danych; lub

   b) przetwarzanie danych jest konieczne do celów wypełniania obowiązków i wykonania szczególnych uprawnień administratora w dziedzinie prawa pracy, o ile jest to dozwolone przez prawo Unii lub prawo państwa członkowskiego przewidujące odpowiednie gwarancje; lub

   c) przetwarzanie jest niezbędne w celu ochrony żywotnych interesów podmiotu danych lub innej osoby, w przypadku gdy podmiot danych nie jest fizycznie lub prawnie zdolny do wyrażenia zgody;

   d) przetwarzanie jest dokonywane w ramach zgodnej z prawem działalności prowadzonej z zachowaniem odpowiednich gwarancji przez fundację, stowarzyszenie lub inną niezarobkową instytucję o celach politycznych, filozoficznych, religijnych lub związkowych, pod warunkiem że przetwarzanie danych dotyczy wyłącznie członków lub byłych członków tej instytucji lub osób utrzymujących z nią stałe kontakty w związku z jej celami oraz że dane nie będą ujawniane osobom trzecim bez zgody podmiotów danych; lub

   e) przetwarzanie dotyczy danych osobowych, które zostały wyraźnie podane do publicznej wiadomości przez podmiot danych; lub

   f) przetwarzanie jest niezbędne do ustalania, realizacji lub ochrony roszczeń prawnych; lub

   g) przetwarzanie jest niezbędne do wykonania zadania w interesie publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które przewidują odpowiednie środki ochrony słusznych interesów podmiotu danych; lub

   h) przetwarzanie danych dotyczących zdrowia jest niezbędne w celu ochrony zdrowia i z zastrzeżeniem warunków i gwarancji, o których mowa w art. 81; lub

i) przetwarzanie jest niezbędne do celów dokumentacji, statystyki lub badań naukowych, z zastrzeżeniem warunków i gwarancji, o których mowa w art. 83; lub

j) przetwarzanie danych dotyczących wyroków skazujących za przestępstwa lub powiązanych środków zabezpieczających odbywa się pod kontrolą oficjalnego organu lub przetwarzanie jest niezbędne dla wypełnienia obowiązku prawnego lub regulacyjnego, któremu podlega administrator, albo w celu wykonania zadania realizowanego w ważnym interesie publicznym, o ile jest to dozwolone na mocy prawa Unii lub prawa państwa członkowskiego przewidującego odpowiednie gwarancje. Kompletny rejestr wyroków skazujących za przestępstwa jest prowadzony wyłącznie pod nadzorem oficjalnego organu.

3. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 86 w celu doprecyzowania kryteriów, warunków i odpowiednich gwarancji przetwarzania szczególnych kategorii danych osobowych, o których mowa w ust. 1, oraz wyjątków określonych w ust. 2.

Artykuł 10
Przetwarzanie nie umożliwiające identyfikacji

Jeśli dane przetwarzane przez administratora nie umożliwiają mu identyfikacji osoby fizycznej, administrator nie ma obowiązku uzyskania dodatkowych informacji w celu identyfikacji podmiotu danych wyłącznie ze względu na konieczność respektowania przepisu niniejszego rozporządzenia.

ROZDZIAŁ III
PRAWA PODMIOTU DANYCH

SEKCJA 1
PRZEJRZYSTOŚĆ ORAZ TRYBY WYKONYWANIA PRAW

Artykuł 11
Przejrzysta informacja i komunikacja

1. Administrator dysponuje przejrzystymi i łatwo dostępnymi politykami w zakresie przetwarzania danych osobowych i wykonywania praw przez podmioty danych.

2. Administrator przekazuje informacje i komunikaty dotyczące przetwarzania danych osobowych podmiotowi danych w czytelnej formie, w jasnym i prostym języku, dostosowane do potrzeb podmiotu danych, w szczególności w przypadku informacji adresowanych bezpośrednio do dziecka.

Artykuł 12
Procedury i mechanizmy wykonywania praw przez podmiot danych

1. Administrator ustanawia procedury udzielania informacji, o których mowa w art. 14 oraz wykonywania praw przez podmioty danych, o których mowa w art. 13 oraz art.

15-19. Administrator w szczególności zapewnia mechanizmy ułatwiające składanie wniosków o przeprowadzenie czynności, o których mowa w art. 13 oraz art. 15-19. Jeśli przetwarzanie danych odbywa się w sposób zautomatyzowany, administrator zapewnia także możliwość elektronicznego składania wniosków.

2. Administrator informuje podmiot danych, niezwłocznie i najpóźniej w ciągu miesiąca od dnia otrzymania wniosku, o tym, czy zostaną podjęte jakieś działania zgodnie z art. 13 oraz art. 15-19 i udziela żądanych informacji. Okres ten można przedłużyć o miesiąc, jeśli wiele podmiotów danych wykonuje swoje prawa a ich współpraca jest w racjonalnym zakresie niezbędna, by zapobiec konieczności podejmowania przez administratora niepotrzebnych i nieproporcjonalnych wysiłków. Informacji udziela się na piśmie. Jeśli podmiot danych składa wniosek w formie elektronicznej, informacje także przekazywane są w formie elektronicznej, chyba że podmiot danych zażąda informacji w innej formie.

3. Jeśli administrator odmawia podjęcia działania na wniosek podmiotu danych, informuje on ten podmiot o powodach odmowy oraz możliwości zgłoszenia skargi organowi nadzorczemu i skorzystania z sądowego środka ochrony prawnej.

4. Przekazanie informacji i podjęcie działań na podstawie wniosków, o których mowa w ust. 1, są wolne od opłat. Jeśli wnioski są wyraźnie przesadne, w szczególności ze względu na ich powtarzający się charakter, administrator może pobrać opłatę za przekazanie wnioskowanych informacji lub podjęcie żądanego działania lub też może uchylić się od podjęcia żądanego działania. W takim przypadku na administratorze spoczywa ciężar udowodnienia wyraźnie przesadnego charakteru wniosku.

5. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 86 w celu doprecyzowania kryteriów i warunków wyraźnie przesadnego charakteru wniosków oraz pobierania opłat, o których mowa w ust. 4.

6. Komisja może ustanowić standardowe formularze i określić standardowe procedury dotyczące informacji, o których mowa w ust. 2, w tym jeśli chodzi o format elektroniczny. Wykonując to uprawnienie, Komisja podejmuje właściwe środki dla mikroprzedsiębiorców oraz małych i średnich przedsiębiorców. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 87 ust. 2.

Artykuł 13
Prawa odbiorców

Administrator informuje o wszelkich operacjach poprawienia lub usunięcia dokonanych zgodnie z art. 16 i art. 17 każdego odbiorcę, któremu ujawniono dane, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku.

SEKCJA 2
INFORMACJE I DOSTĘP DO DANYCH

Artykuł 14
Informacje przekazywane podmiotowi danych

1. W przypadku zbierania danych osobowych odnoszących się do podmiotu danych, administrator udziela temu podmiotowi co najmniej następujących informacji:

   a) tożsamość i dane kontaktowe administratora oraz ewentualnie przedstawiciela administratora i inspektora ochrony danych;

   b) cele przetwarzania danych, do których dane są przeznaczone, w tym postanowienia umów i warunków ogólnych, jeśli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. b) oraz słuszne interesy realizowane przez administratora, jeśli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f);

   c) okres, przez który dane osobowe będą przechowywane ;

   d) istnienie prawa do wystąpienia do administratora o uzyskanie wglądu do danych, poprawienie ich lub usunięcie danych osobowych odnoszących się do podmiotu danych lub prawo wniesienia sprzeciwu wobec przetwarzania tych danych osobowych;

   e) prawa złożenia skargi organowi nadzorczemu oraz dane kontaktowe organu nadzorczego;

   f) odbiorcy lub kategorie odbiorców danych osobowych;

   g) w stosownych przypadkach, zamiar przekazania danych przez administratora do państwa trzeciego lub organizacji międzynarodowej oraz informacje na temat poziomu ochrony zapewnianego przez to państwo trzecie lub organizację międzynarodową przez odniesienie do decyzji Komisji stwierdzającej odpowiedni poziom ochrony;

   h) wszelkie dalsze informacje potrzebne do zagwarantowania rzetelnego przetwarzania danych w stosunku do podmiotu danych, uwzględniając konkretne okoliczności, w których odbywa się zbieranie danych.

2. W przypadku zbierania danych osobowych od podmiotu danych, administrator, poza przekazaniem informacji, o których mowa w ust. 1, informuje podmiot danych o tym, czy przekazanie danych osobowych jest obowiązkowe czy dobrowolne, a także o ewentualnych skutkach nieprzekazania tych danych.

3. W przypadku zbierania danych osobowych nie od podmiotu danych, administrator, poza przekazaniem informacji, o których mowa w ust. 1, informuje podmiot danych o źródle pochodzenia tych danych osobowych.

4. Administrator udziela informacji, o których mowa w ust. 1, 2 i 3:

   a) w momencie uzyskania danych osobowych od podmiotu danych; lub

b) jeżeli dane osobowe nie są zbierane od podmiotu danych, w momencie ich rejestrowania lub w rozsądnym terminie po zebraniu danych, uwzględniając szczególne okoliczności, w których dane są zbierane lub przetwarzane w inny sposób lub jeśli przewiduje się ujawnienie innemu odbiorcy, najpóźniej w momencie pierwszego ujawnienia danych.

5. Ustępów 1-4 nie stosuje się, w przypadku gdy:

a) podmiot danych dysponuje już informacjami, o których mowa w ust. 1, 2 i 3; lub

b) dane nie są zbierane od podmiotu danych a udzielenie tych informacji okazało się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku; lub

c) dane nie są zbierane od podmiotu danych a rejestrowanie lub ujawnianie ich jest wyraźnie przewidziane przez przepisy prawa; lub

d) dane nie są zbierane od podmiotu danych a udzielenie tych informacji naruszy prawa i wolności osób trzecich określone w prawie Unii lub prawie państw członkowskich, zgodnie z art. 21.

6. W przypadku, o którym mowa w ust. 5 lit. b), administrator zapewnia odpowiednie środki mające na celu ochronę słusznych interesów podmiotu danych.

7. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 86 w celu doprecyzowania kryteriów kategorii odbiorców, o których mowa w ust. 1 lit. f), wymogów dotyczących zawiadomienia o potencjalnym dostępie, o których mowa w ust. 1 lit. g), kryteriów przekazywania dalszych informacji, o których mowa w ust. 1 lit. h), niezbędnych dla niektórych sektorów i w niektórych sytuacjach oraz warunków i odpowiednich gwarancji w przypadku wyjątków określonych w ust. 5 lit. b). Wykonując to uprawnienie, Komisja podejmuje właściwe środki dla mikroprzedsiębiorców oraz małych i średnich przedsiębiorców

8. Komisja może ustanowić standardowe formularze do celów udzielania informacji, o których mowa w ust. 1-3, uwzględniając, w stosownych przypadkach, szczególny charakter i potrzeby różnych sektorów oraz sytuacji przetwarzania danych. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 87 ust. 2.

Artykuł 15

Prawo dostępu przysługujące podmiotowi danych

1. Podmiot danych ma prawo do uzyskania od administratora, na wniosek złożony w dowolnym momencie, potwierdzenia, czy przetwarzane są dane osobowe odnoszące się do niego. W przypadku przetwarzania takich danych osobowych administrator przekazuje następujące informacje:

a) cele przetwarzania;

b) kategorie przedmiotowych danych osobowych;

c) odbiorcy lub kategorie odbiorców, którym dane osobowe mają być lub zostały ujawnione, w szczególności odbiorcy w państwach trzecich;

d) okres przechowywania danych osobowych;

e) istnienie prawa do żądania od administratora poprawienia lub usunięcia danych osobowych odnoszących się do podmiotu danych lub prawa wniesienia sprzeciwu wobec przetwarzania tych danych osobowych;

f) prawa do złożenia organowi nadzorczemu skargi oraz dane kontaktowe organu nadzorczego;

g) przekazanie danych osobowych podlegających przetwarzaniu i wszelkich dostępnych informacji o ich źródle;

h) znaczenie i przewidywane skutki takiego przetwarzania, co najmniej w przypadku środków, o których mowa w art. 20.

2. Podmiot danych ma prawo do uzyskania od administratora informacji na temat danych osobowych podlegających przetwarzaniu. Jeśli podmiot danych składa wniosek w formie elektronicznej, informacje także przekazywane są w formie elektronicznej, chyba że podmiot danych zażąda informacji w innej formie.

3. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 86 w celu doprecyzowania kryteriów i wymogów dotyczących informowania podmiotu danych o treści danych osobowych, o których mowa w ust. 1 lit. g).

4. Komisja może opracować standardowe formularze i procedury w zakresie wnioskowania o dostęp do informacji, o których mowa w ust. 1 oraz udzielania dostępu do tych informacji, w tym w celu weryfikacji tożsamości podmiotu danych oraz przekazywania danych osobowych podmiotowi danych, uwzględniając szczególny charakter i potrzeby różnych sektorów oraz sytuacji przetwarzania danych. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 87 ust. 2.

SEKCJA 3

POPRAWIANIE I USUWANIE

Artykuł 16

Prawo do poprawienia

Podmiot danych ma prawo do uzyskania przez administratora poprawienia nieścisłych danych osobowych, które go dotyczą. Podmiot danych ma prawo do uzyskania uzupełnienia niekompletnych danych osobowych, w tym w drodze sprostowania.

Artykuł 17

Prawo do bycia zapomnianym i do usunięcia danych

1. Podmiot danych ma prawo do uzyskania od administratora usunięcia danych osobowych odnoszących się do niego oraz zaprzestania dalszego rozpowszechniania tych danych, zwłaszcza w odniesieniu do danych osobowych, które zostały udostępnione przez podmiot danych, kiedy był on dzieckiem, jeśli zastosowanie ma jedna z następujących przesłanek:

   a) dane nie są już potrzebne do celów, do których były zebrane lub przetwarzane w inny sposób;

   b) podmiot danych odwołuje zgodę, na której opiera się przetwarzanie zgodnie z art. 6 ust. 1 lit. a), lub gdy minął okres przechowywania, na który wyrażono zgodę oraz jeśli nie ma już podstawy prawnej przetwarzania danych;

   c) podmiot danych sprzeciwia się przetwarzaniu danych osobowych zgodnie z art. 19;

   d) przetwarzanie danych nie jest zgodne z niniejszym rozporządzeniem z innych powodów.

2. W przypadku podania przez administratora, o którym mowa w ust. 1, danych osobowych do wiadomości publicznej, podejmuje on wszelkie uzasadnione kroki, w tym środki techniczne, w odniesieniu do danych, za których publikację odpowiada, by poinformować osoby trzecie przetwarzające takie dane, iż podmiot danych wnioskuje o usunięcie linków do danych, kopii lub replikacji tych danych osobowych. Jeśli administrator upoważnił osobę trzecią do publikacji danych osobowych, uważa się go za odpowiedzialnego za tę publikację.

3. Administrator niezwłocznie usuwa dane, z wyjątkiem w zakresie, w jakim zatrzymanie danych osobowych jest niezbędne:

   a) do wykonywania prawa wolności wypowiedzi zgodnie z art. 80;

   b) w celu realizacji interesu publicznego w dziedzinie zdrowia publicznego zgodnie z art. 81;

   c) do celów dokumentacji, statystyki i badań naukowych zgodnie z art. 83;

   d) dla wypełnienia spoczywającego na administratorze obowiązku prawnego w zakresie zatrzymania danych osobowych, nałożonego przez prawo Unii lub prawo państwa członkowskiego; przepisy prawa państwo członkowskie spełniają cel polegający na realizacji celu publicznego, szanują istotę prawa do ochrony danych osobowych oraz są proporcjonalne do wyznaczonego zgodnego z prawem celu;

   e) w przypadkach określonych w ust. 4.

4. Zamiast usuwania, administrator ogranicza przetwarzanie danych osobowych, jeśli:

a) podmiot danych kwestionuje ich ścisłość, przez czas pozwalający administratorowi na sprawdzenie ścisłości danych;

b) administrator nie potrzebuje już danych osobowych do wykonania swojego zadania, ale muszą być one przechowywane do celów dowodowych;

c) przetwarzanie jest niezgodne z prawem i podmiot danych sprzeciwia się ich usunięciu, wnioskując w zamian o ograniczenie ich wykorzystywania;

d) podmiot danych wnioskuje o przekazanie danych osobowych do innego automatycznego systemu przetwarzania zgodnie z art. 18 ust. 2.

5. Dane osobowe, o których mowa w ust. 4, mogą, z wyjątkiem przechowywania, być przetwarzane wyłącznie do celów dowodowych, bądź też za zgodą podmiotu danych, bądź w celu ochrony praw innej osoby fizycznej lub prawnej bądź w celu realizacji interesu publicznego.

6. Jeżeli przetwarzanie danych osobowych jest ograniczone na mocy ust. 4, administrator informuje podmiot danych przed zniesieniem ograniczenia dotyczącego przetwarzania.

7. Administrator wdraża mechanizmy służące zapewnieniu przestrzegania terminów usunięcia danych osobowych lub okresowego przeglądu dokonywanego w celu ustalenia potrzeby przechowywania danych.

8. W przypadku usunięcia danych, administrator nie przetwarza w inny sposób tych danych osobowych.

9. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 86 w celu doprecyzowania:

a) kryteriów i wymogów stosowania ust. 1 w poszczególnych sektorach oraz w szczególnych sytuacjach przetwarzania danych;

b) warunków usuwania linków do danych, kopii lub replikacji danych osobowych z publicznie dostępnych usług łączności, o których mowa w ust. 2;

c) kryteriów i warunków ograniczania przetwarzania danych osobowych, o których mowa w ust. 4.

Artykuł 18

Prawo przenoszenia danych

1. Podmiot danych ma prawo, jeśli dane osobowe są przetwarzane w sposób elektroniczny oraz w zorganizowanym i powszechnie używanym formacie, do uzyskania od administratora kopii danych podlegających przetwarzaniu w formacie elektronicznym i zorganizowanym, który jest powszechnie używany i umożliwia dalsze wykorzystywanie przez podmiot danych.

2. Jeżeli podmiot danych przekazał dane osobowe a przetwarzanie opiera się na zgodzie lub umowie, podmiot danych ma prawo do przekazania tych danych osobowych i

innych informacji przez siebie przekazanych i przechowywanych w systemie automatycznego przetwarzania danych, do innego systemu, w powszechnie używanym formacie elektronicznym, bez przeszkód ze strony administratora, z którego baz dane osobowe zostają wycofane.

3. Komisja może opracować format elektroniczny, o którym mowa w ust. 1 oraz techniczne standardy, sposoby i procedury przekazywania danych osobowych na mocy ust. 2. Te akty wykonawcze są przyjmowane zgodnie z procedurą sprawdzającą, o której mowa w art. 87 ust. 2.

SEKCJA 4

PRAWO WNIESIENIA SPRZECIWU I PROFILOWANIE

Artykuł 19

Prawo wniesienia sprzeciwu

1. Podmiot danych ma prawo, z przyczyn dotyczących jego szczególnej sytuacji, w dowolnym momencie wnieść sprzeciw wobec przetwarzania danych osobowych opartego na art. 6 ust. 1 lit. d), e) i f), chyba że administrator wykaże ważne i uzasadnione podstawy przetwarzania, które mają charakter nadrzędny wobec interesów lub podstawowych praw i wolności podmiotu danych.

2. Jeżeli dane osobowe są przetwarzane do celów marketingu bezpośredniego, podmiot danych ma prawo nieodpłatnie wnieść sprzeciw wobec przetwarzania jego danych osobowych do takich celów marketingowych. O prawie tym należy wyraźnie poinformować podmiot danych w zrozumiały sposób, tak by informację tę można było łatwo odróżnić od innych informacji

3. W przypadku podtrzymania sprzeciwu na mocy ust. 1 i 2, administrator nie może wykorzystywać ani w inny sposób przetwarzać przedmiotowych danych osobowych,

Artykuł 20

Środki oparte na profilowaniu

1. Każda osoba fizyczna ma prawo nie podlegać środkowi, który wywołuje skutki prawne dotyczące tej osoby fizycznej lub ma istotny wpływ na tę osobę fizyczną, a który opiera się wyłącznie na automatycznym przetwarzaniu danych mającym służyć ocenie niektórych aspektów osobistych tej osoby fizycznej lub też analizie bądź przewidzeniu zwłaszcza wyników w pracy, sytuacji ekonomicznej, miejsca przebywania, zdrowia, preferencji osobistych, wiarygodności lub zachowania tej osoby fizycznej.

2. Z zastrzeżeniem innych przepisów niniejszego rozporządzenia, dana osoba może zostać poddana jednemu ze środków, o których mowa w ust. 1, jedynie wtedy gdy przetwarzanie:

   a) odbywa się w trakcie zawierania lub wykonania umowy, jeśli wniosek w sprawie zawarcia lub wykonania umowy złożony przez podmiot danych został

zrealizowany lub jeśli przewidziano właściwe środki w celu zabezpieczenia słusznych interesów podmiotu danych, jak np. prawo do uzyskania interwencji ze strony człowieka; lub

b) jest wyraźnie dozwolone przez prawo Unii lub państwa członkowskiego, które ustanawia również właściwe środki w celu zabezpieczenia słusznych interesów podmiotu danych; lub

c) odbywa się na podstawie zgody podmiotu danych, z zastrzeżeniem warunków określonych w art. 7 oraz właściwych gwarancji.

3. Automatyczne przetwarzanie danych osobowych, które ma służyć ocenie niektórych aspektów osobistych osoby fizycznej, nie opiera się jedynie na szczególnych kategoriach danych osobowych, o których mowa w art. 9.

4. W przypadkach o których mowa w ust. 2, informacje, które ma przekazać administrator na mocy art. 14, obejmują informacje dotyczące istnienia przetwarzania w drodze środka takiego jak ten, o którym mowa w ust. 1 oraz przewidywanego wpływu tego przetwarzania na podmiot danych.

5. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 86 w celu doprecyzowania kryteriów i warunków odpowiednich środków służących zabezpieczeniu słusznych interesów podmiotu danych, o których mowa w ust. 2.

SEKCJA 5
OGRANICZENIA

Artykuł 21
Ograniczenia

1. Unia lub państwo członkowskie mogą, w drodze środka ustawodawczego, ograniczyć zakres obowiązków i praw przewidzianych w art. 5 lit. a)-e), art. 11-20 i art. 32, gdy takie ograniczenie stanowi konieczny i proporcjonalny środek w demokratycznym społeczeństwie, służący:

a) zagwarantowaniu bezpieczeństwa publicznego;

b) zapewnieniu zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich lub ścigania;

c) zabezpieczeniu innych interesów publicznych Unii lub państwa członkowskiego, w szczególności ważnego interesu gospodarczego lub finansowego Unii lub państwa członkowskiego, w tym kwestii pieniężnych, budżetowych i podatkowych oraz ochrony stabilności i integralności rynku;

d) zapewnieniu zapobiegania naruszeniom zasad etyki w zawodach podlegających regulacji, prowadzenia dochodzeń w tych sprawach, wykrywania i ścigania tych naruszeń;

e) zapewnieniu funkcji kontrolnych, inspekcyjnych i regulacyjnych związanych, nawet sporadycznie, z wykonywaniem władzy publicznej w przypadkach, o których mowa w lit. a), b) c) i d);

f) ochronie podmiotu danych lub praw i wolności innych osób.

2. Środek ustawodawczy, o którym mowa w ust. 1, zawiera przepisy szczególne dotyczące przynajmniej celów przetwarzania oraz wyznaczenia administratora.

ROZDZIAŁ IV
ADMINISTRATOR I PODMIOT PRZETWARZAJĄCY

SEKCJA 1
OBOWIĄZKI OGÓLNE

Artykuł 22
Odpowiedzialność administratora ○

1. Administrator przyjmuje polityki i realizuje odpowiednie środki w celu zapewnienia, by przetwarzanie danych osobowych odbywało się zgodnie z niniejszym rozporządzeniem oraz wykazania tej zgodności.

2. Środki przewidziane w ust. 1 obejmują w szczególności:

a) prowadzenie dokumentacji zgodnie z art. 28;

b) realizację wymogów bezpieczeństwa danych ustanowionych w art. 30;

c) dokonywanie oceny skutków w zakresie ochrony danych zgodnie z art. 33;

d) spełnianie wymogu uprzedniego uzyskania zezwolenia organu nadzorczego lub uprzedniej konsultacji z tym organem zgodnie z art. 34 ust. 1 i 2;

e) wyznaczenie inspektora ochrony danych zgodnie z art. 35 ust. 1.

3. Administrator wdraża mechanizmy służące zapewnieniu weryfikacji skuteczności środków, o których mowa w ust. 1 i 2. Jeśli jest to proporcjonalne, weryfikacja ta przeprowadzona jest przez niezależnych audytorów wewnętrznych lub zewnętrznych.

4. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 86 w celu określenia dalszych kryteriów i wymogów dotyczących właściwych środków, o których mowa w ust. 1, innych niż te omówione w ust. 2, warunków mechanizmów weryfikacji i audytu, o których mowa w ust. 3, a także kryteriów proporcjonalności zgodnie z ust. 3, oraz rozważenia szczególnych środków dla mikroprzedsiębiorców oraz małych i średnich przedsiębiorców.

Artykuł 23

Uwzględnienie ochrony danych już w fazie projektowania oraz ochrona danych jako opcja domyślna

1. Uwzględniając najnowsze osiągnięcia techniczne oraz koszty wdrożenia, administrator, zarówno w momencie ustalania środków niezbędnych do przetwarzania, jak i w momencie samego przetwarzania, wdraża odpowiednie środki i procedury techniczne i organizacyjne, tak by przetwarzanie odpowiadało wymogom niniejszego rozporządzenia oraz gwarantowało ochronę praw podmiotu danych.

2. Administrator wdraża mechanizmy służące zapewnieniu, by domyślnie przetwarzane były jedynie te dane osobowe, które są niezbędne dla realizacji każdorazowego szczególnego celu przetwarzania oraz by w szczególności nie były one zbierane lub zatrzymywane dłużej niż przez okres niezbędny do realizacji tych celów, zarówno jeśli chodzi o ilość danych, jak i okres ich przechowywania. Mechanizmy te zapewniają w szczególności, by dane osobowe nie były domyślnie udostępniane nieograniczonej liczbie osób.

3. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 86 w celu określenia dalszych kryteriów i wymogów dotyczących właściwych środków i mechanizmów, o których mowa w ust. 1 i 2, w szczególności wymogów w zakresie uwzględnienia ochrony danych już w fazie projektowania w odniesieniu do sektorów, produktów i usług.

4. Komisja może ustanowić standardy techniczne dotyczące wymogów ustanowionych w ust. 1 i 2. Te akty wykonawcze są przyjmowane zgodnie z procedurą sprawdzającą, o której mowa w art. 87 ust. 2.

Artykuł 24

Współadministratorzy

Jeśli administrator określa cele, warunki i środki przetwarzania danych osobowych wspólnie z innymi administratorami, współadministratorzy danych ustalają zakres odpowiedzialności za zgodność z obowiązkami wynikającymi z niniejszego rozporządzenia spoczywającej na każdym z nich, w szczególności jeśli chodzi o procedury i mechanizmy wykonania praw podmiotu danych, w drodze wspólnych ustaleń.

Artykuł 25

Przedstawiciele administratorów nie mających siedziby w Unii

1. W sytuacji, o której mowa w art. 3 ust. 2, administrator wyznacza swojego przedstawiciela na terytorium Unii.

2. Obowiązku tego nie stosuje się do:

   a) administratora mającego siedzibę w państwie trzecim, jeśli Komisja zdecydowała, iż dane państwo trzecie zapewnia odpowiedni poziom ochrony zgodnie z art. 41; lub

b) przedsiębiorstwa zatrudniającego mniej niż 250 osób; lub

c) organu lub podmiotu publicznego; lub

d) administratora jedynie sporadycznie oferującego towary lub usługi podmiotom danych mającym miejsce zamieszkania na terytorium Unii.

3. Przedstawiciel ma siedzibę w jednym z państw członkowskich, w którym mają miejsce zamieszkania podmioty danych i których dane osobowe są przetwarzane w związku z oferowaniem im towarów lub których zachowanie jest monitorowane.

4. Wyznaczenie przedstawiciela przez administratora pozostaje bez uszczerbku dla postępowań sądowych, które można by wszcząć przeciwko samemu administratorowi.

Artykuł 26
Podmiot przetwarzający

1. Jeśli operacja przetwarzania jest realizowana w imieniu administratora, administrator wybiera podmiot przetwarzający dający wystarczające gwarancje wdrożenia odpowiednich środków i procedur technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom niniejszego rozporządzenia i gwarantowało ochronę praw podmiotów danych, w szczególności jeśli chodzi o techniczne środki bezpieczeństwa i środki organizacyjne regulujące przetwarzanie, które ma być prowadzone, oraz zapewnia zgodność z tym środkami.

2. Przetwarzanie przez podmiot przetwarzający jest regulowane umową lub innym aktem prawnym wiążącym podmiot przetwarzający z administratorem i stanowiącym w szczególności, że podmiot przetwarzający:

a) działa wyłącznie na polecenie administratora, w szczególności gdy przekazywanie danych osobowych jest zakazane;

b) zatrudnia wyłącznie personel, który zobowiązał się do zachowania poufności lub na którym spoczywa ustawowy obowiązek zachowania poufności;

c) podejmuje wszelkie wymagane środki na mocy art. 30;

d) zatrudnia inny podmiot przetwarzający jedynie za uprzednią zgodą administratora;

e) o ile to możliwe ze względu na charakter przetwarzania, opracowuje w porozumieniu z administratorem niezbędne techniczne i organizacyjne wymogi wykonania przez administratora spoczywającego na nim obowiązku odpowiedzi na wniosek dotyczących wykonania przez podmiot danych praw ustanowionych w rozdziale III;

f) pomaga administratorowi zapewnić zgodność z obowiązkami określonymi w art. 30-34;

g) przekazuje całość wyników administratorowi po zakończeniu przetwarzania i nie przetwarza danych osobowych w inny sposób;

h) udostępnia administratorowi i organowi nadzorczemu wszelkie informacje niezbędne dla kontroli zgodności z obowiązkami określonymi w tym artykule.

3. Administrator i podmiot przetwarzający sporządzają pisemną dokumentację zaleceń administratora i obowiązków podmiotu przetwarzającego, o których mowa w ust. 2.

4. Jeśli podmiot przetwarzający przetwarza dane osobowe inne, niż te, których przetwarzanie zlecił administrator, podmiot przetwarzający jest uważany za administratora w zakresie tego przetwarzania i podlega przepisom dotyczącym współadministratorów ustanowionym w art. 24.

5. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 86 w celu doprecyzowania kryteriów i wymogów dotyczących zakresu odpowiedzialności, obowiązków i zadań w odniesieniu do podmiotu przetwarzającego zgodnie z ust. 1, oraz warunków, które umożliwiają uproszczenie przetwarzania danych osobowych w ramach grupy przedsiębiorstw, w szczególności do celów kontroli i sprawozdawczości.

Artykuł 27

Przetwarzanie z upoważnienia administratora i podmiotu przetwarzającego

Podmiot przetwarzający oraz każda osoba działająca z upoważnienia administratora lub podmiotu przetwarzającego, która ma dostęp do danych osobowych, przetwarzają je tylko na polecenie administratora, lub gdy wymaga tego prawo Unii lub państwa członkowskiego.

Artykuł 28

Dokumentacja

1. Każdy administrator i podmiot przetwarzający oraz ewentualnie przedstawiciel administratora prowadzą dokumentację wszystkich operacji przetwarzania, za które są odpowiedzialni.

2. Dokumentacja zawiera przynajmniej informacje na temat:

a) imienia i nazwiska/nazwy oraz danych kontaktowych administratora lub współadministratora albo podmiotu przetwarzającego oraz ewentualnego przedstawiciela;

b) imienia i nazwiska/nazwy oraz danych kontaktowych ewentualnego inspektora ochrony danych;

c) celów przetwarzania, w tym słusznych interesów realizowanych przez administratora, jeśli przetwarzanie opiera się na art. 6 ust. 1 lit. f);

d) opisu kategorii podmiotów danych oraz kategorii danych osobowych odnoszących się do nich;

e) odbiorców lub kategorii odbiorców danych osobowych, w tym administratorów, którym ujawniane są dane osobowe na potrzeby realizacji słusznych interesów będących ich celem;

f) w odpowiednich przypadkach, przekazywania danych do państw trzecich lub organizacji międzynarodowych, w tym identyfikacji tego państwa trzeciego lub organizacji międzynarodowej oraz, w przypadku przekazywania, o którym mowa w art. 44 ust. 1 lit. h), dokumentacji dotyczącej odpowiednich gwarancji;

g) ogólnego wskazania terminów usunięcia różnych kategorii danych;

h) opisu mechanizmów, o których mowa w art. 22 ust. 3.

3. Administrator i podmiot przetwarzający oraz ewentualny przedstawiciel administratora udostępniają dokumentację organowi nadzorczemu na jego wniosek.

4. Obowiązków, o których mowa w ust. 1 i 2, nie stosuje się do następujących administratorów i podmiotów przetwarzających:

a) osoby fizycznej przetwarzającej dane osobowe w celu innym niż handlowy; lub

b) przedsiębiorstwa lub organizacji zatrudniających mniej niż 250 osób, którzy przetwarzają dane osobowe jedynie w ramach działalności pobocznej w stosunku do działalności głównej.

5. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 86 w celu doprecyzowania kryteriów i wymogów dotyczących dokumentacji, o której mowa w ust. 1, by uwzględnić w szczególności zakres odpowiedzialności administratora i podmiotu przetwarzającego oraz ewentualnie przedstawiciela administratora.

6. Komisja może ustanowić standardowe formularze dotyczące dokumentacji, o której mowa w ust. 1. Te akty wykonawcze są przyjmowane zgodnie z procedurą sprawdzającą, o której mowa w art. 87 ust. 2.

Artykuł 29

Współpraca z organem nadzorczym

1. Administrator i podmiot przetwarzający oraz ewentualnie przedstawiciel administratora współpracują z organem nadzorczym na jego wniosek w zakresie wykonania swoich zadań, w szczególności poprzez przekazywanie informacji, o których mowa w art. 53 ust. 2 lit. a) oraz udzielanie dostępu w myśl lit. b) tego ustępu.

2. Administrator i podmiot przetwarzający udzielają odpowiedzi na zapytanie organu nadzorczego wykonującego uprawnienia przekazane mu na podstawie art. 53 ust. 2 w rozsądnym terminie, wskazanym przez ten organ. Odpowiedź na uwagi organu nadzorczego zawiera opis podjętych środków i osiągniętych wyników

SEKCJA 2
BEZPIECZEŃSTWO DANYCH

Artykuł 30
Bezpieczeństwo przetwarzania

1. Administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, by zapewnić poziom bezpieczeństwa stosowny do ryzyk związanych z przetwarzaniem oraz charakterem danych osobowych, które należy chronić, uwzględniając najnowsze osiągnięcia techniczne oraz koszty ich wdrożenia.

2. Administrator i podmiot przetwarzający, po dokonaniu oceny ryzyk, podejmują środki, o których mowa w ust. 1, by chronić dane osobowe przed ich przypadkowym lub niezgodnym z prawem zniszczeniem bądź przypadkową utratą oraz by zapobiec wszelkim innym formom niezgodnego z prawem przetwarzania, w szczególności nieuprawnionemu ujawnieniu, rozpowszechnieniu, dostępowi lub zmianie danych osobowych.

3. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 86 w celu doprecyzowania kryteriów i warunków dotyczących środków technicznych i organizacyjnych, o których mowa w ust. 1 i 2, w tym zdefiniowania pojęcia najnowszych osiągnięć technicznych, dla konkretnych sektorów oraz w konkretnych sytuacjach przetwarzania danych, uwzględniając w szczególności rozwój technologii oraz rozwiązania w zakresie uwzględnienia ochrony prywatności już w fazie projektowania oraz ochrony danych jako opcji domyślnej, chyba że zastosowanie ma ust. 4.

4. Komisja może przyjąć, w razie potrzeby, akty wykonawcze mające na celu sprecyzowanie wymogów ustanowionych w ust. 1 i 2 obowiązujących w różnych sytuacjach, w szczególności w celu:

   a) zapobiegania wszelkiemu nieuprawnionemu dostępowi do danych osobowych;

   b) zapobiegania nieuprawnionemu ujawnianiu, odczytywaniu, kopiowaniu, zmienianiu lub usuwaniu danych osobowych;

   c) zapewnienia weryfikacji zgodności z prawem operacji przetwarzania.

   Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 87 ust. 2.

Artykuł 31
Zgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu

1. W przypadku naruszenia ochrony danych osobowych, administrator zgłasza organowi nadzorczemu takie naruszeniu bez nieuzasadnionej zwłoki i jeśli jest to możliwe, nie później niż w ciągu 24 godzin od momentu dowiedzenia się o tym naruszeniu. Jeśli organ nadzorczy nie zostanie zawiadomiony w ciągu 24 godzin, do zgłoszenia należy dołączyć umotywowane wyjaśnienie.

2. Na mocy art. 26 ust. 2 lit. f) podmiot przetwarzający ostrzega i informuje administratora niezwłocznie po stwierdzeniu naruszenia ochrony danych osobowych.

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

   a) opisywać charakter naruszenia ochrony danych osobowych, w tym podawać kategorie i liczbę zainteresowanych podmiotów danych oraz kategorie i liczbę rekordów danych, których dotyczy naruszenie;

   b) podawać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub innego punktu kontaktowego, w którym można uzyskać więcej informacji;

   c) zalecać środki mające na celu zmniejszenie ewentualnych negatywnych skutków naruszenia ochrony danych osobowych;

   d) opisywać konsekwencje naruszenia ochrony danych;

   e) opisywać środki proponowane lub podjęte przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych.

4. Administrator sporządza dokumentację dotyczącą wszelkich naruszeń ochrony danych osobowych, obejmującą okoliczności naruszenia, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi umożliwiać organowi nadzorczemu sprawdzenie zgodności z niniejszym artykułem. Dokumentacja zawiera wyłącznie informacje niezbędne do realizacji powyższego celu.

5. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 86 w celu doprecyzowania kryteriów i wymogów dotyczących stwierdzenia naruszenia ochrony danych osobowych, o którym mowa w ust. 1 i 2, oraz szczególnych okoliczności, w których administrator i podmiot przetwarzający mają obowiązek zgłosić naruszenie ochrony danych osobowych.

6. Komisja może ustanowić standardowe formularze zgłoszenia przekazywanego organowi nadzorczemu, procedury mające zastosowanie do wymogu zgłoszenia, a także formę i sposób prowadzenia dokumentacji, o której mowa w art. 4, w tym terminy usuwania zawartych w niej informacji. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 87 ust. 2.

Artykuł 32

Zawiadomienie podmiotu danych o naruszeniu ochrony danych osobowych

1. Gdy istnieje prawdopodobieństwo, że naruszenie ochrony danych osobowych może niekorzystnie wpłynąć na ochronę danych osobowych lub prywatność podmiotu danych, administrator, po dokonaniu zgłoszenia, o którym mowa w art. 31, bez nieuzasadnionej zwłoki informuje podmiot danych o naruszeniu ochrony danych osobowych.

2. Zawiadomienie przekazane podmiotowi danych, o którym mowa w ust. 1, opisuje charakter naruszenia ochrony danych osobowych i zawiera przynajmniej informacje i zalecenia, o których mowa w art. 31 ust. 3 lit. b) i c).

3. Zawiadomienie podmiotu danych o naruszeniu ochrony danych osobowych nie jest wymagane, jeśli administrator wykaże, zgodnie z wymogami organu nadzorczego, że wdrożył odpowiednie technologiczne środki ochrony oraz że środki te zostały zastosowane do danych, których dotyczyło naruszenie ochrony danych osobowych. Tego rodzaju technologiczne środki ochrony sprawiają, że dane stają się nieczytelne dla każdego, kto nie jest uprawniony do dostępu do nich.

4. Bez uszczerbku dla obowiązku administratora w zakresie zawiadomienia podmiotu danych o naruszeniu ochrony danych osobowych, jeśli administrator nie zawiadomił wcześniej podmiotu danych o naruszeniu ochrony danych osobowych, organ nadzorczy może tego od niego zażądać, jeśli stwierdzi możliwość wystąpienia niekorzystnych skutków naruszenia.

5. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 86 w celu doprecyzowania kryteriów i wymogów dotyczących okoliczności, w których naruszenie ochrony danych osobowych może niekorzystnie wpłynąć na dane osobowe, o których mowa w ust. 1.

6. Komisja może określić format zawiadomienia przekazywanego podmiotowi danych, o którym mowa w ust. 1, oraz procedury mające zastosowanie do tego zawiadomienia. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 87 ust. 2.

SEKCJA 3
OCENA SKUTKÓW W ZAKRESIE OCHRONY DANYCH I UPRZEDNIE ZEZWOLENIE

Artykuł 33
Ocena skutków w zakresie ochrony danych

1. Jeśli operacje przetwarzania stwarzają szczególne ryzyko dla praw i wolności podmiotów danych z racji swego charakteru, zakresu lub celów, administrator lub podmiot przetwarzający przeprowadzają w imieniu administratora danych ocenę skutków przewidywanych operacji przetwarzania w zakresie ochrony danych osobowych.

2. Szczególne ryzyko, o którym mowa w ust. 1, stwarzają w szczególności następujące operacje przetwarzania:

   a) systematyczna i kompleksowa ocena aspektów osobowych osoby fizycznej bądź operacje przetwarzania mające na celu analizę lub przewidzenie w szczególności sytuacji ekonomicznej, miejsca pobytu, stanu zdrowia, preferencji osobistych, wiarygodności lub zachowania osoby fizycznej, która opiera się na automatycznym przetwarzaniu, i na której opierają się środki, które wywołują skutki prawne dotyczące danej osoby lub mają na nią istotny wpływ;

   b) przetwarzanie informacji na temat życia seksualnego, stanu zdrowia, rasy i pochodzenia etnicznego oraz świadczenia usług opieki zdrowotnej, badań epidemiologicznych lub badań mających na celu wykrycie chorób

psychicznych bądź zakaźnych, jeśli dane są przetwarzane w celu podjęcia na szeroką skalę środków lub decyzji dotyczących konkretnych osób;

c) monitorowanie publicznie dostępnych miejsc, zwłaszcza przy wykorzystaniu urządzeń optyczno-elektronicznych (wideonadzór) na szeroką skalę;

d) przetwarzanie danych osobowych w wielkoskalowych zbiorach danych dotyczących dzieci, danych genetycznych lub biometrycznych;

e) inne operacje przetwarzania, które na mocy art. 34 ust. 2 lit. b) wymagają konsultacji z organem nadzorczym.

3. Ocena obejmuje przynajmniej ogólny opis przewidywanych operacji przetwarzania, ocenę ryzyk dla praw i wolności podmiotów danych, środki przewidywane w celu sprostania ryzykom, gwarancje, środki i mechanizmy bezpieczeństwa mające zagwarantować ochronę danych osobowych oraz wykazać zgodność z niniejszym rozporządzeniem, uwzględniając prawa i słuszne interesy podmiotów danych i innych zainteresowanych osób.

4. Administrator zwraca się o opinie do podmiotów danych lub ich przedstawicieli w zakresie planowanego przetwarzania, bez uszczerbku dla ochrony handlowych lub publicznych interesów lub bezpieczeństwa operacji przetwarzania.

5. Jeśli administrator jest organem lub podmiotem publicznym i jeśli przetwarzanie wynika z obowiązku prawnego na mocy art. 6 ust. 1 lit. c) przewidującego zasady i procedury operacji przetwarzania przewidziane przez prawo Unii, ust. 1-4 nie stosuje się, chyba że państwa członkowskie uznają przeprowadzenie takiej oceny przed przetwarzaniem za niezbędne.

6. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 86 w celu doprecyzowania kryteriów i warunków operacji przetwarzania mogących stwarzać szczególne ryzyko, o którym mowa w ust. 1 i 2 oraz wymogów w zakresie oceny, o których mowa w ust. 3, w tym warunków skalowalności, weryfikowalności i sprawdzenia. Wykonując to uprawnienie, Komisja rozważa szczególne środki dla mikroprzedsiębiorców oraz małych i średnich przedsiębiorców.

7. Komisja może określić standardy i procedury przeprowadzania, weryfikowania i kontroli oceny, o której mowa w 3. Te akty wykonawcze są przyjmowane zgodnie z procedurą sprawdzającą, o której mowa w art. 87 ust. 2.

Artykuł 34

Uprzednie zezwolenie i uprzednia konsultacja

1. Administrator lub podmiot przetwarzający, w zależności od przypadku, uzyskują zezwolenie organu nadzorczego przed przetwarzaniem danych osobowych, by zapewnić zgodność planowanego przetwarzania z niniejszym rozporządzeniem, w szczególności by złagodzić ryzyko dla podmiotów danych, jeśli administrator lub podmiot przetwarzający przyjmą klauzule umowne przewidziane w art. 42 ust. 2 lit. d) lub nie wprowadzą odpowiednich gwarancji do prawnie wiążących instrumentów, o których mowa w art. 42 ust. 5, dotyczących przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej.

2. Administrator lub podmiot przetwarzający działający w imieniu administratora przeprowadzają konsultacje z organem nadzorczym przed przetwarzaniem danych, by zapewnić zgodność planowanego przetwarzania z niniejszym rozporządzeniem, w szczególności by załagodzić związane z tym ryzyko dla podmiotu danych, jeśli:

   a) ocena skutków ochrony danych przewidziana w art. 33 wskazuje, że operacje przetwarzania danych mogą, ze względu na swój charakter, zakres lub cele, wiązać się z wysokim poziomem szczególnych ryzyk; lub

   b) organ nadzorczy uzna za niezbędne przeprowadzenie uprzedniej konsultacji na temat operacji przetwarzania mogących stanowić szczególne ryzyko dla praw i wolności podmiotów danych ze względu na swój charakter, zakres lub cele, określonych w ust. 4.

3. Jeśli w opinii organu nadzorczego planowane przetwarzanie nie jest zgodne z niniejszym rozporządzeniem, w szczególności jeśli ryzyka nie zostały dostatecznie zidentyfikowane lub złagodzone, zakazuje planowanego przetwarzania i występuje z odpowiednimi propozycjami mającymi na celu zniwelowanie braku zgodności.

4. Organ nadzorczy ustanawia i udostępnia publicznie wykaz operacji przetwarzania, w przypadku których wymagana jest uprzednia konsultacja na mocy ust. 2 lit. b). Organ nadzorczy przekazuje następnie takie wykazy Europejskiej Radzie Ochrony Danych.

5. Jeśli wykaz, o którym mowa w ust. 4, obejmuje przetwarzanie związane z oferowaniem towarów lub usług podmiotom danych w wielu państwach członkowskich, lub z monitorowaniem ich zachowania, bądź może w sposób istotny wpłynąć na swobodny przepływ danych osobowych na terytorium Unii, organ nadzorczy stosuje mechanizm zgodności, o którym mowa w art. 57, przed przyjęciem takiego wykazu.

6. Administrator lub podmiot przetwarzający przekazują organowi nadzorczemu ocenę skutków w zakresie ochrony danych, o której mowa w art. 33 oraz, na żądanie, wszelkie inne informacje mogące umożliwić organowi nadzorczemu ocenę zgodności przetwarzania, w szczególności ryzyk dla ochrony danych osobowych podmiotu danych oraz powiązanych gwarancji.

7. Państwa członkowskie przeprowadzają z organem nadzorczym konsultacje w toku opracowywania środka ustawodawczego, który ma być przyjęty przez parlament narodowy lub środka opartego na tym środku ustawodawczym, który definiuje charakter przetwarzania, by zapewnić zgodność zamierzonego przetwarzania z niniejszym rozporządzeniem, w szczególności by załagodzić ryzyka dla podmiotów danych.

8. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 86 w celu doprecyzowania kryteriów i warunków ustalenia wysokiego poziomu szczególnych ryzyk, o których mowa w ust. 2 lit. a).

9. Komisja może opracować standardowe formularze i procedury dotyczące uprzedniego zezwolenia oraz uprzedniej konsultacji, o których mowa w ust. 1 i 2, oraz standardowe formularze i procedury dotyczące informowania organu

nadzorczego na mocy ust. 6. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 87 ust. 2.

SEKCJA 4
INSPEKTOR OCHRONY DANYCH

Artykuł 35
Wyznaczenie inspektora ochrony danych

1. Administrator i podmiot przetwarzający wyznaczają inspektora ochrony danych, w każdym przypadku, w którym:

   a) przetwarzania dokonuje organ lub podmiot publiczny; lub

   b) przetwarzania dokonuje przedsiębiorstwo zatrudniające 250 osób lub więcej; lub

   c) główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania podmiotów danych.

2. W przypadku, o którym mowa w ust. 1 lit. b), grupa przedsiębiorstw może wyznaczyć jednego inspektora ochrony danych.

3. Jeśli administrator lub podmiot przetwarzający są organem lub podmiotem publicznym, inspektor ochrony danych może być wyznaczony dla szeregu jego jednostek organizacyjnych, z uwzględnieniem struktury organizacyjnej organu lub podmiotu publicznego.

4. W przypadkach innych niż te, o których mowa w ust. 1, administrator, podmiot przetwarzający, zrzeszenia lub inne podmioty reprezentujące różne kategorie administratorów lub podmiotów przetwarzających mogą wyznaczyć jednego inspektora ochrony danych.

5. Administrator lub podmiot przetwarzający wyznaczają inspektora ochrony danych na podstawie jego kwalifikacji zawodowych oraz w szczególności jego wiedzy specjalistycznej z zakresu prawa ochrony danych, praktyki i zdolności do wykonywania zadań, o których mowa w art. 37. Niezbędny poziom wiedzy specjalistycznej ustala się w szczególności zgodnie z prowadzonym przetwarzaniem danych oraz ochroną wymaganą dla danych osobowych przetwarzanych przez administratora lub podmiot przetwarzający.

6. Administrator lub podmiot przetwarzający gwarantują, by inne obowiązki zawodowe inspektora ochrony danych były zgodne z zadaniami i obowiązkami tej osoby jako inspektora ochrony danych i by nie skutkowały one konfliktem interesów.

7. Administrator lub podmiot przetwarzający wyznaczają inspektora ochrony danych na okres co najmniej dwóch lat. Inspektor ochrony danych może być powoływany na kolejne kadencje. Inspektora ochrony danych można odwołać w czasie trwania kadencji jedynie wtedy, gdy przestał spełniać warunki niezbędne do pełnienia przez niego obowiązków.

8. Inspektor ochrony danych może być zatrudniony przez administratora lub podmiot przetwarzający lub wykonywać swoje zadania na podstawie umowy o świadczenie usług.

9. Administrator lub podmiot przetwarzający informują organ nadzorczy oraz opinię publiczną o imieniu i nazwisku oraz danych kontaktowych inspektora ochrony danych.

10. Podmioty danych mają prawo kontaktować się z inspektorem ochrony danych we wszystkich kwestiach związanych z przetwarzaniem swoich danych oraz wnioskować o możliwość wykonania praw przysługujących im na mocy niniejszego rozporządzenia.

11. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 86 w celu doprecyzowania kryteriów i wymogów dotyczących głównej działalności administratora lub podmiotu przetwarzającego, o której mowa w ust. 1 lit. c) oraz kryteriów dotyczących kwalifikacji zawodowych inspektora ochrony danych, o których mowa w ust. 5.

Artykuł 36

Status inspektora ochrony danych

1. Administrator lub podmiot przetwarzający dopilnowują, by inspektor ochrony danych był właściwie i terminowo włączany we wszystkie kwestie dotyczące ochrony danych osobowych.

2. Administrator i podmiot przetwarzający dopilnowują, by inspektor ochrony danych wykonywał swoje obowiązki i zadania niezależnie i nie otrzymywał żadnych poleceń dotyczących pełnienia swojej funkcji. Inspektor ochrony danych podlega bezpośrednio kierownictwu administratora lub podmiotu przetwarzającego.

3. Administrator lub podmiot przetwarzający wspierają inspektora ochrony danych w wykonywaniu przez niego zadań i zapewniają personel, pomieszczenia, sprzęt i zasoby niezbędne do wykonywania obowiązków i zadań, o których mowa w art. 37.

Artykuł 37

Zadania inspektora ochrony danych

1. Administrator lub podmiot przetwarzający powierzają inspektorowi ochrony danych przynajmniej poniższe zadania:

   a) informowanie administratora lub podmiotu przetwarzającego o ich obowiązkach wynikających z niniejszego rozporządzenia oraz dokumentowanie tej działalności i uzyskiwanych odpowiedzi;

   b) monitorowanie wykonania i stosowania polityk administratora lub podmiotu przetwarzającego w zakresie ochrony danych osobowych, w tym przydział obowiązków, szkolenie personelu zaangażowanego w operacje przetwarzania oraz powiązane kontrole;

c) monitorowanie wykonania i stosowania niniejszego rozporządzenia, w szczególności jeśli chodzi o wymogi dotyczące uwzględnienia ochrony danych już w fazie projektowania, ochrony danych jako opcji domyślnej i bezpieczeństwa danych oraz informowania podmiotów danych, a także wniosków w ramach wykonywania praw przysługujących im na mocy niniejszego rozporządzenia.

d) zapewnienie prowadzenia dokumentacji, o której mowa w art. 28;

e) monitorowanie dokumentacji, zgłoszeń i zawiadomień dotyczących naruszeń ochrony danych osobowych na mocy art. 31 i 32;

f) monitorowanie przeprowadzenia oceny skutków w zakresie ochrony danych przez administratora lub podmiot przetwarzający oraz wniosków o uprzednie zezwolenie lub uprzednią konsultację, jeśli są one wymagane na mocy art. 33 i art. 34;

g) monitorowanie odpowiedzi na wnioski organów nadzorczych oraz, w ramach kompetencji inspektora ochrony danych, współpraca z organem nadzorczym na wniosek tego organu lub z inicjatywy inspektora ochrony danych;

h) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem oraz zasięganie opinii organu nadzorczego, w odpowiednich przypadkach, z inicjatywy inspektora ochrony danych.

2. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 86 w celu doprecyzowania kryteriów i wymogów dotyczących zadań, certyfikacji, statusu, uprawnień i zasobów inspektora ochrony danych, o których mowa w ust. 1.

SEKCJA 5
KODEKSY POSTĘPOWANIA I CERTYFIKACJA

Artykuł 38
Kodeksy postępowania

1. Państwa członkowskie, organy nadzorcze i Komisja zachęcają do sporządzania kodeksów postępowania, które mają przyczynić się do właściwego stosowania niniejszego rozporządzenia, z uwzględnieniem szczególnych cech różnych sektorów, w których odbywa się przetwarzanie, w szczególności w zakresie:

a) rzetelnego i przejrzystego przetwarzania danych;

b) zbierania danych;

c) informowania opinii publicznej i podmiotów danych;

d) wniosków podmiotów danych w wykonaniu przysługujących im praw;

e) informowania i ochrony dzieci;

f) przekazywania danych państwom trzecim lub organizacjom międzynarodowym;

g) mechanizmów monitorowania i zapewnienia zgodności z kodeksem przez administratorów, którzy zobowiązali się do jego przestrzegania;

h) postępowań pozasądowych oraz innych trybów rozstrzygania sporów w celu rozstrzygania sporów między administratorami a podmiotami danych w zakresie przetwarzania danych osobowych, bez uszczerbku dla praw podmiotów danych na mocy art. 73 i 75.

2. Zrzeszenia i inne podmioty reprezentujące określone kategorie administratorów lub podmiotów przetwarzających w jednym państwie członkowskim, które pragną opracować kodeksy postępowania bądź zmienić lub uzupełnić obowiązujące kodeksy postępowania, mogą przedstawić je organowi nadzorczemu w tym państwie członkowskim celem zasięgnięcia opinii. Organ nadzorczy może wydać opinię dotyczącą zgodności projektu kodeksu postępowania lub proponowanej zmiany z niniejszym rozporządzeniem. Organ nadzorczy zasięga opinii podmiotów danych lub ich przedstawicieli na temat tych projektów.

3. Zrzeszenia i inne podmioty reprezentujące pewne kategorie administratorów w wielu państwach członkowskich mogą przedkładać Komisji projekty kodeksów postępowania i zmiany lub uzupełnienia obowiązujących kodeksów postępowania.

4. Komisja może przyjąć akty wykonawcze w celu podjęcia decyzji, czy kodeksy postępowania i zmiany lub uzupełnienia obowiązujących kodeksów postępowania przedłożone jej na mocy ust. 3 mają ogólną moc obowiązującą w całej Unii. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą określoną w art. 87 ust. 2.

5. Komisja zapewnia odpowiednie propagowanie informacji i kodeksach, których ogólną moc obowiązującą stwierdzono zgodnie z ust. 4.

Artykuł 39
Certyfikacja

1. Państwa członkowskie i Komisja zachęcają, w szczególności na poziomie europejskim, do ustanawiania mechanizmów certyfikacji w zakresie danych osobowych oraz pieczęci i oznaczeń w zakresie ochrony danych, które umożliwią podmiotom danych szybką ocenę poziomu ochrony danych zapewnionej przez administratorów i podmioty przetwarzające. Mechanizmy certyfikacji w zakresie ochrony danych przyczyniają się właściwego stosowania niniejszego rozporządzenia, z uwzględnieniem szczególnych cech różnych sektorów oraz rozmaitych operacji przetwarzania.

2. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 86 w celu doprecyzowania kryteriów i wymogów dotyczących mechanizmów certyfikacji w zakresie ochrony danych, o których mowa w ust. 1, w tym warunków przyznawania i odwoływania, oraz wymogów w zakresie uznawania na terytorium Unii i w państwach trzecich.

3. Komisja może ustanowić standardy techniczne dla mechanizmów certyfikacji oraz pieczęci i oznaczeń w zakresie ochrony danych, a także sposoby promowania i uznawania mechanizmów certyfikacji oraz pieczęci i oznaczeń w zakresie ochrony danych. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą określoną w art. 87 ust. 2.

ROZDZIAŁ V
PRZEKAZYWANIE DANYCH OSOBOWYCH DO PAŃSTW TRZECICH LUB ORGANIZACJI MIĘDZYNARODOWYCH

Artykuł 40
Ogólne zasady przekazywania

Przekazanie danych osobowych, które są lub mają być przetwarzane po przekazaniu do państwa trzeciego lub organizacji międzynarodowej może nastąpić tylko wtedy gdy, z zastrzeżeniem innych przepisów niniejszego rozporządzenia, administrator lub podmiot danych spełnią warunki wymienione w tym rozdziale, w tym dotyczące wtórnego przekazania danych z państwa trzeciego lub od organizacji międzynarodowej do innego państwa trzeciego lub innej organizacji międzynarodowej.

Artykuł 41
Przekazywanie na podstawie decyzji stwierdzającej odpowiedni poziom ochrony

1. Przekazanie może nastąpić, jeżeli Komisja zdecydowała, iż państwo trzecie, terytorium lub sektor, w którym odbywa się przetwarzanie danych w tym państwie trzecim lub organizacja międzynarodowa zapewniają odpowiedni poziom ochrony. Takie przekazanie nie wymaga żadnego dodatkowego zezwolenia.

2. Przy ocenie odpowiedniości poziomu ochrony Komisja uwzględnia następujące elementy:

   a) praworządność, ogólne i sektorowe przepisy obowiązujące w tym zakresie, w tym dotyczące bezpieczeństwa publicznego, obronności, bezpieczeństwa narodowego i prawa karnego, zasad wykonywania zawodu i środków bezpieczeństwa, które są przestrzegane w tym państwie lub organizacji międzynarodowej, a także skuteczne i egzekwowalne prawa, w tym prawa do skutecznych administracyjnych i sądowych środków ochrony prawnej przysługujące podmiotom danych, w szczególności tym podmiotom danych mającym miejsce zamieszkania w Unii, których dane osobowe są przekazywane;

   b) istnienie i skuteczne działanie przynajmniej jednego niezależnego organu nadzorczego w państwie trzecim lub organizacji międzynarodowej, odpowiedzialnego za zapewnienie zgodności z przepisami o ochronie danych, pomoc i doradzanie podmiotom danych w zakresie wykonania przysługujących im praw, a także współpracę z organami nadzorczymi Unii i państw członkowskich; oraz

c) międzynarodowe zobowiązania zaciągnięte przez dane państwo trzecie lub organizację międzynarodową.

3. Komisja może zdecydować, że państwo trzecie, terytorium lub sektor, w którym odbywa się przetwarzanie danych w państwie trzecim lub organizacja międzynarodowa zapewniają odpowiedni poziom ochrony w rozumieniu ust. 2. Te akty wykonawcze są przyjmowane zgodnie z procedurą sprawdzającą, o której mowa w art. 87 ust. 2.

4. Akty wykonawcze określają geograficzny i sektorowy zakres stosowania oraz, w stosownych przypadkach, wskazują organ nadzorczy wymieniony w ust. 2 lit. b).

5. Komisja może zdecydować, że państwo trzecie, terytorium lub sektor, w którym odbywa się przetwarzanie danych w państwie trzecim lub organizacja międzynarodowa nie zapewniają właściwego poziomu ochrony w rozumieniu ust. 2 tego artykułu, w szczególności w przypadkach w których odnośne przepisy ogólne i sektorowe obowiązujące w państwie trzecim lub organizacji międzynarodowej nie gwarantują skutecznych i egzekwowalnych praw, w tym prawa do skutecznych administracyjnych i sądowych środków ochrony prawnej podmiotom danych, w szczególności tym podmiotom danych mającym miejsce zamieszkania w Unii, których dane osobowe są przetwarzane. Te akty wykonawcze są przyjmowane zgodnie z procedurą sprawdzającą, o której mowa w art. 87 ust. 2 lub w przypadkach wyjątkowo pilnych w odniesieniu do osób fizycznych w zakresie ich prawa do ochrony danych osobowych, zgodnie z procedurą, o której mowa w art. 87 ust. 3.

6. W przypadku podjęcia przez Komisję decyzji na mocy art. 5 wszelkie operacje przekazywania danych osobowych do państwa trzeciego, na terytorium lub do sektora, w którym odbywa się przetwarzanie danych w tym państwie lub do organizacji międzynarodowej są zakazane, bez uszczerbku dla przepisów art. 42-44. We właściwym czasie Komisja przystąpi do konsultacji z państwem trzecim lub organizacją międzynarodową w celu zaradzenia sytuacji wynikającej z decyzji podjętej na mocy ust. 5 tego artykułu.

7. Komisja publikuje w *Dzienniku Urzędowym Unii Europejskiej* wykaz tych państw trzecich, terytoriów i sektorów, w których odbywa się przetwarzanie danych w państwie trzecim oraz organizacji międzynarodowych, co do których zdecydowano, że zapewniają odpowiedni poziom ochrony lub tego poziomu nie zapewniają.

8. Decyzje przyjęte przez Komisję na mocy art. 25 ust. 6 lub art. 26 ust. 4 dyrektywy 95/46/WE pozostają w mocy do czasu ich zmiany, zastąpienia lub uchylenia przez Komisję.

Artykuł 42

Operacje przekazywania dzięki odpowiednim gwarancjom

1. W przypadkach, w których Komisja nie podjęła decyzji na mocy art. 41, administrator lub podmiot przetwarzający mogą przekazać dane osobowe do państwa trzeciego lub organizacji międzynarodowej jedynie wtedy, gdy wprowadzą oni odpowiednie gwarancje w zakresie ochrony danych do prawnie wiążącego instrumentu.

2. Odpowiednie gwarancje, o których mowa w ust. 1, mogą mieć w szczególności postać:

a) wiążących reguł korporacyjnych zgodnie z art. 43, lub:

b) standardowych klauzul ochrony danych przyjętych przez Komisję. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 87 ust. 2; lub

c) standardowych klauzul ochrony danych przyjętych przez organ nadzorczy zgodnie z mechanizmem zgodności, o którym w art. 57, w przypadku gdy Komisja uzna je za ogólnie obowiązujące na mocy art. 62 ust. 1 lit. b); lub

d) klauzul umownych podpisanych między administratorem lub podmiotem przetwarzającym a odbiorcą danych upoważnionym przez organ nadzorczy zgodnie z ust. 4.

3. Operacja przekazywania na podstawie standardowych klauzul ochrony danych lub wiążących reguł korporacyjnych, o których mowa w ust. 2 lit. a), b) lub c), nie wymaga dodatkowego zezwolenia.

4. Jeśli operacja przekazywania odbywa się na podstawie klauzul umownych, o których mowa w ust. 2 lit. d) niniejszego artykułu, administrator lub podmiot przetwarzający uzyskują od organu nadzorczego uprzednie zezwolenie na zastosowanie klauzul umownych zgodnie z art. 34 ust. 1 lit. a). Jeśli przekazanie wiąże się z przetwarzaniem, które dotyczy podmiotu danych w innym państwie członkowskim lub innych państwach członkowskich bądź ma istotny wpływ na swobodny przepływ danych osobowych w całej Unii, organ nadzorczy stosuje mechanizm zgodności, o którym mowa w art. 57.

5. Jeśli prawnie wiążący instrument nie przewiduje odpowiednich gwarancji w zakresie ochrony danych, administrator lub podmiot przetwarzający uzyskują uprzednie zezwolenie na przekazanie lub przekazywanie lub też na włączenie stosownych przepisów do porozumień administracyjnych przewidujących podstawę takiego przekazania. Takie zezwolenie organu nadzorczego jest zgodne z art. 34 ust. 1 lit. a). Jeśli przekazanie wiąże się z przetwarzaniem, które dotyczy podmiotów danych w innym państwie członkowskim lub innych państwach członkowskich bądź ma istotny wpływ na swobodny przepływ danych osobowych w całej Unii, organ nadzorczy stosuje mechanizm zgodności, o którym mowa w art. 57. Zezwolenia wydane przez organ nadzorczy na podstawie art. 26 ust. 2 dyrektywy 95/46/WE zachowują ważność do czasu ich zmiany, zastąpienia lub uchylenia przez ten organ.

Artykuł 43

Operacje przekazywania na podstawie wiążących reguł korporacyjnych

1. Organ nadzorczy zatwierdza wiążące reguły korporacyjne zgodnie z mechanizmem zgodności przewidzianym w art. 58 pod warunkiem, że:

a) są one prawnie wiążące i mają zastosowanie do oraz są egzekwowane przez wszystkich członków grupy przedsiębiorstw administratora lub podmiotu przetwarzającego, i obejmują ich pracowników;

b) wyraźnie przyznają podmiotom danych egzekwowalne prawa;

c) spełniają wymogi ustanowione w ust. 2.

2. Wiążące reguły korporacyjne określają co najmniej:

a) strukturę i dane kontaktowe grupy przedsiębiorstw i jej członków;

b) operację lub zestaw operacji przekazywania danych, w tym kategorie danych osobowych, rodzaj przetwarzania i jego cele, typy podmiotów danych oraz nazwę państwa trzeciego lub państw trzecich:

c) ich prawnie wiążący charakter, w wymiarze wewnętrznym i zewnętrznym;

d) ogólne zasady ochrony danych, w szczególności zasadę celowości, jakość danych, podstawę prawna przetwarzania, przetwarzanie szczególnie chronionych danych osobowych, środki mające na celu zapewnienie bezpieczeństwa danych oraz wymogi w zakresie wtórnego przekazywania organizacjom, które nie są związane politykami;

e) prawa podmiotów danych oraz środki umożliwiające wykonywanie tych praw, w tym prawo do niepodlegania środkowi opartemu na profilowaniu zgodnie z art. 20, prawo do zgłaszania skarg właściwemu organowi nadzorczemu i przed właściwymi sądami państw trzecich zgodnie z art. 75 oraz prawo do uzyskania środka zaradczego i w stosownych przypadkach odszkodowania za naruszenie wiążących reguł korporacyjnych;

f) przyjęcia przez administratora lub podmiot przetwarzający mających siedzibę na terytorium państwa członkowskiego odpowiedzialności za naruszenie wiążących reguł korporacyjnych przez członka grupy przedsiębiorstw niemającego siedziby na terytorium Unii; administrator lub podmiot przetwarzający mogą być zwolnieni z tej odpowiedzialności, w całości lub w części, jeśli udowodnią, że członek ten nie ponosi odpowiedzialności za wydarzenie, które doprowadziło do powstania szkody;

g) sposób przekazywania podmiotom danych informacji na temat wiążących reguł korporacyjnych, w szczególności na temat przepisów, o których mowa w lit. d), e) i f) tego ustępu zgodnie z art. 11;

h) zadania inspektora ochrony danych wyznaczonego zgodnie z art. 35, w tym monitorowanie w ramach grupy przedsiębiorstw zgodności z wiążącymi regułami korporacyjnymi, a także monitorowanie szkoleń i rozpatrywania skarg;

i) mechanizmy obowiązujące w grupie przedsiębiorstw, które mają na celu zapewnienie weryfikacji przestrzegania wiążących reguł korporacyjnych;

j) mechanizmy dotyczące zgłaszania i rejestrowania zmian w politykach i zgłaszania tych zmian organowi nadzorczemu;

k) mechanizm współpracy z organem nadzorczym mającej na celu zapewnienie przestrzegania przez wszystkich członków grupy przedsiębiorstw, w

szczególności poprzez udostępnienie organowi nadzorczemu wyników weryfikacji środków, o których mowa w lit. i) tego ustępu.

3. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 86 w celu doprecyzowania kryteriów i wymogów dotyczących wiążących reguł korporacyjnych w rozumieniu tego artykułu, w szczególności jeśli chodzi o kryteria ich zatwierdzania, stosowanie ust. 2 lit. b), d) i e) do wiążących reguł korporacyjnych, które przyjęły podmioty przetwarzające oraz innych niezbędnych wymogów w celu zapewnienia ochrony danych osobowych osoby, której one dotyczą.

4. Komisja może wskazać format i procedury wymiany informacji drogą elektroniczną między administratorami, podmiotami przetwarzającymi i organami nadzorczymi do celów wiążących reguł korporacyjnych w rozumieniu tego artykułu. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą określoną w art. 87 ust. 2.

Artykuł 44
Odstępstwa

1. W braku decyzji stwierdzającej odpowiedni poziom ochrony na mocy art. 41 lub odpowiednich gwarancji na mocy art. 42, operacja lub zestaw operacji przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej może nastąpić wyłącznie pod warunkiem, że:

a) podmiot danych wyraził zgodę na proponowane przekazanie, po uzyskaniu informacji o zagrożeniach związanych z takim przekazaniem ze względu na brak decyzji stwierdzającej odpowiedni poziom ochrony oraz odpowiednich gwarancji; lub

b) przekazanie jest niezbędne do wykonania umowy między podmiotem danych a administratorem lub wprowadzenia w życie środków poprzedzających umowę na wniosek podmiotu danych; lub

c) przekazanie jest konieczne do zawarcia lub wykonania umowy zawartej w interesie podmiotu danych między administratorem a inną osobą fizyczną lub prawną, lub

d) przekazanie jest niezbędne ze względu na istotny interes publiczny; lub

e) przekazanie jest niezbędne do ustalania, realizacji lub ochrony roszczeń prawnych; lub

f) przekazanie jest konieczne do ochrony żywotnych interesów podmiotu danych lub innej osoby, w przypadku gdy podmiot danych nie ma fizycznej lub prawnej zdolności do wyrażenia zgody; lub

g) przekazanie następuje z rejestru, który zgodnie z prawem Unii lub państwa członkowskiego ma służyć za źródło informacji dla ogółu społeczeństwa, udostępnionego do konsultacji obywateli i każdej osoby mogącej wykazać słuszny interes, o ile warunki określone przez prawo Unii lub państwa

członkowskiego odnośnie do wglądu do takiego rejestru zostały w danym przypadku spełnione; lub

h) przekazanie jest konieczne dla potrzeb wynikających ze słusznych interesów administratora lub podmiotu przetwarzającego, których nie można uznać za częste lub masowe i jeżeli administrator lub podmiot przetwarzający ocenili wszystkie okoliczności towarzyszące operacji przekazywania danych lub operacjom przekazywania danych i na podstawie tej oceny w razie potrzeby przewidzieli odpowiednie gwarancje w zakresie ochrony danych osobowych.

2. Przekazanie na mocy ust. 1 lit. g) nie obejmuje całości danych osobowych lub wszystkich kategorii danych osobowych obecnych w rejestrze. Jeśli rejestr służy do wglądu osobom mającym uzasadniony interes, przekazanie następuje jedynie na wniosek tych osób lub jeśli mają one być odbiorcami tych danych.

3. Jeśli przetwarzanie odbywa się na podstawie ust. 1 lit. h), administrator lub podmiot przetwarzający zwracają szczególną uwagę na charakter danych, cel i czas trwania planowanej operacji przetwarzania lub planowanych operacji przetwarzania, a także sytuację w państwie pochodzenia, państwie trzecim i państwie ostatecznego przeznaczenia oraz, w razie potrzeby, istnienie odpowiednich gwarancji w zakresie ochrony danych.

4. Ustęp 1 lit. b), c) i h) nie ma zastosowania do działalności prowadzonej przez organy publiczne w ramach wykonywania ich uprawnień publicznych.

5. Interes publiczny, o którym mowa w ust. 1 lit. d), musi być uznany w prawie Unii lub państwa członkowskiego, któremu podlega administrator.

6. Administrator lub podmiot przetwarzający sporządzają włączają dokumentację dotyczącą oceny, a także istnienia odpowiednich gwarancji, o których mowa w ust. 1 lit. h) tego artykułu do dokumentacji, o której mowa w art. 28 i informują organ nadzorczy o przekazaniu.

7. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 86 w celu doprecyzowania znaczenia „istotnego interesu publicznego” w rozumieniu ust. 1 lit. d), a także kryteriów i wymogów dotyczących odpowiednich gwarancji, o których mowa w ust. 1 lit. h).

Artykuł 45

Międzynarodowa współpraca na rzecz ochrony danych osobowych

1. W stosunku do państw trzecich i organizacji międzynarodowych Komisja i organy nadzorcze podejmują stosowne kroki na rzecz:

a) opracowania skutecznych mechanizmów współpracy międzynarodowej, by ułatwić egzekwowanie przepisów służących ochronie danych osobowych;

b) zapewnienia międzynarodowej wzajemnej współpracy w zakresie egzekwowania przepisów dotyczących ochrony danych, w tym poprzez zawiadomienia, przekazywanie skarg, pomoc w dochodzeniach i wymianę

informacji, z zastrzeżeniem odpowiednich gwarancji ochrony danych osobowych i innych podstawowych praw i wolności;

c) włączenia zainteresowanych podmiotów w dyskusję i działalność mające na celu pogłębienie współpracy międzynarodowej w zakresie egzekwowania przepisów dotyczących ochrony danych osobowych;

d) promowania wymiany i dokumentowania przepisów i praktyk w zakresie ochrony danych.

2. Do celów ust. 1, Komisja podejmie odpowiednie kroki, by poprawić współpracę z państwami trzecimi lub organizacjami międzynarodowymi, w szczególności ich organami nadzorczymi, jeśli Komisja zdecydowała, że zapewniają one odpowiedni poziom ochrony w rozumieniu art. 41 ust. 3.

ROZDZIAŁ VI
NIEZALEŻNE ORGANY NADZORCZE

SEKCJA 1
NIEZALEŻNY STATUS

Artykuł 46
Organ nadzorczy

1. Każde państwo członkowskie ustanowi przepisy przewidujące, że przynajmniej jeden organ publiczny jest odpowiedzialny za monitorowanie stosowania niniejszego rozporządzenia oraz za przyczynianie się do jego jednolitego stosowania na terytorium całej Unii w celu ochrony podstawowych praw i wolności osób fizycznych w odniesieniu do przetwarzania danych oraz ułatwienia swobodnego przepływu danych w Unii. Dla tych celów organy nadzorcze współpracują ze sobą i z Komisją.

2. W przypadku gdy w państwie członkowskim został ustanowiony więcej niż jeden organ nadzorczy, państwo członkowskie wskazuje organ nadzorczy, który działa jako pojedynczy punkt kontaktowy, co ma pozwolić na skuteczne uczestnictwo tych organów w Europejskiej Radzie Ochrony Danych, oraz ustala mechanizm zapewniający poszanowanie przez inne organy przepisów dotyczących mechanizmu zgodności, o którym mowa w art. 57.

3. Każde państwo członkowskie zawiadamia Komisję o przepisach prawa, które przyjęło na mocy niniejszego rozdziału, najpóźniej przed terminem określonym w art. 91 ust. 2 i bezzwłocznie o każdej kolejnej zmianie mającej na nie wpływ.

Artykuł 47
Niezależność

1. Organ nadzorczy działa w sposób w pełni niezależny podczas wykonywania obowiązków i powierzonych mu uprawnień.

2. Członkowie organu nadzorczego podczas wykonywania swoich obowiązków nie zwracają się do nikogo o instrukcje ani ich od nikogo nie przyjmują.

3. Członkowie organu nadzorczego powstrzymują się od wszelkich czynności niezgodnych ze swoimi obowiązkami i podczas swojej kadencji nie podejmują żadnej funkcji, zarobkowej lub niezarobkowej, stojącej w sprzeczności z tymi obowiązkami.

4. Członkowie organu nadzorczego po zakończeniu swojej kadencji postępują w sposób uczciwy i ostrożny w odniesieniu do obejmowania stanowisk i przyjmowania korzyści.

5. Każde państwo członkowskie zapewnia, by organ nadzorczy został wyposażony w odpowiednie zasoby ludzkie, techniczne i finansowe, pomieszczenia i infrastrukturę niezbędne do skutecznego wykonywania swoich obowiązków i uprawnień, w tym do ich wykonywania w kontekście wzajemnej pomocy, współpracy i uczestnictwa w Europejskiej Radzie Ochrony Danych.

6. Każde państwo członkowskie zapewnia, by organ nadzorczy miał własny personel, który jest powoływany przez szefa organu nadzorczego i podlega jego kierownictwu.

7. Państwa członkowskie zapewniają, by organ nadzorczy podlegał kontroli finansowej, która nie narusza jego niezależności. Państwa członkowskie dopilnują, by organy nadzorcze dysponowały odrębnymi budżetami rocznymi. Budżety są podawane do wiadomości publicznej.

Artykuł 48

Ogólne warunki dotyczące członków organu nadzorczego

1. Państwa członkowskie zapewniają, by członkowie organu nadzorczego byli wybierani albo przez parlament albo przez rząd danego państwa członkowskiego.

2. Członków wybiera się spośród osób, których niezależność jest niekwestionowana i których doświadczenie i umiejętności wymagane do wykonywania obowiązków, w szczególności w dziedzinie ochrony danych osobowych, zostały wykazane.

3. W razie upływu kadencji, rezygnacji lub przymusowego pozbawienia funkcji członek organu przestaje pełnić swoje obowiązki zgodnie z art. 5.

4. Członek może być odwołany lub pozbawiony praw do emerytury lub innych alternatywnych świadczeń przez właściwy sąd krajowy, jeżeli nie spełnia już warunków wymaganych do wykonywania obowiązków lub dopuścił się poważnego uchybienia.

5. W przypadku upływu kadencji członka lub jego rezygnacji wykonuje on dalej swoje obowiązki do chwili wyboru nowego członka.

Artykuł 49
Zasady dotyczące ustanowienia organu nadzorczego

Każde państwo członkowskie przyjmuje przepisy w granicach niniejszego rozporządzenia w zakresie:

a) ustanowienia i statusu organu nadzorczego;

b) kwalifikacji, doświadczenia i umiejętności wymaganych do pełnienia obowiązków członka organu nadzorczego;

c) regulacji i procedur w zakresie wyznaczania członków organu nadzorczego, jak również regulacji odnoszących się do działań lub funkcji niedających się pogodzić z pełnionymi obowiązkami;

d) okresu kadencji członków organu nadzorczego, która nie trwa krócej niż cztery lata, z wyjątkiem pierwszej kadencji po wejściu w życie niniejszego rozporządzenia, która może trwać krócej, w przypadku gdy jest to niezbędne, aby chronić niezależność organu nadzorczego poprzez rozłożoną w czasie procedurę wyboru;

e) określenia, czy członkowie organu nadzorczego mogą być ponownie wyznaczeni;

f) przepisów i wspólnych warunków pełnienia obowiązków przez członków i personel organu nadzorczego;

g) regulacji i procedur odnoszących się do zakończenia pełnienia obowiązków przez członków organu nadzorczego, w tym jeżeli nie spełniają już warunków wymaganych do wykonywania obowiązków lub jeżeli są winni poważnego uchybienia.

Artykuł 50
Tajemnica służbowa

Członkowie i personel organu nadzorczego, podczas kadencji i po jej zakończeniu, podlegają obowiązkowi zachowania tajemnicy służbowej w odniesieniu do wszelkich poufnych informacji, które uzyskali w toku wykonywania obowiązków służbowych.

SEKCJA 2
OBOWIĄZKI I UPRAWNIENIA

Artykuł 51
Właściwość

1. Każdy organ nadzorczy wykonuje, na terytorium własnego państwa członkowskiego, uprawnienia nadane mu zgodnie z niniejszym rozporządzeniem.

2. W przypadku gdy przetwarzanie danych osobowych odbywa się w kontekście działalności administratora lub podmiotu przetwarzającego ustanowionych na terytorium Unii, a administrator lub podmiot przetwarzający prowadzą działalność w więcej niż jednym państwie członkowskim, organ nadzorczy głównej siedziby administratora lub podmiotu przetwarzającego jest odpowiedzialny za nadzór nad działalnością administratora lub podmiotu przetwarzającego we wszystkich państwach członkowskich, bez uszczerbku dla przepisów rozdziału VII niniejszego rozporządzenia.

3. Organ nadzorczy nie ma właściwości do nadzorowania operacji przetwarzania dokonywanych przez sądy w toku wykonywania przez nie funkcji sądowych.

Artykuł 52
Obowiązki

1. Organ nadzorczy:

a) monitoruje i zapewnia stosowanie rozporządzenia;

b) rozpoznaje skargi złożone przez każdy podmiot danych lub przez zrzeszenie reprezentujące podmiot danych, zgodnie z art. 73, prowadzi dochodzenie, we właściwym zakresie, dotyczące danej sprawy i informuje w rozsądnym czasie podmiot danych lub zrzeszenie o postępach w sprawie i wyniku skargi, w szczególności jeżeli niezbędne jest dalsze dochodzenie lub koordynacja z innym organem nadzorczym;

c) dzieli się informacjami i zapewnia wzajemną pomoc udzielaną innym organom nadzorczym oraz spójność stosowania i wykonywania rozporządzenia;

d) prowadzi dochodzenia albo z własnej inicjatywy albo na podstawie skargi lub wniosku innego organu nadzorczego, i informuje w rozsądnym czasie podmiot danych, jeżeli skierował on skargę do tego organu nadzorczego, o wyniku dochodzeń;

e) monitoruje zmiany w odpowiednich dziedzinach, o ile mają one wpływ na ochronę danych osobowych, w szczególności rozwój technologii informacyjno-telekomunikacyjnych i praktyki handlowe;

f) jest konsultowany przez instytucje i organy państw członkowskich na temat środków prawnych i administracyjnych dotyczących ochrony praw i wolności osób fizycznych w odniesieniu do przetwarzania danych osobowych;

g) zezwala na operacje przetwarzania, o których mowa w art. 34, i jest w ich sprawie konsultowany;

h) wydaje opinię na temat projektów kodeksów postępowania na podstawie art. 38 ust. 2;

i) zatwierdza wiążące reguły korporacyjne na mocy art. 43;

j) uczestniczy w działalności Europejskiej Rady Ochrony Danych.

2. Każdy organ nadzorczy działa na rzecz pogłębiania w społeczeństwie świadomości w zakresie ryzyka, przepisów, gwarancji oraz praw związanych z przetwarzaniem danych osobowych. Szczególną uwagę zwraca się na działania skierowane do dzieci.

3. Organ nadzorczy, na wniosek, doradza każdemu podmiotowi danych na temat korzystania z praw na podstawie niniejszego rozporządzenia, a w stosownych przypadkach współpracuje w tym celu z organami nadzorczymi w innych państwach członkowskich.

4. W odniesieniu do skarg, o których mowa w ust. 1 lit. b), organ nadzorczy udostępnia formularz skargi, który może być wypełniony elektronicznie, przy czym dostępne są także inne środki łączności.

5. Organ nadzorczy wykonuje obowiązki na rzecz podmiotów danych bez pobierania opłat.

6. W przypadku gdy żądania są wyraźnie nadmierne, w szczególności ze względu na ich powtarzalny charakter, organ nadzorczy może zażądać opłaty lub nie podjąć działania, o które wnosił podmiot danych. Na organie nadzorczym spoczywa ciężar udowodnienia, że żądanie miało wyraźnie nadmierny charakter.

Artykuł 53
Uprawnienia

1. Każdy organ nadzorczy jest uprawniony do:

   a) zawiadamiania administratora lub podmiotu przetwarzającego o domniemanym naruszeniu przepisów regulujących przetwarzanie danych osobowych, a w stosownych przypadkach, nakazania administratorowi lub podmiotowi przetwarzającemu usunięcia naruszenia w konkretny sposób w celu poprawy ochrony podmiotu danych;

   b) nakazania administratorowi lub podmiotowi przetwarzającemu dane spełnienia żądań przedstawionych przez podmioty danych dotyczących skorzystania z praw przewidzianych w niniejszym rozporządzeniu;

   c) nakazania administratorowi i podmiotowi przetwarzającemu dane, a w stosownych przypadkach przedstawicielowi, dostarczenia każdej informacji istotnej w toku wykonywania jego obowiązków;

   d) zapewnienia zgodności z uprzednimi zezwoleniami i konsultacjami, o których mowa w art. 34;

   e) ostrzegania lub upominania administratora lub podmiotu przetwarzającego;

   f) nakazania poprawienia, usuwania lub zniszczenia wszystkich danych, jeżeli były one przetwarzane z naruszeniem przepisów niniejszego rozporządzenia oraz powiadomienia o takich działaniach osób trzecich, którym dane zostały ujawnione;

   g) nałożenia czasowego lub ostatecznego zakazu przetwarzania;

h) zawieszenia przepływu danych do odbiorcy w państwie trzecim lub w organizacji międzynarodowej;

i) do wydawania opinii na każdy temat związany z ochroną danych osobowych;

j) do informowania parlamentu narodowego, rządu lub innych politycznych instytucji, jak również opinii publicznej o każdym zagadnieniu związanym z ochroną danych osobowych.

2. Każdy organ nadzorczy ma uprawnienia dochodzeniowe pozwalające mu uzyskać od administratora lub podmiotu przetwarzającego:

a) dostęp do wszystkich danych osobowych i do wszystkich informacji niezbędnych do wykonywania obowiązków;

b) dostęp do każdego pomieszczenia, w tym do każdego sprzętu i środków służących do przetwarzania danych, gdy istnieją zasadne podstawy, by przypuszczać, że dochodzi tam do naruszenia niniejszego rozporządzenia.

Uprawnienia, o których mowa w lit. b), są wykonywane zgodnie prawem Unii i prawem państwa członkowskiego.

3. Każdy organ nadzorczy ma uprawnienie do zwrócenia uwagi organom sądowym na naruszenie niniejszego rozporządzenia i do wszczynania postępowania prawnego, w szczególności zgodnie z art. 74 ust. 4 i art. 75 ust. 2.

4. Każdy organ nadzorczy ma uprawnienie do nakładania sankcji administracyjnych za naruszenie przepisów prawa administracyjnego, w szczególności o którym w art. 79 ust. 4, 5 i 6.

Artykuł 54
Sprawozdanie z działalności

Każdy organ nadzorczy musi sporządzać roczne sprawozdanie ze swojej działalności. Sprawozdanie jest przedstawione parlamentowi narodowemu i jest udostępniane opinii publicznej, Komisji oraz Europejskiej Radzie Ochrony Danych.

ROZDZIAŁ VII
WSPÓŁPRACA I ZGODNOŚĆ

SEKCJA 1
WSPÓŁPRACA

Artykuł 55
Wzajemna pomoc

1. Organy nadzorcze przekazują sobie odpowiednie informacje i zapewniają sobie wzajemną pomoc w celu spójnego wykonania i stosowania niniejszego rozporządzenia i przyjmują środki na rzecz zapewnienia skutecznej wzajemnej współpracy. Wzajemna pomoc obejmuje w szczególności wnioski o udzielenie informacji i środki nadzorcze, takie jak wnioski o udzielenie uprzednich zezwoleń i konsultacji, inspekcje i sprawne przekazywanie informacji dotyczących rozpoczęcia spraw i ich rozwoju, w przypadku gdy operacje przetwarzania danych będą miały prawdopodobnie wpływ na podmioty danych w wielu państwach członkowskich.

2. Każdy organ nadzorczy podejmuje wszystkie odpowiednie środki niezbędne do udzielenia odpowiedzi na wniosek innego organu nadzorczego bez zwłoki i nie później niż w terminie jednego miesiąca od otrzymania wniosku. Takie środki mogą obejmować w szczególności przekazywanie odpowiednich informacji na temat przebiegu dochodzenia lub realizacji środków egzekucyjnych w celu doprowadzenia do zaprzestania lub zabronienia operacji przetwarzania niezgodnych z niniejszym rozporządzeniem.

3. Wniosek o udzielenie pomocy zawiera wszystkie niezbędne informacji, w tym cel i uzasadnienie wniosku. Informacje będące przedmiotem wymiany wykorzystywane są wyłącznie w odniesieniu do sprawy określonej we wniosku.

4. Organ nadzorczy, do którego został skierowany wniosek o pomoc, nie może odmówić realizacji wniosku, chyba że:

   a) nie jest właściwy do zajęcia się wnioskiem; lub

   b) realizacja wniosku byłaby niezgodna z przepisami niniejszego rozporządzenia.

5. Organ nadzorczy, do którego został skierowany wniosek, informuje organ nadzorczy, który złożył wniosek, o wynikach lub, zależnie od okoliczności, o postępach w sprawie lub środkach podjętych w celu realizacji wniosku przez organ nadzorczy, do którego został skierowany wniosek.

6. Organy nadzorcze przekazują informacje, których dotyczył wniosek innych organów nadzorczych, w drodze elektronicznej i w najkrótszym możliwym terminie, przy użyciu standardowego formatu.

7. Nie pobiera się opłat od działania podjętego w wyniku przesłania wniosku o wzajemną pomoc.

8. W przypadku gdy organ nadzorczy, na wniosek innego organu nadzorczego, nie podjął działania w terminie jednego miesiąca, organ, który złożył wniosek, jest właściwy do podjęcia środków tymczasowych na terytorium swojego państwa członkowskiego zgodnie z art. 51 ust. 1 i przekazuje sprawę Europejskiej Radzie Ochrony Danych w trybie procedury, o której mowa w art. 57.

9. Organ nadzorczy określa okres obowiązywania takich środków tymczasowych. Okres ten nie przekracza trzech miesięcy. Organ nadzorczy bezzwłocznie informuje o tych środkach Europejską Radę Ochrony Danych i Komisję, podając pełne uzasadnienie.

10. Komisja może określić formułę oraz procedurę wzajemnej pomocy, o której mowa w niniejszym artykule, oraz metody wymiany informacji przy wykorzystaniu środków elektronicznych między organami nadzorczymi oraz między organami nadzorczymi a Europejską Radą Ochrony Danych, w szczególności w odniesieniu do standardowego formatu, o którym mowa w ust. 6. Te środki egzekucyjne są przyjmowane zgodnie z procedurą sprawdzającą, o której mowa w art. 87 ust. 2.

Artykuł 56
Wspólne operacje organów nadzorczych

1. W celu zacieśnienia współpracy i zwiększenia wzajemnej pomocy organy nadzorcze wykonują wspólne zadania dochodzeniowe, przyjmują wspólne środki egzekucyjne i prowadzą inne wspólne operacje, podczas których wyznaczeni członkowie lub personel organów nadzorczych z innych państw członkowskich uczestniczą w operacjach na terytorium danego państwa członkowskiego.

2. W przypadkach gdy operacje przetwarzania będą miały prawdopodobny wpływ na podmioty danych organ nadzorczy każdego z tych państw członkowskich ma prawo uczestniczyć, stosownie do okoliczności, w wykonywaniu wspólnych zadań dochodzeniowych lub wspólnych operacji. Właściwy organ nadzorczy wzywa organ nadzorczy każdego z tych państw członkowskich do uczestnictwa w wykonywaniu danego zadania dochodzeniowego lub wspólnej operacji i odpowiada bezzwłocznie na wniosek organu nadzorczego zawierający prośbę o uczestnictwo w operacjach.

3. Każdy organ nadzorczy, jako przyjmujący organ nadzorczy, zgodnie z własnym prawem krajowym i za zgodą wysyłającego organu nadzorczego, może przyznać członkom lub personelowi wysyłającego organu nadzorczego, uczestniczącym we wspólnych operacjach, uprawnienia wykonawcze, w tym zadania dochodzeniowe, lub, o ile jest to dozwolone prawem przyjmującego organu nadzorczego, pozwolić członkom lub personelowi wysyłającego organu nadzorczego wykonywać ich uprawnienia wykonawcze zgodnie z prawem wysyłającego organu nadzorczego. Te uprawnienia wykonawcze mogą być wykonywane wyłącznie pod kierownictwem i, co do zasady, w obecności członków lub personelu przyjmującego organu nadzorczego. Członkowie lub personel wysyłającego organu nadzorczego podlegają prawu krajowemu przyjmującego organu nadzorczego. Odpowiedzialność za ich działania ponosi przyjmujący organ nadzorczy.

4. Organy nadzorcze określają praktyczne elementy konkretnych działań w ramach współpracy.

5. W przypadku gdy organ nadzorczy nie spełni w terminie jednego miesiąca obowiązku ustanowionego w ust. 2, inne organy nadzoru są uprawnione do przyjęcia środka tymczasowego na terytorium swojego państwa członkowskiego zgodnie z art. 51. ust. 1.

6. Organ nadzorczy określa okres obowiązywania środka tymczasowego, o którym mowa w ust. 5. Okres ten nie przekracza trzech miesięcy. Organ nadzorczy bezzwłocznie informuje o tych środkach Europejską Radę Ochrony Danych i Komisję, podając pełne uzasadnienie, i przekazuje sprawę do mechanizmu, o którym mowa w art. 57.

SEKCJA 2
ZGODNOŚĆ

Artykuł 57
Mechanizm zgodności

Dla celów określonych w art. 46 ust. 1 organy nadzorcze współpracują ze sobą i Komisją poprzez mechanizm zgodności określony w niniejszej sekcji.

Artykuł 58
Opinia Europejskiej Rady Ochrony Danych

1. Zanim organ nadzorczy przyjmie środek, o którym mowa w art. 2, organ ten przesyła projekt środka Europejskiej Radzie Ochrony Danych i Komisji.

2. Obowiązek określony w ust. 1 ma zastosowanie do środka, który ma na celu wywarcie skutków prawnych i który:

   a) odnosi się do działań związanych ze sprzedażą towarów lub świadczeniem usług podmiotom danych w wielu państwach członkowskich lub z monitorowaniem ich zachowania; lub

   b) może mieć znaczący wpływ na swobodny przepływ danych osobowych na terytorium Unii; lub

   c) ma na celu przyjęcie wykazu operacji przetwarzania podlegających uprzedniej konsultacji na mocy art. 34 ust. 5; lub

   d) ma na celu określenie standardowych klauzul ochrony danych, o których mowa w art. 42 ust. 2 lit. c); lub

   e) ma na celu zezwolenie na klauzule umowne, o których mowa w art. 42 ust. 2 lit. d); lub

   f) ma na celu zatwierdzenie wiążących reguł korporacyjnych w rozumieniu art. 43.

3. Każdy organ nadzorczy lub Europejska Rada Ochrony Danych mogą zażądać, aby jakakolwiek sprawa została załatwiona w ramach mechanizmu zgodności, w szczególności w przypadku gdy organ nadzorczy nie przedstawi projektu środka, o którym mowa w ust. 2, lub nie wywiązuje się z obowiązków dotyczących wzajemnej pomocy zgodnie z art. 55 lub wspólnych operacji zgodnie z art. 56.

4. W celu zapewnienia właściwego i spójnego stosowania niniejszego rozporządzenia Komisja może zażądać, aby dowolna sprawa została załatwiona w ramach mechanizmu zgodności.

5. Organy nadzorcze i Komisja przekazują drogą elektroniczną każdą odpowiednią informację, w tym zależnie od okoliczności, streszczenie stanu faktycznego, projekt środka i powody, które przemawiają za koniecznością przyjęcia takiego środka, przy zastosowaniu standardowego formatu.

6. Przewodniczący Europejskiej Rady Ochrony Danych przekazuje niezwłocznie drogą elektroniczną stosowne informacje, które zostały mu przekazane, przy zastosowaniu standardowego formatu, członkom Europejskiej Rady Ochrony Danych i Komisji. Przewodniczący Europejskiej Rady Ochrony Danych zapewnia tłumaczenie stosownych informacji, jeżeli jest to konieczne.

7. Europejska Rada Ochrony Danych wydaje opinię na temat danej sprawy, jeżeli Europejska Rada Ochrony Danych podejmie taką decyzję zwykłą większością głosów swoich członków lub jakikolwiek organ nadzorczy lub Komisja tego zażąda w terminie jednego tygodnia od otrzymania stosownej informacji zgodnie z ust. 5. Opinię przyjmuje się w terminie jednego miesiąca zwykłą większością głosów członków Europejskiej Rady Ochrony Danych. Przewodniczący Europejskiej Rady Ochrony Danych informuje, bez nieuzasadnionej zwłoki, organ nadzorczy, o którym mowa, zależnie od okoliczności, w ust. 1 i ust. 3, Komisję i organ nadzorczy właściwy na podstawie art. 51 o opinii i podaje ją do publicznej wiadomości.

8. Organ nadzorczy, o którym mowa w ust. 1, i organ nadzorczy właściwy na podstawie art. 51 uwzględnia opinię Europejskiej Rady Ochrony Danych i w terminie dwóch tygodni od uzyskania informacji na temat opinii przez przewodniczącego Europejskiej Rady Ochrony Danych, przekazuje drogą elektroniczną przewodniczącemu Europejskiej Rady Ochrony Danych i Komisji informację, czy utrzymuje czy zmienia projekt środka, a w tym ostatnim przypadku przekazuje zmieniony projekt środka, przy zastosowaniu standardowego formatu.

Artykuł 59
Opinia Komisji

1. W terminie dziesięciu tygodni od wniesienia sprawy na podstawie art. 58 lub najpóźniej w terminie sześciu tygodni w przypadku art. 61, Komisja może przyjąć opinię związaną ze sprawami wniesionymi na mocy art. 58 lub art. 61 w celu zapewnienia właściwego i spójnego stosowania rozporządzenia.

2. W przypadku gdy Komisja przyjęła opinię zgodnie z ust. 1 dany organ nadzorczy uwzględnia w jak najszerszym stopniu opinię Komisji i informuje Komisję i

Europejską Radę Ochrony Danych, czy zamierza utrzymać czy zmienić projekt środka.

3. W okresie, o którym mowa w ust. 1, organ nadzorczy nie może przyjąć projektu środka.

4. W przypadku gdy dany organ nadzorczy nie zamierza uwzględnić opinii Komisji informuje o tym Komisję i Europejską Radę Ochrony Danych w terminie, o którym mowa w ust. 1, i przedstawia uzasadnienie. W tym przypadku projektu środka nie przyjmuje się przez okres kolejnego miesiąca.

Artykuł 60
Zawieszenie projektu środka

1. W terminie jednego miesiąca po przekazaniu informacji, o której mowa w art. 59 ust. 4, oraz w przypadku gdy Komisja ma poważne wątpliwości, czy projekt środka zapewniłby właściwe stosowanie niniejszego rozporządzenia czy też przeciwnie wiązałby się z jego niespójnym stosowaniem, Komisja może przyjąć uzasadnioną decyzję nakładającą na organ nadzorczy obowiązek zawieszenia przyjęcia danego projektu środka, uwzględniając opinię wydaną przez Europejską Radę Ochrony Danych na mocy art. 58 ust. 7 lub art. 61 ust. 2, w przypadku gdy wydaje się to konieczne w celu:

   a) pogodzenia rozbieżnych stanowisk organu nadzorczego i Europejskiej Rady Ochrony Danych, jeżeli nadal wydaje się to możliwe; lub

   b) przyjęcia środka zgodnie z art. 62 ust. 1 lit. a).

2. Komisja określi czas trwania zawieszenia, który nie przekracza 12 miesięcy.

3. W okresie, o którym mowa w ust. 2, organ nadzorczy nie może przyjąć danego projektu środka.

Artykuł 61
Tryb pilny

1. W wyjątkowych okolicznościach, gdy organ nadzorczy uznaje, że istnieje potrzeba pilnego działania w celu ochrony interesów podmiotów danych, w szczególności kiedy istnieje niebezpieczeństwo, że skorzystanie z prawa przez podmiot danych może być znacząco utrudnione przez zmianę istniejącego stanu lub w celu uniknięcia poważnych niedogodności lub z innych powodów, w drodze odstępstwa od procedury, o której mowa w art. 58, organ ten może przyjąć niezwłocznie środki tymczasowe o ograniczonym okresie obowiązywania. Organ nadzorczy bezzwłocznie informuje o tych środkach Europejską Radę Ochrony Danych i Komisję, podając pełne uzasadnienie.

2. Jeżeli organ nadzorczy przyjął środek zgodnie z ust. 1 i uznaje, że należy przyjąć pilnie środki ostateczne, może wystąpić o opinię w trybie pilnym do Europejskiej Rady Ochrony Danych, podając uzasadnienie potrzeby wydania takiej opinii, w tym pilności przyjęcia środków ostatecznych.

3. Każdy organ nadzorczy może wystąpić o wydanie opinii w trybie pilnym w przypadku, gdy właściwy organ nadzorczy nie przyjął odpowiednich środków w sytuacji, w której istnieje potrzeba pilnego działania w celu ochrony interesów podmiotów danych, podając przesłanki potrzeby przyjęcia takiej opinii, w tym potrzebę pilnego działania.

4. W drodze odstępstwa od art. 58 ust. 7, opinię w trybie pilnym, o której mowa w ust. 2 i 3 niniejszego artykułu, przyjmuje się w terminie dwóch tygodni zwykłą większością członków Europejskiej Rady Ochrony Danych.

Artykuł 62
Akty wykonawcze

1. Komisja może przyjmować akty wykonawcze, aby:

   a) rozstrzygnąć w sprawie właściwego i spójnego stosowania niniejszego rozporządzenia zgodnie z jego celami i wymogami w związku ze sprawami przekazanymi przez organy nadzorcze na mocy art. 58 lub art. 61, odnośnie do sprawy, w związku z którą przyjęto uzasadnioną decyzję na podstawie art. 60 ust. 1, lub odnośnie do sprawy, w związku z którą organ nadzorczy nie przedstawił projektu środka i poinformował, że nie zamierza postąpić zgodnie z opinią Komisji na mocy art. 59;

   b) rozstrzygnąć w okresie, o którym mowa w art. 59 ust. 1, w sprawie ogłoszenia projektu standardowych klauzul ochrony danych, o których mowa w art. 58 ust. 2 lit. d) jako ogólnie obowiązujących;

   c) określić formułę i procedurę stosowania mechanizmu zgodności, o którym mowa w niniejszej sekcji;

   d) określić zasady wymiany informacji drogą elektroniczną między organami nadzorczymi oraz między organami nadzorczymi i Europejską Radą Ochrony Danych, w szczególności standardowego formatu, o którym mowa w art. 58 ust. 5, 6 i 8.

   Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 87 ust. 2.

2. W przypadku należycie uzasadnionej, szczególnie pilnej potrzeby związanej z interesem podmiotów danych w przypadkach określonych w ust. 1 lit. a), Komisja przyjmuje akty wykonawcze mające natychmiastowe zastosowanie zgodnie z procedurą, o której mowa w art. 87 ust. 3. Akty te obowiązują nie dłużej niż 12 miesięcy.

3. Brak środka lub jego przyjęcie na podstawie niniejszej sekcji pozostaje bez uszczerbku dla każdego innego środka przyjętego przez Komisję na podstawie Traktatów.

Artykuł 63
Egzekwowanie

1. Dla celów niniejszego rozporządzenia egzekwowalny środek organu nadzorczego jednego państwa członkowskiego jest egzekwowany we wszystkich państwach członkowskich, których to dotyczy.

2. W przypadku gdy organ nadzorczy nie przedstawi projektu środka w mechanizmie zgodności, naruszając art. 58 ust. 1-5, środek tego organu nadzorczego nie jest ważny zgodnie z prawem i nie podlega wykonaniu.

SEKCJA 3
EUROPEJSKA RADA OCHRONY DANYCH

Artykuł 64
Europejska Rada Ochrony Danych

1. Niniejszym ustanawia się Europejską Radę Ochrony Danych.

2. Do Europejskiej Rady Ochrony Danych należą szef jednego organu nadzorczego każdego państwa członkowskiego oraz Europejski Inspektor Ochrony Danych.

3. W przypadku gdy w państwie członkowskim więcej niż jeden organ nadzorczy jest odpowiedzialny za monitorowanie stosowania przepisów na mocy niniejszego rozporządzenia, organy te powołują szefa jednego z tych organów nadzorczych jako wspólnego przedstawiciela.

4. Komisja ma prawo do udziału w działaniach i posiedzeniach Europejskiej Rady Ochrony Danych i wyznacza swojego przedstawiciela. Przewodniczący Europejskiej Rady Ochrony Danych informuje bezzwłocznie Komisję o wszystkich działaniach Europejskiej Rady Ochrony Danych.

Artykuł 65
Niezależność

1. Europejska Rada Ochrony Danych działa w toku wykonywania zadań na mocy art. 66 i 67 w sposób niezależny.

2. Bez uszczerbku dla wniosków Komisji, o których mowa w art. 66 ust. 1 lit. b) i ust. 2, Europejska Rada Ochrony Danych podczas wykonywania swoich zadań nie zwraca się do nikogo o instrukcje ani ich od nikogo nie przyjmuje.

Artykuł 66
Zadania Europejskiej Rady Ochrony Danych

1. Europejska Rada Ochrony Danych zapewnia spójne stosowanie niniejszego rozporządzenia. W tym celu Europejska Rada Ochrony Danych, z własnej inicjatywy lub na wniosek Komisji, podejmuje następujące działania:

a) doradza Komisji na temat każdej sprawy związanej z ochroną danych osobowych w Unii, w tym na temat każdego projektu zmian niniejszego rozporządzenia;

b) bada z własnej inicjatywy lub na wniosek jednego ze swoich członków lub Komisji każdą kwestię, której zakres obejmuje stosowanie niniejszego rozporządzenia i wydaje wytyczne, zalecenia oraz najlepsze praktyki skierowane do organów nadzorczych w celu zachęcenia do spójnego stosowania niniejszego rozporządzenia;

c) dokonuje przeglądu praktycznego zastosowania wytycznych, zaleceń oraz najlepszych praktyk, o których mowa w lit. b) i regularnie składa sprawozdania Komisji na ten temat;

d) wydaje opinie na temat projektów decyzji organów nadzorczych zgodnie z mechanizmem zgodności, o którym mowa w art. 57;

e) promuje współpracę i skuteczną dwustronną i wielostronną wymianę informacji i praktyk między organami nadzorczymi;

f) promuje wspólne programy szkoleń i ułatwia wymianę personelu między organami nadzorczymi, jak również, w stosownych przypadkach, z organami nadzorczymi państw trzecich lub organizacji międzynarodowych;

g) promuje wymianę wiedzy i dokumentów na temat ustawodawstwa i praktyki dotyczących ochrony danych z organami nadzorczymi na świecie.

2. W przypadku gdy Komisja zwraca się o opinię doradczą do Europejskiej Rady Ochrony Danych może określić termin, w jakim Europejska Rada Ochrony Danych wydaje taką opinię, przy uwzględnieniu pilności sprawy.

3. Europejska Rada Ochrony Danych przekazuje swoje opinie, wytyczne, zalecenia i najlepsze praktyki Komisji i komitetowi, o którym mowa w art. 87, oraz podaje je do wiadomości publicznej.

4. Komisja informuje Europejską Radę Ochrony Danych na temat działania podjętego na podstawie opinii, wytycznych, zaleceń i najlepszych praktyk wydanych przez Europejską Radę Ochrony Danych.

Artykuł 67
Sprawozdania

1. Europejska Rada Ochrony Danych regularnie i w terminie informuje Komisję na temat wyników swojej działalności. Sporządza roczne sprawozdanie na temat sytuacji dotyczącej ochrony osób fizycznych w odniesieniu do przetwarzania danych osobowych w Unii i państwach trzecich.

Sprawozdanie obejmuje przegląd praktycznego zastosowania opinii, wytycznych, zaleceń i opisów najlepszych praktyk, o których mowa w art. 66 ust. 1 lit. c).

2. Sprawozdanie jest podawane do wiadomości publicznej i przekazywane Parlamentowi Europejskiemu, Radzie i Komisji.

Artykuł 68
Procedura

1. Europejska Rada Ochrony Danych podejmuje decyzję zwykłą większością swoich członków.

2. Europejska Rada Ochrony Danych przyjmuje własny regulamin wewnętrzny i ustala własne zasady działania. W szczególności przyjmuje regulacje dotyczące dalszego wykonywania obowiązków przez członka w sytuacji, kiedy wygaśnie jego kadencja lub złoży on rezygnację, ustanowienia podgrup zajmujących się określonymi tematami lub sektorami oraz odnoszące się do procedur w związku z mechanizmem zgodności, o którym mowa w art. 57.

Artykuł 69
Przewodniczący

1. Europejska Rada Ochrony Danych wybiera przewodniczącego i dwóch wiceprzewodniczących spośród swoich członków. Europejski Inspektor Ochrony Danych pełni funkcję jednego z wiceprzewodniczących, chyba że został on wybrany na przewodniczącego.

2. Kadencja przewodniczącego i wiceprzewodniczących trwa pięć lat i jest odnawialna.

Artykuł 70
Zadania przewodniczącego

1. Przewodniczący ma następujące zadania:

   a) zwołuje posiedzenia Europejskiej Rady Ochrony Danych i sporządza ich porządek obrad;

   b) zapewnia terminowe wykonanie zadań Europejskiej Rady Ochrony Danych, w szczególności w związku z mechanizmem zgodności, o którym mowa w art. 57.

2. Europejska Rada Ochrony Danych określa podział zadań między przewodniczącego a wiceprzewodniczących w swoim regulaminie wewnętrznym.

Artykuł 71
Sekretariat

1. Europejska Rada Ochrony Danych ma do dyspozycji sekretariat: obsługę sekretariatu zapewnia Europejski Inspektor Ochrony Danych.

2. Sekretariat pod kierownictwem przewodniczącego zapewnia Europejskiej Radzie Ochrony Danych wsparcie analityczne, administracyjne i logistyczne.

3. Sekretariat jest w szczególności odpowiedzialny za:

a) bieżącą działalność Europejskiej Rady Ochrony Danych;

b) przekazywanie informacji między członkami Europejskiej Rady Ochrony Danych, jej przewodniczącym i Komisją oraz informowanie innych instytucji i opinii publicznej;

c) stosowanie środków elektronicznych do wewnętrznej i zewnętrznej komunikacji;

d) tłumaczenie odpowiednich informacji;

e) przygotowanie posiedzeń oraz działań następczych w stosunku do posiedzeń Europejskiej Rady Ochrony Danych;

f) przygotowanie, sporządzanie i publikowanie opinii i innych tekstów przyjętych przez Europejską Radę Ochrony Danych.

Artykuł 72
Poufność

1. Obrady Europejskiej Rady Ochrony Danych są poufne.

2. Dokumenty przedłożone członkom Europejskiej Rady Ochrony Danych, ekspertom i przedstawicielom osób trzecich są poufne, chyba że dostęp do tych dokumentów został przyznany zgodnie z rozporządzeniem nr 1049/2001 lub Europejska Rada Ochrony Danych w inny sposób podaje je do wiadomości publicznej.

3. Na członkach Europejskiej Rady Ochrony Danych, a także na ekspertach i przedstawicielach osób trzecich spoczywa obowiązek zachowania poufności, o którym mowa w niniejszym artykule. Przewodniczący dopilnuje, by eksperci i przedstawiciele osób trzecich zostali powiadomieni o wymogach poufności, które się na nich nakłada.

ROZDZIAŁ VIII

ŚRODKI OCHRONY PRAWNEJ, ODPOWIEDZIALNOŚĆ I SANKCJE

Artykuł 73
Prawo do złożenia skargi do organu nadzorczego

1. Bez uszczerbku dla innych administracyjnych lub sądowych środków ochrony prawnej, każdy podmiot danych ma prawo złożyć skargę do organu nadzorczego w dowolnym państwie członkowskim, jeżeli uznaje, że przetwarzanie danych osobowych ich dotyczących nie jest zgodne z przepisami niniejszego rozporządzenia.

2. Każdy podmiot, organizacja lub zrzeszenie, których celem jest ochrona praw podmiotów danych oraz interesów dotyczących ochrony ich danych osobowych, i które zostały prawidłowo ustanowione zgodnie z prawem państwa członkowskiego, ma prawo złożyć skargę do organu nadzorczego dowolnego państwa członkowskiego w imieniu jednego lub więcej podmiotów danych, jeżeli uznaje, że prawa podmiotu danych na podstawie niniejszego rozporządzenia zostały naruszone w wyniku przetwarzania danych osobowych.

3. Niezależnie od skargi podmiotu danych każdy podmiot, organizacja lub zrzeszenie, o których mowa w ust. 2, ma prawo złożyć skargę do organu nadzorczego w dowolnym państwie członkowskim, jeżeli uznaje, że doszło do naruszenia ochrony danych osobowych.

Artykuł 74

Prawo do sądowego środka ochrony prawnej przeciwko organowi nadzorczemu

1. Każda osoba fizyczna lub prawna ma prawo do sądowego środka ochrony prawnej od decyzji organu nadzorczego, które jej dotyczą.

2. Każdy podmiot danych ma prawo do sądowego środka ochrony prawnej zobowiązującego organ nadzorczy do podjęcia działania w sprawie skargi w przypadku braku decyzji chroniącej jego prawa lub w przypadku gdy organ nadzorczy nie poinformuje podmiotu danych w terminie trzech miesięcy o postępach w rozpatrywania skargi lub rezultatach jej rozpatrzenia na mocy art. 52 ust. 1 lit. b).

3. Postępowanie przeciwko organowi nadzorczemu wszczyna się przed sądem państwa członkowskiego, w którym organ nadzorczy ma siedzibę.

4. Podmiot danych, którego dotyczy decyzja organu nadzorczego w innym państwie członkowskim niż to, w którym podmiot danych ma miejsce zwykłego pobytu, może zażądać, aby organ nadzorczy państwa członkowskiego, w którym ma miejsce zwykłego pobytu, wszczął postępowanie w jego imieniu przeciwko właściwemu organowi nadzorczemu w innym państwie członkowskim.

5. Państwa członkowskie wykonują prawomocne orzeczenia sądów, o których mowa w niniejszym artykule.

Artykuł 75

Prawo do sądowego środka ochrony prawnej przeciwko administratorowi lub podmiotowi przetwarzającemu

1. Bez uszczerbku dla jakiegokolwiek dostępnego administracyjnego środka ochrony prawnej, w tym prawa do złożenia skargi do organu nadzorczego, o której mowa w art. 73, każda osoba fizyczna ma prawo do sądowego środka ochrony prawnej, jeżeli uznaje, że jej prawa na podstawie niniejszego rozporządzenia zostały naruszone w wyniku przetwarzania jej danych osobowych w warunkach niezgodnych z niniejszym rozporządzeniem.

2. Postępowanie przeciwko administratorowi i podmiotowi przetwarzającemu wszczyna się przed sądem państwa członkowskiego, w którym administrator lub

podmiot przetwarzający mają siedzibę. Alternatywnie takie postępowanie może być wszczęte przed sądem państwa członkowskiego, w którym podmiot danych ma miejsce zwykłego pobytu, chyba że administrator jest organem publicznym wykonującym swoje uprawnienia publiczne.

3. W przypadku gdy postępowanie toczy się w ramach mechanizmu zgodności, o którym mowa w art. 58, a dotyczy tego samego środka, decyzji lub praktyki, sąd może zawiesić postępowanie, które się przed nim toczy, chyba że pilny charakter sprawy dotyczącej ochrony praw podmiotu danych nie pozwala oczekiwać na wynik postępowania w ramach mechanizmu zgodności.

4. Państwa członkowskie wykonują prawomocne orzeczenia sądów, o których mowa w niniejszym artykule.

Artykuł 76
Wspólne zasady postępowań sądowych

1. Każdy podmiot, organizacja lub zrzeszenie, o których mowa w art. 73 ust. 2, ma prawo do wykonywania praw, o których mowa w art. 74 i 75, w imieniu jednego lub większej liczby podmiotów danych.

2. Każdy organ nadzorczy ma prawo wszcząć postępowanie prawne i wnieść sprawę do sądu w celu wykonania przepisów niniejszego rozporządzenia lub zapewnienia spójności ochrony danych osobowych na terytorium Unii.

3. W przypadku gdy właściwy sąd państwa członkowskiego ma uzasadnione powody, by sądzić, że równoległe postępowanie toczy się w innym państwie członkowskim, kontaktuje się z właściwym sądem innego państwa członkowskiego, aby potwierdzić fakt prowadzenia takiego równoległego postępowania.

4. W przypadku gdy równoległe postępowanie w drugim państwie członkowskim dotyczy tego samego środka, decyzji lub praktyki, sąd może zawiesić postępowanie.

5. Państwa członkowskie dopilnują, by skargi przewidziane w prawie krajowym umożliwiały szybkie przyjęcie środków, łącznie ze środkami tymczasowymi mającymi na celu przerwanie każdego domniemanego naruszenia prawa oraz zapobieżenie wszelkim dalszym naruszeniom przedmiotowych interesów.

Artykuł 77
Prawo do odszkodowania i odpowiedzialność

1. Każda osoba, która poniosła szkodę w wyniku niezgodnej z prawem operacji przetwarzania danych lub działania niezgodnego z przepisami ustanowionymi w niniejszym rozporządzeniu, ma prawo do odszkodowania od administratora lub podmiotu przetwarzającego, odpowiedzialnego za poniesioną szkodę.

2. Jeżeli w przetwarzaniu bierze udział więcej niż jeden administrator lub podmiot przetwarzający, każdy administrator i podmiot przetwarzający odpowiada solidarnie za całą kwotę odszkodowania.

3. Administrator lub podmiot przetwarzający może zastać zwolniony z tej odpowiedzialności, w całości lub w części, jeżeli udowodni, że nie jest odpowiedzialny za zdarzenie, które doprowadziło do powstania szkody.

Artykuł 78
Kary

1. Państwa członkowskie ustanawiają przepisy dotyczące kar stosowanych w przypadku naruszenia przepisów niniejszego rozporządzenia oraz przyjmują wszystkie środki niezbędne do zapewnienia, że są one wykonywane, w tym w sytuacji gdy administrator nie wypełnił obowiązku wyznaczenia swojego przedstawiciela. Przewidziane kary muszą być skuteczne, proporcjonalne i odstraszające.

2. W przypadku gdy administrator ustanowił przedstawiciela, wszystkie kary mają zastosowanie do przedstawiciela, bez uszczerbku dla jakiejkolwiek kary, która może grozić administratorowi.

3. Każde państwo członkowskie zawiadamia Komisję o przepisach prawa, które przyjęło na mocy ust. 1, najpóźniej w terminie określonym w art. 91 ust. 2 i bezzwłocznie o każdej kolejnej zmianie mającej na nie wpływ.

Artykuł 79
Sankcje administracyjne

1. Każdy organ nadzorczy jest uprawniony do nakładania sankcji administracyjnych zgodnie niniejszym artykułem.

2. Sankcja administracyjna w każdym indywidualnym przypadku jest skuteczna, proporcjonalna i odstraszająca. Kwotę grzywny administracyjnej określa się z należytym uwzględnieniem charakteru, powagi i czasu trwania naruszenia, umyślnego lub lekkomyślnego charakteru naruszenia, stopnia odpowiedzialności osoby fizycznej lub prawnej oraz poprzednich naruszeń popełnionych przez tą osobę, technicznych i organizacyjnych środków i procedur wdrażanych na mocy art. 23 i stopnia współpracy z organem nadzorczym w celu usunięcia naruszenia.

3. W przypadku zaistnienia pierwszego przypadku nieumyślnego naruszenia niniejszego rozporządzeniem nie nakłada się sankcji, lecz udziela ostrzeżenia na piśmie, w przypadku gdy:

   a) osoba fizyczna przetwarza dane osobowe nie dla celów handlowych; lub,

   b) przetwarzanie danych osobowych przez przedsiębiorstwo lub organizację zatrudniającą mniej niż 250 osób ma jedynie charakter poboczny w stosunku do głównej działalności.

4. Organ nadzorczy nakłada grzywnę do wysokości 250 000 EUR lub w przypadku przedsiębiorstwa do 0,5 % jego rocznego światowego obrotu, na każdy podmiot, który umyślnie lub lekkomyślnie:

a) nie ustanowił mechanizmów umożliwiających podmiotom danych składanie wniosków lub nie odpowiada podmiotom danych bezzwłocznie lub odpowiada nie w wymaganym formacie zgodnie z art. 12 ust. 1 i 2;

b) pobiera opłatę za informację lub odpowiedzi na wnioski podmiotów danych naruszając w ten sposób art. 12 ust. 4.

5. Organ nadzorczy nakłada grzywnę do wysokości 500 000 EUR lub w przypadku przedsiębiorstwa do 1 % jego rocznego światowego obrotu, na każdy podmiot, który umyślnie lub lekkomyślnie:

a) nie dostarcza podmiotom danych informacji lub nie dostarcza pełnych informacji lub nie dostarcza informacji w wystarczająco przejrzysty sposób zgodnie z art. 11, art. 12 ust. 3 i art. 14;

b) nie zapewnia dostępu podmiotom danych lub nie poprawia danych osobowych zgodnie z art. 15 i 16 lub nie przekazuje odpowiednich informacji odbiorcy zgodnie z art. 13;

c) nie respektuje prawa do bycia zapomnianym i do usunięcia danych lub nie wprowadza mechanizmów, aby zapewnić, że terminy są przestrzegane lub nie podejmuje wszelkich właściwych kroków, aby poinformować osoby trzecie, że podmioty danych zażądały wszystkich usunięcia linków do danych, lub kopii lub replikacji danych osobowych na podstawie art. 17;

d) nie dostarcza kopii danych osobowych w formie elektronicznej lub utrudnia podmiotowi danych przekazanie danych osobowych do innego zastosowania, naruszając art. 18;

e) nie określa w sposób wystarczający odpowiednich obowiązków współadministratorów danych zgodnie z art. 24;

f) nie prowadzi dokumentacji lub prowadzi ją w sposób niewystarczający na mocy art. 28, art. 31 ust. 4 i art. 44 ust. 3;

g) nie przestrzega, w przypadkach które dotyczą szczególnych kategorii danych, na mocy art. 80, 82 i 83, przepisów odnoszących się do wolności wypowiedzi lub do przetwarzania w kontekście zatrudnienia lub dotyczących warunków przetwarzania do celów dokumentacji, statystyki i badań naukowych.

6. Organ nadzorczy nakłada grzywnę do wysokości 1 000 000 EUR lub w przypadku przedsiębiorstwa do 2 % jego rocznego światowego obrotu, na każdy podmiot, który umyślnie lub lekkomyślnie:

a) przetwarza dane osobowe bez żadnej lub wystarczającej podstawy prawnej przetwarzania lub nie przestrzega warunków dotyczących uzyskania zgody na mocy art. 6, 7 i 8;

b) przetwarza szczególne kategorie danych niezgodnie z art. 9 i art. 81;

c) nie respektuje sprzeciwu lub wymogu na mocy art. 19;

d) nie przestrzega warunków odnoszących się do środków opartych na profilowaniu na mocy art. 20;

e) nie przyjmuje wewnętrznych polityk lub nie wdraża właściwych środków w celu zapewnienia i wykazania zgodności na mocy art. 22, 23 i 30;

f) nie wyznacza przedstawiciela na mocy art. 25;

g) przetwarza lub wydaje polecenie przetwarzania danych osobowych, z naruszeniem obowiązków odnoszących się do przetwarzania w imieniu administratora na mocy art. 26 i 27;

h) nie ostrzega, ani nie zawiadamia o naruszeniu ochrony danych osobowych lub nie zawiadamia terminowo i w całości o naruszeniu danych organu nadzorczego lub podmiotu danych na mocy art. 31 i 32;

i) nie przeprowadza oceny skutków w zakresie ochrony danych lub przetwarza dane osobowe bez uzyskania uprzedniej zgody organu nadzorczego lub bez uprzednich konsultacji z nim na mocy art. 33 i 34;

j) nie wskazuje inspektora ochrony danych lub nie zapewnia warunków umożliwiających wykonanie zadań na mocy art. 35, 36 i 37;

k) nadużywa pieczęci lub oznaczeń w zakresie ochrony danych w rozumieniu art. 39;

l) wykonuje lub zleca przekazanie danych do państwa trzeciego lub organizacji międzynarodowej, na co nie zezwala decyzja stwierdzająca odpowiedni poziom ochrony lub odpowiednie gwarancje lub odstępstwo na mocy art. 40-44;

m) nie przestrzega nakazu lub tymczasowego albo ostatecznego zakazu dotyczącego przetwarzania lub zawieszenia przepływu danych przez organ nadzorczy na podstawie art. 53 ust. 1;

n) nie przestrzega obowiązków dotyczących udzielenia pomocy lub odpowiedzi lub dostarczenia odpowiednich informacji organowi nadzorczemu lub udostępnienia mu pomieszczeń na mocy art. 28 ust. 3, art. 29, art. 34 ust. 6 i art. 53 ust. 2;

o) nie przestrzega przepisów dotyczących zachowaniu tajemnicy służbowej na mocy art. 84.

7. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 86 w celu aktualizacji kwot grzywien administracyjnych, o których mowa ust. 4, 5 i 6, biorąc pod uwagę warunki, o których mowa ust. 2.

ROZDZIAŁ IX
PRZEPISY DOTYCZĄCE OKREŚLONYCH SYTUACJI ZWIĄZANYCH Z PRZETWARZANIEM DANYCH

Artykuł 80
Przetwarzanie danych osobowych i wolność wypowiedzi

1. Państwa członkowskie stanowią przepisy przewidujące wyłączenia i odstępstwa od przepisów dotyczące ogólnych zasad w rozdziale II, praw podmiotów danych w rozdziale III, administratora i podmiotu przetwarzającego w rozdziale IV, przekazywania danych osobowych do państw trzecich w rozdziale V, niezależnych organów nadzorczych w rozdziale VI oraz współpracy i zgodności w rozdziale VII w przypadku przetwarzania danych osobowych wyłącznie w celach dziennikarskich lub w celu uzyskania wyrazu artystycznego lub literackiego, aby pogodzić prawo do ochrony danych osobowych z przepisami dotyczącymi wolności wypowiedzi.

2. Każde państwo członkowskie zawiadamia Komisję o przepisach prawa, które przyjęło na mocy ust. 1, najpóźniej w terminie określonym w art. 91 ust. 2 i bezzwłocznie o każdym kolejnym akcie zmieniającym lub zmianie, które mają na nie wpływ.

Artykuł 81
Przetwarzanie danych osobowych dotyczących zdrowia

1. W granicach niniejszego rozporządzenia i zgodnie z art. 9 ust. 2 lit. h) przetwarzanie danych osobowych dotyczących zdrowia musi odbywać się na podstawie prawa Unii lub prawa państwa członkowskiego, które przewiduje odpowiednie i konkretne środki mające na celu zabezpieczenie uzasadnionych interesów podmiotu danych i które są niezbędne:

   a) dla celów medycyny prewencyjnej lub medycyny pracy, diagnostyki medycznej, opieki lub leczenia lub zarządzania opieką zdrowotną, w przypadkach, gdy dane te są przetwarzane przez pracownika służby zdrowia podlegającego obowiązkowi zachowania tajemnicy zawodowej lub przez inną osobę również podlegającą równoważnemu obowiązkowi zachowania poufności na podstawie prawa państwa członkowskiego lub przepisów ustanowionych przez właściwe organy krajowe; lub

   b) ze względu na interes publiczny w dziedzinie zdrowia publicznego, taki jak ochrona przed poważnymi transgranicznymi zagrożeniami dla zdrowia lub zapewnienie wysokich standardów jakości i bezpieczeństwa, między innymi w przypadku produktów leczniczych lub wyrobów medycznych; lub

   c) ze względu na inne przesłanki z zakresu interesu publicznego w takich obszarach jak ochrona socjalna, szczególnie w celu zapewnienia odpowiedniej jakości i efektywności ekonomicznej procedur stosowanych do rozstrzygania roszczeń w sprawie świadczeń i usług w ramach systemu ubezpieczeń zdrowotnych.

2. Przetwarzanie danych osobowych dotyczących zdrowia, które jest niezbędne do celów dokumentacji, statystyki i badań naukowych, takie jak prowadzenie rejestrów pacjentów założonych w celu udoskonalenia diagnostyki i rozróżnienia między podobnymi rodzajami chorób i przygotowania opracowań dotyczących terapii, podlega warunkom i gwarancjom, o których mowa w art. 83.

3. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 86 w celu dalszego określenia innych przesłanek z zakresu interesu publicznego w obszarze zdrowia publicznego, o których mowa ust. 1 lit. b), jak również kryteriów i wymogów dla gwarancji przetwarzanie danych osobowych dla celów, o których mowa w ust. 1.

Artykuł 82

Przetwarzanie w kontekście zatrudnienia

1. W granicach niniejszego rozporządzenia państwa członkowskie mogą przyjąć przepisy szczególne regulujące przetwarzanie danych osobowych pracowników w kontekście zatrudnienia, w szczególności dla celów procedury rekrutacyjnej, wykonania umowy o pracę, w tym zwolnienia z obowiązków określonych przez przepisy prawa lub przez umowy zbiorowe, zarządzania, planowania i organizacji pracy, bezpieczeństwa i higieny pracy, oraz dla celów wykonywania praw i korzystania ze świadczeń związanych z zatrudnieniem, indywidualnie lub zbiorowo, oraz dla celu zakończenia stosunku pracy.

2. Każde państwo członkowskie zawiadamia Komisję o przepisach prawa, które przyjęło na mocy ust. 1, najpóźniej w terminie określonym w art. 91 ust. 2 i bezzwłocznie o każdej kolejnej zmianie mającej na nie wpływ.

3. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 86 w celu dalszego określenia innych warunków i wymogów gwarancji przetwarzania danych osobowych dla celów, o których mowa w ust. 1.

Artykuł 83

Przetwarzanie do celów dokumentacji, statystyki i badań naukowych

1. W granicach niniejszego rozporządzenia można przetwarzać dane osobowe do celów dokumentacji, statystyki i badań naukowych jedynie wtedy, gdy:

   a) nie można ich inaczej osiągnąć przez przetwarzanie danych, które nie umożliwia lub przestaje umożliwiać identyfikację osoby, której dane dotyczą;

   b) dane umożliwiające przypisanie informacji do zidentyfikowanej podmiotu danych lub do zidentyfikowania, są przechowywane oddzielnie od innych informacji, tak długo jak cele te można osiągnąć w ten sposób.

2. Podmioty prowadzące badania historyczne, statystyczne lub naukowe mogą publikować lub ujawniać publicznie w inny sposób dane osobowe jedynie wtedy, gdy:

a) podmiot danych udzielił zgody, z zastrzeżeniem warunków ustanowionych w art. 7;

b) publikacja danych osobowych jest niezbędna do zaprezentowania ustaleń uzyskanych w wyniku badań lub do ułatwienia badań w takim zakresie, w jakim interesy lub podstawowe prawa i wolności podmiotu danych nie mają charakteru nadrzędnego; lub

c) osoba, której dane dotyczą podała dane do wiadomości publicznej.

3. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 86 w celu dalszego określenia kryteriów i wymogów gwarancji przetwarzania danych osobowych dla celów, o których mowa w ust. 1 i ust. 2, jak również niezbędnych ograniczeń prawa do informacji i dostępu przysługującego podmiotowi danych oraz doprecyzowania warunków praw podmiotów danych w tych okolicznościach i gwarancji tych praw.

Artykuł 84

Obowiązki dotyczące zachowania tajemnicy

1. W granicach niniejszego rozporządzenia państwa członkowskie mogą przyjąć przepisy szczególne określające uprawnienia dochodzeniowe organów nadzorczych ustanowione w art. 53 ust. 2 w odniesieniu do administratorów i podmiotów przetwarzających, którzy podlegają obowiązkowi zachowania tajemnicy zawodowej lub innym równoważnym obowiązkom zachowania tajemnicy na podstawie prawa krajowego lub przepisów ustanowionych przez właściwe podmioty krajowe, w przypadku gdy jest to konieczne i proporcjonalne dla pogodzenia prawa do ochrony danych osobowych i obowiązku zachowania tajemnicy. Niniejsze przepisy stosuje się w odniesieniu do danych osobowych, które administrator lub podmiot przetwarzający otrzymał lub uzyskał w działaniu objętym obowiązkiem zachowania tajemnicy.

2. Każde państwo członkowskie zawiadamia Komisję o przepisach prawa przyjętych na mocy ust. 1 najpóźniej w terminie określonym w art. 91 ust. 2 i bezzwłocznie o każdej kolejnej zmianie mającej na nie wpływ.

Artykuł 85

Obowiązujące przepisy dotyczące ochrony danych stosowane przez kościoły i związki wyznaniowe

1. W przypadku gdy państwo członkowskie, kościoły i związki lub wspólnoty wyznaniowe stosują, w momencie wejścia w życie niniejszego rozporządzenia, kompleksowe regulacje dotyczące ochrony jednostek w odniesieniu do przetwarzania danych osobowych, regulacje takie mogą być nadal stosowane, pod warunkiem że są dostosowane do przepisów niniejszego rozporządzenia.

2. Kościoły i związki wyznaniowe, które stosują kompleksowe regulacje zgodnie z ust. 1, stanowią regulacje przewidujące ustanowienie niezależnego organu nadzorczego zgodnie z rozdziałem VI niniejszego rozporządzenia.

ROZDZIAŁ X
AKTY DELEGOWANE I WYKONAWCZE

Artykuł 86
Wykonywanie przekazanych uprawnień

1. Powierzenie Komisji uprawnień do przyjęcia aktów delegowanych podlega warunkom określonym w niniejszym artykule.

2. Uprawnienia do przyjęcia aktów delegowanych, o których mowa w art. 6 ust. 5, art. 8 ust. 3, art. 9 ust. 3, art. 12 ust. 5, art. 14 ust. 7, art. 15 ust. 3, art. 17 ust. 9, art. 20 ust. 6, art. 22 ust. 4, art. 23 ust. 3, art. 26 ust. 5, art. 28 ust. 5, art. 30 ust. 3, art. 31 ust. 5, art. 32 ust. 5, art. 33 ust. 6, art. 34 ust. 8, art. 35 ust. 11, art. 37 ust. 2, art. 39 ust. 2, art. 43 ust. 3, art. 44 ust. 7, art. 79 ust. 6, art. 81 ust. 3, art. 82 ust. 3 i art. 83 ust. 3, powierza się Komisji na czas nieokreślony od dnia wejścia w życie niniejszego rozporządzenia.

3. Przekazanie uprawnień, o którym mowa w art. 6 ust. 5, art. 8 ust. 3, art. 9 ust. 3, art. 12 ust. 5, art. 14 ust. 7, art. 15 ust. 3, art. 17 ust. 9, art. 20 ust. 6, art. 22 ust. 4, art. 23 ust. 3, art. 26 ust. 5, art. 28 ust. 5, art. 30 ust. 3, art. 31 ust. 5, art. 32 ust. 5, art. 33 ust. 6, art. 34 ust. 8, art. 35 ust. 11, art. 37 ust. 2, art. 39 ust. 2, art. 43 ust. 3, art. 44 ust. 7, art. 79 ust. 6, art. 81 ust. 3, art. 82 ust. 3 i art. 83 ust. 3, może zostać w dowolnym momencie odwołane przez Parlament Europejski lub przez Radę. Decyzja o odwołaniu kończy przekazanie określonych w niej uprawnień. Decyzja o odwołaniu staje się skuteczna od następnego dnia po jej opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej* lub w określonym w tej decyzji późniejszym terminie. Nie wpływa ona na ważność jakichkolwiek już obowiązujących aktów delegowanych.

4. Niezwłocznie po przyjęciu aktu delegowanego Komisja przekazuje go równocześnie Parlamentowi Europejskiemu i Radzie.

5. Akt delegowany przyjęty na podstawie art. art. 6 ust. 5, art. 8 ust. 3, art. 9 ust. 3, art. 12 ust. 5, art. 14 ust. 7, art. 15 ust. 3, art. 17 ust. 9, art. 20 ust. 6, art. 22 ust. 4, art. 23 ust. 3, art. 26 ust. 5, art. 28 ust. 5, art. 30 ust. 3, art. 31 ust. 5, art. 32 ust. 5, art. 33 ust. 6, art. 34 ust. 8, art. 35 ust. 11, art. 37 ust. 2, art. 39 ust. 2, art. 43 ust. 3, art. 44 ust. 7, art. 79 ust. 6, art. 81 ust. 3, art. 82 ust. 3 i art. 83 ust. 3 wchodzi w życie tylko jeśli Parlament Europejski albo Rada nie wyraziły sprzeciwu w terminie dwóch miesięcy od przekazania tego aktu Parlamentowi Europejskiemu i Radzie, lub jeśli, przed upływem tego terminu, zarówno Parlament Europejski, jak i Rada poinformowały Komisję, że nie wniosą sprzeciwu. Termin ten przedłuża się o dwa miesiące z inicjatywy Parlamentu Europejskiego lub Rady.

Artykuł 87
Procedura komitetowa

1. Komisję wspomaga komitet. 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.

3. W przypadku odesłania do niniejszego ustępu stosuje się art. 8 rozporządzenia (UE) nr 182/2011 w związku z jego art. 5.

ROZDZIAŁ XI
PRZEPISY KOŃCOWE

Artykuł 88
Uchylenie dyrektywy 95/46/WE

1. Uchyla się dyrektywę 95/46/WE.

2. Odesłania do uchylonej dyrektywy należy odczytywać jako odesłania do niniejszego rozporządzenia. Odniesienia do Grupy Roboczej ds. Ochrony Osób Fizycznych w zakresie Przetwarzania Danych Osobowych ustanowionej w art. 29 dyrektywy 95/46/WE należy odczytywać jako odniesienia do Europejskiej Rady Ochrony Danych ustanowionej w niniejszym rozporządzeniu.

Artykuł 89
Stosunek do dyrektywy 2002/58/WE i jej zmiana

1. Niniejsze rozporządzenie nie nakłada dodatkowych obowiązków na osoby fizyczne i prawne w odniesieniu do przetwarzania danych w związku z ogólnie dostępnymi usługami łączności elektronicznej w publicznych sieciach łączności na terenie Unii w sprawach, w których podmioty te podlegają szczególnym obowiązkom służącym temu samemu celowi określonemu w dyrektywie 2002/58/WE.

2 Skreśla się art. 1 ust. 2 dyrektywy 2002/58/WE.

Artykuł 90
Ocena

Komisja przedstawia Parlamentowi Europejskiemu i Radzie sprawozdania na temat oceny i przeglądu niniejszego rozporządzenia w regularnych odstępach czasu. Pierwsze sprawozdanie przedstawia się najpóźniej cztery lata po wejściu w życie niniejszego rozporządzenia. Kolejne sprawozdania przedstawia się następnie co cztery lata. Komisja, jeżeli jest to konieczne, przedkłada odpowiednie propozycje w celu zmiany niniejszego rozporządzenia oraz dostosowania innych instrumentów prawnych, w szczególności biorąc pod uwagę rozwój technologii informacyjnych oraz postęp zachodzący w społeczeństwie informacyjnym. Sprawozdania są podawane do wiadomości publicznej.

Artykuł 91

Wejście w życie i stosowanie

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

2. Niniejsze rozporządzenie stosuje się od [*dwa lata od daty, o której mowa w ust. 1*].

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

Sporządzono w Brukseli, dnia 25.1.2012 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. Dziedzina(-y) polityki w strukturze ABM/ABB, których dotyczy wniosek/inicjatywa

1.3. Charakter wniosku/inicjatywy

1.4. Cel/cele

1.5. Uzasadnienie wniosku/inicjatywy

1.6. Czas trwania działania i jego wpływu finansowego

1.7. Przewidywany(-e) tryb(-y) 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. Dział(y) wieloletnich ram finansowych i pozycja(pozycje) wydatków w budżecie, 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

Niniejsza ocena skutków finansowych doprecyzowuje wymogi w zakresie wydatków administracyjnych, które należy ponieść, aby przeprowadzić reformę ochrony danych, co zostało wyjaśnione w ocenie skutków dotyczącej tej kwestii. Reforma obejmuje dwa wnioski ustawodawcze: ogólne rozporządzenie o ochronie danych i dyrektywę w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy na potrzeby zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich i ścigania albo wykonywania kar kryminalnych. Niniejsza ocena skutków finansowych dotyczy wpływu obu instrumentów na budżet.

Zgodnie z podziałem zadań środki są potrzebne Komisji oraz Europejskiemu Inspektorowi Ochrony Danych (EIOD).

W odniesieniu do Komisji niezbędne środki zostały już włączone do proponowanej perspektywy finansowej na lata 2014–2020. Ochrona danych jest jednym z celów programu „Prawa podstawowe i obywatelstwo”, który również wspiera działania mające na celu wprowadzenie w życie ram prawnych. Środki administracyjne, w tym zapotrzebowanie na personel, zostały uwzględnione w budżecie administracyjnym DG JUST.

W odniesieniu do EIOD niezbędne środki należy uwzględnić w odpowiednich rocznych budżetach EIOD. Środki zostały wykazane szczegółowo w załączniku do niniejszej oceny skutków finansowych. W celu zapewnienia zasobów potrzebnych do wykonywania nowych zadań przez Europejską Radę Ochrony Danych, której sekretariat będzie obsługiwany przez EIOD, konieczne będzie przeprogramowanie działu 5 perspektywy finansowej na lata 2014–2020.

1.1. Tytuł wniosku/inicjatywy

Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych)

Wniosek dotyczący dyrektywy Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy na potrzeby zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich i ścigania albo wykonywania kar kryminalnych oraz swobodnego przepływu takich danych

1.2. Dziedzina(-y) polityki w strukturze ABM/ABB, których dotyczy wniosek/inicjatywa[49]

Wymiar sprawiedliwości – ochrona danych osobowych

Wpływ na budżet dotyczy Komisji i EIOD. Wpływ na budżet Komisji został szczegółowo wykazany w tabelach niniejszej oceny skutków finansowych. Wydatki operacyjne są częścią programu „Prawa podstawowe i obywatelstwo" i zostały już uwzględnione w ocenie skutków finansowych programu, podobnie jak wydatki administracyjne – w kopercie DG ds. Sprawiedliwości. Elementy dotyczące EIOD zostały przedstawione w załączniku.

1.3. Charakter wniosku/inicjatywy

☐ Wniosek/inicjatywa dotyczy **nowego działania**

☐ Wniosek/inicjatywa dotyczy **nowego działania będącego następstwem projektu pilotażowego/działania przygotowawczego**[50]

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

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

1.4. Cele

1.4.1. Wieloletni(e) cel(e) strategiczny(-e) Komisji wskazany(-e) we wniosku/inicjatywie

Reforma ma na celu uzupełnienie osiągnięć pierwotnych celów, biorąc pod uwagę najnowsze zmiany i wyzwania, tj.:

- wzrost skuteczności prawa podstawowego do ochrony danych i umożliwienie osobom fizycznym kontroli nad swoimi danymi, w szczególności w kontekście zmian technologicznych i wzrastającej globalizacji;

- poprawa wymiaru ochrony danych związanego z rynkiem wewnętrznym poprzez ograniczenie rozdrobnienia, wzmocnienie spójności i uproszczenie otoczenia regulacyjnego, a tym samym zlikwidowanie niepotrzebnych kosztów i ograniczenie ciężaru administracyjnego;

Dodatkowo wejście w życie traktatu lizbońskiego – w szczególności wprowadzenie nowej podstawy prawnej (art. 16 TFUE) – daje szansę na osiągnięcie nowego celu, tj.

- ustanowienie kompleksowych ram ochrony danych obejmujących wszystkie obszary.

---

49 ABM: Activity Based Management: zarządzanie kosztami działań - ABB: Activity Based Budgeting: budżet zadaniowy.

50 O którym mowa w art. 49 ust. 6 lit. a) lub b) rozporządzenia finansowego.

1.4.2. Cel(e) szczegółowy(-e) i działanie(-a) ABM/ABB, których dotyczy wniosek/inicjatywa

Cel szczegółowy nr 1: zapewnić spójne egzekwowanie przepisów dotyczących ochrony danych Cel szczegółowy nr 2: zracjonalizować obecny system zarządzania, aby pomóc w zapewnieniu bardziej spójnego wdrożenia Działanie(-a) ABM/ABB, którego(-ych) dotyczy wniosek/inicjatywa […]

1.4.3. Oczekiwany(-e) wynik(i) i wpływ

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

W odniesieniu do administratorów, zarówno podmioty publiczne, jak i prywatne, skorzystają z większej pewności prawnej dzięki zharmonizowanym i jaśniejszym przepisom i procedurom UE dotyczącym ochrony danych, tworząc równe szanse i zapewniając spójne wdrażanie przepisów dotyczących ochrony danych, a także znaczące ograniczenie ciężaru administracyjnego.

Osoby fizyczne będą mogły lepiej kontrolować swoje dane osobowe i będą miały zaufanie do otoczenia cyfrowego, nadal korzystając z ochrony, w tym w przypadku gdy ich dane są przetwarzane za granicą. Wzrośnie również odpowiedzialność podmiotów przetwarzających dane osobowe.

Kompleksowy system ochrony danych będzie również obejmował obszary związane z policją i wymiarem sprawiedliwości, włącznie z dawnym trzecim filarem i poza nim.

1.4.4. Wskaźniki wyników i wpływu

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

(Zobacz ocena skutków, sekcja 8)

Wskaźniki są oceniane okresowo i obejmą następujące elementy:

- czas i koszty poniesione przez administratorów danych na uzgodnienie z ustawodawstwem „innych państw członkowskich”;
- środki przydzielone organom ds. ochrony danych;
- ustanowienie inspektorów ochrony danych w publicznych i prywatnych podmiotach;
- wykorzystanie oceny skutków w zakresie ochrony danych;
- liczba skarg złożonych przez podmioty danych i odszkodowanie otrzymane przez podmioty danych;
- liczba spraw, w których wszczęto postępowanie przeciwko administratorom danych;
- grzywny nałożone na administratorów odpowiedzialnych za naruszenie ochrony danych.

1.5. Uzasadnienie wniosku/inicjatywy

1.5.1. Potrzeba(-y), która(-e) ma(-ją) zostać zaspokojona(-e) w perspektywie krótko- lub długoterminowej

Obecne rozbieżności we wdrażaniu, wykładni i wykonaniu dyrektywy przez państwa członkowskie ***utrudniają funkcjonowanie rynku wewnętrznego i współpracę między organami publicznymi w odniesieniu do polityk UE.*** Dzieje się to wbrew podstawowemu celowi dyrektywy, jakim jest ułatwienie swobodnego przepływu danych osobowych na rynku

wewnętrznym. Szybki rozwój nowych technologii i globalizacja jeszcze bardziej zaostrzają ten problem.

Osoby fizyczne korzystają z różnych praw ochrony danych, ze względu na ich rozdrobnienie i niespójne wdrażanie i egzekwowanie w różnych państwach członkowskich. Ponadto osoby fizyczne ***nie są ani świadome, ani nie mają kontroli nad tym, co się dzieje z ich danymi osobowymi***, a zatem nie są w stanie skutecznie korzystać ze swoich praw.

1.5.2. Wartość dodana z tytułu zaangażowania Unii Europejskiej

W obecnej sytuacji państwa członkowskie nie są w stanie same zredukować problemów. Dotyczy to w szczególności problemów pojawiających się w wyniku rozdrobnienia w przepisach krajowych wdrażających europejskie ramy regulujące ochronę danych. Istnieją zatem poważne przesłanki ustanowienia ram prawnych dla ochrony danych na poziomie UE. Istnieje w szczególności potrzeba ustanowienia zharmonizowanych i spójnych ram pozwalających na sprawne przekazywanie danych osobowych ponad granicami w Unii Europejskiej, przy jednoczesnym zapewnieniu skutecznej ochrony wszystkich osób fizycznych w całej UE.

1.5.3. Główne wnioski wyciągnięte z podobnych działań

Przedstawione wnioski opierają się na doświadczeniach zyskanych przy dyrektywie 95/46/WE i problemach, z którymi trzeba było się zmierzyć z powodu rozdrobnienia przepisów dokonujących transpozycji i wdrożenia dyrektywy, które zablokowało osiągnięcie obu jej celów, tj. wysokiego poziomu ochrony danych i jednolitego rynku ochrony danych.

1.5.4. Spójność z ewentualnymi innymi instrumentami finansowymi oraz możliwa synergia

Obecny pakiet dotyczący reformy w zakresie ochrony danych ma na celu opracowanie stabilnych, spójnych i nowoczesnych ram ochrony danych na szczeblu UE – neutralnych pod względem technologicznym i odpornych na zmiany, które przyniosą następne dziesięciolecia. Będzie on korzystny dla osób fizycznych dzięki wzmocnieniu ich praw do ochrony danych, w szczególności w środowisku cyfrowym, i uprości otoczenie prawne dla podmiotów gospodarczych i sektora publicznego, tym samym stymulując rozwój gospodarki cyfrowej na rynku wewnętrznym UE i poza nim, zgodnie z celami strategii „Europa 2020”.

Głównymi dokumentami, które tworzą pakiet dotyczący reformy w zakresie ochrony danych, są:

– rozporządzenie zastępujące dyrektywę 95/46/WE;

– dyrektywa w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy na potrzeby zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich i ścigania albo wykonywania kar kryminalnych oraz swobodnego przepływu takich danych.

Do wniosków ustawodawczych dołączono sprawozdanie z wdrożenia przez państwa członkowskie aktu, który jest obecnie głównym instrumentem UE w zakresie ochrony danych

w obszarze współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych, tj. decyzji ramowej 2008/977/WSiSW.

1.6. Czas trwania działania i jego wpływu finansowego

☐ Wniosek/inicjatywa o **określonym czasie trwania**

1. ☐ Czas trwania wniosku/inicjatywy: od [DD/MM]RRRR r. do [DD/MM]RRRR r.

2. ☐ Czas trwania wpływu finansowego: od RRRR r. do RRRR r.

☑ Wniosek/inicjatywa **o nieokreślonym czasie trwania**

1. Wprowadzenie w życie z okresem rozruchu od 2014 r. do 2016 r.,

2. po którym następuje faza operacyjna.

1.7. Przewidywany(-e) tryb(y) zarządzania[51]

☑ **Bezpośrednie zarządzanie scentralizowane** przez Komisję

☐ **Pośrednie zarządzanie scentralizowane** poprzez przekazanie zadań wykonawczych:

3. ☐ agencjom wykonawczym

4. ☐ organom utworzonym przez Wspólnoty[52]

5. ☐ krajowym organom publicznym/organom mającym obowiązek świadczenia usługi publicznej

3. ☐ osobom odpowiedzialnym za wykonanie określonych działań na mocy tytułu V Traktatu o Unii Europejskiej, określonym we właściwym prawnym akcie podstawowym w rozumieniu art. 49 rozporządzenia finansowego

☐ **Zarządzanie dzielone** z państwami członkowskimi

☐ **Zarządzanie zdecentralizowane** z państwami trzecimi

☐ **Zarządzanie wspólne** z organizacjami międzynarodowymi ***(należy wyszczególnić)***

W przypadku wskazania więcej niż jednego trybu, należy podać dodatkowe informacje w części „Uwagi".

Uwagi

//

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

[52] O którym mowa w art. 185 rozporządzenia finansowego.

2. ŚRODKI ZARZĄDZANIA

2.1. Zasady nadzoru i sprawozdawczości

Należy określić częstotliwość i warunki.

Pierwsza ocena zostanie dokonana cztery lata po wejściu w życie instrumentów prawnych. W instrumentach prawnych przewidziano wyraźną klauzulę przeglądu, na podstawie której Komisja będzie dokonywać oceny wdrażania. Komisja będzie następnie przedstawiać sprawozdanie ze swojej oceny Parlamentowi Europejskiemu i Radzie. Dalsze oceny będą się odbywać co cztery lata. Komisja będzie wykorzystywać wypracowaną przez siebie metodologię oceny. Powyższe oceny będą przeprowadzane za pomocą ukierunkowanych analiz wdrażania instrumentów prawnych, kwestionariuszy skierowanych do krajowych organów ds. ochrony danych, dyskusji ekspertów, warsztatów, ankiet Eurobarometru itp.

2.2. System zarządzania i kontroli

2.2.1. Zidentyfikowane ryzyko

Do wniosków dotyczących rozporządzenia i dyrektywy dołączono ocenę skutków, która została sporządzona dla reformy ram ochrony danych w UE.

Nowy instrument prawny wprowadzi mechanizm zgodności, dzięki któremu niezależne organy nadzorcze w państwach członkowskich będą stosować powyższe ramy w spójny i jednolity sposób. Mechanizm ten będzie funkcjonował za pośrednictwem Europejskiej Rady Ochrony Danych, składającej się z szefów krajowych organów nadzorczych i Europejskiego Inspektora Ochrony Danych (EIOD), która zastąpi obecną Grupę Roboczą Art. 29. EIOD zapewni obsługę sekretariatu tego podmiotu.

W przypadku ewentualnych sprzecznych decyzji organów nadzorczych państw członkowskich zostaną przeprowadzone konsultacje z Europejską Radą Ochrony Danych w celu uzyskania jej opinii w przedmiotowych kwestiach. Jeśli powyższa procedura zawiedzie lub jeżeli organ nadzorczy odmówi zastosowania się do opinii, Komisja może, w celu zapewnienia właściwego i spójnego stosowania niniejszego rozporządzenia, sama wydać opinię lub, w stosownych przypadkach, podjąć decyzję, jeżeli ma poważne wątpliwości co do tego, czy projekt środka zapewniłby właściwe stosowanie niniejszego rozporządzenia czy też przeciwnie – wiązałby się z jego niespójnym stosowaniem.

Na funkcjonowanie mechanizmu zgodności niezbędne są dodatkowe środki dla EIOD (12 osób zatrudnionych na pełnym etacie oraz odpowiednie środki administracyjne i operacyjne, np. na systemy i operacje informatyczne), aby zapewnić obsługę sekretariatu, a także dla Komisji (5 osób zatrudnionych na pełnym etacie oraz odpowiednie środki administracyjne i operacyjne) na obsługę spraw objętych mechanizmem zgodności.

2.2.2. Przewidywane metody kontroli

Obecne metody kontroli stosowane przez EIOD i Komisję obejmą dodatkowe środki.

2.3. Środki zapobiegania nadużyciom finansowym i nieprawidłowościom

Określić istniejące lub przewidywane środki zapobiegania i ochrony

Obecne środki zapobiegania nadużyciom finansowym i nieprawidłowościom stosowane przez EIOD i Komisję obejmą dodatkowe środki.

3. SZACUNKOWY WPŁYW FINANSOWY WNIOSKU/INICJATYWY

3.1. Dział(y) wieloletnich ram finansowych i pozycja(pozycje) wydatków w budżecie, na które wniosek/inicjatywa ma wpływ

1. Istniejące pozycje w budżecie

Według działów wieloletnich ram finansowych i pozycji w budżecie

Dział wieloletnich ram finansowych	Pozycja w budżecie	Rodzaj środków	Wkład			
	Numer [Treść…..….]	Zróżnicowane /niezróżnicowane[53]	państw EFTA[54]	krajów kandydujących[55]	państw trzecich	w rozumieniu art. 18 ust. 1 lit. aa) rozporządzenia finansowego

3.2. Szacunkowy wpływ na wydatki

3.2.1. Synteza szacunkowego wpływu na wydatki

w mln EUR (do 3 miejsc po przecinku)

Dział wieloletnich ram finansowych:	Numer	

			Rok **N**[56]**= 2014**	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										

53 Środki zróżnicowane/ środki niezróżnicowane
54 EFTA: Europejskie Stowarzyszenie Wolnego Handlu
55 Kraje kandydujące oraz w stosownych przypadkach potencjalne kraje kandydujące Bałkanów Zachodnich.
56 Rok N jest rokiem, w którym rozpoczyna się wprowadzanie w życie wniosku/inicjatywy.

Numer pozycji w budżecie	Środki na zobowiązania	(1)								
	Środki na płatności	(2)								
Numer pozycji w budżecie	Środki na zobowiązania	(1a)								
	Środki na płatności	(2a)								
Środki administracyjne finansowane ze środków przydzielonych na określone programy operacyjne[57]										
Numer pozycji w budżecie		(3)								
OGÓŁEM środki dla dyrekcji generalnej	Środki na zobowiązania	=1+1a +3								
	Środki na płatności	=2+2a +3								

• OGÓŁEM środki operacyjne	Środki na zobowiązania	(4)								
	Środki na płatności	(5)								
• OGÓŁEM środki administracyjne finansowane ze środków przydzielonych na określone programy operacyjne		(6)								
OGÓŁEM środki na DZIAŁ 3 wieloletnich ram finansowych	Środki na zobowiązania	=4+ 6								
	Środki na płatności	=5+ 6								

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

• OGÓŁEM środki operacyjne	Środki na zobowiązania	(4)								
	Środki na płatności	(5)								
• OGÓŁEM środki administracyjne finansowane ze środków przydzielonych na określone programy operacyjne		(6)								
Ogółem środki	Środki na	=4+ 6								

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

na DZIAŁY 1 do 4 wieloletnich ram finansowych (kwota referencyjna)	zobowiązania									
	Środki na płatności	=5+ 6								

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

w mln EUR (do 3 miejsc po przecinku)

		Rok **N= 2014**	Rok **2015**	Rok **2016**	Rok **2017**	Rok **2018**	Rok **2019**	Rok **2020**	**OGÓŁEM**
DG: JUST									
• Zasoby ludzkie		2,922	2,922	2,922	2,922	2,922	2,922	2,922	**20,454**
• Pozostałe wydatki administracyjne		0,555	0,555	0,555	0,555	0,555	0,555	0,555	**3,885**
OGÓŁEM Dyrekcja Generalna ds. Sprawiedliwości		**3,477**	**3,477**	**3,477**	**3,477**	**3,477**	**3,477**	**3,477**	**24,339**

OGÓŁEM środki na DZIAŁ 5 wieloletnich ram finansowych	(Środki na zobowiązania ogółem = środki na płatności ogółem)	**3,477**	**3,477**	**3,477**	**3,477**	**3,477**	**3,477**	**3,477**	**24,339**

w mln EUR (do 3 miejsc po przecinku)

		Rok **N**[58]	Rok **N+1**	Rok **N+2**	Rok **N+3**	wprowadzić taką liczbę kolumn dla poszczególnych lat, jaka jest niezbędna, by odzwierciedlić	**OGÓŁEM**

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

						cały okres wpływu (por. pkt 1.6)			
OGÓŁEM środki na DZIAŁY 1 do 5 wieloletnich ram finansowych	Środki na zobowiązania	3,477	3,477	3,477	3,477	3,477	3,477	3,477	24,339
	Środki na płatności	3,477	3,477	3,477	3,477	3,477	3,477	3,477	24,339

3.2.2. Szacunkowy wpływ na środki operacyjne

6. ☑ Wniosek/inicjatywa nie wiąże się z koniecznością wykorzystania środków operacyjnych

Wysoki poziom ochrony danych osobowych jest również jednym z celów programu „Prawa podstawowe i obywatelstwo”.

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

Środki na zobowiązania w mln EUR (do 3 miejsc po przecinku)

Określić cele i realizacje			Rok **N=2014**		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**	
	REALIZACJA																	
⇩	Rodzaj[59]	Średni koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba całkowita	Koszt całkowity
CEL SZCZEGÓŁOWY nr 1																		
Realizacja	Akta[60]																	
Cel szczegółowy nr 1 - suma cząstkowa																		
CEL SZCZEGÓŁOWY nr 2																		
Realizacja	Sprawy[61]																	
Cel szczegółowy nr 2 - suma cząstkowa																		
KOSZT OGÓŁEM																		

59 Realizacje odnoszą się do produktów i usług, które zostaną zapewnione (np. liczba sfinansowanych wymian studentów, liczba kilometrów zbudowanych dróg itp.).

60 Opinie, decyzje, posiedzenia Rady dotyczące procedur.

61 Sprawy rozpatrywane w ramach mechanizmu zgodności.

3.2.3. *Szacunkowy wpływ na środki administracyjne*

3.2.3.1. Streszczenie

8. ☐ Wniosek/inicjatywa nie wiąże się z koniecznością wykorzystania środków administracyjnych

9. ☑ Wniosek/inicjatywa wiąże się z koniecznością wykorzystania środków administracyjnych, jak określono poniżej:

w mln EUR (do 3 miejsc po przecinku)

	Rok **N**[62] **2014**	Rok **2015**	Rok **2016**	Rok **2017**	Rok **2018**	Rok **2019**	Rok **2020**	**OGÓŁEM**
DZIAŁ 5 wieloletnich ram finansowych								
Zasoby ludzkie	2,922	2,922	2,922	2,922	2,922	2,922	2,922	**20,454**
Pozostałe wydatki administracyjne	0,555	0,555	0,555	0,555	0,555	0,555	0,555	**3,885**
DZIAŁ 5 wieloletnich ram finansowych – suma cząstkowa	**3,477**	**3,477**	**3,477**	**3,477**	**3,477**	**3,477**	**3,477**	**24,339**

Poza DZIAŁEM 5 [63]wieloletnich ram finansowych								
Zasoby ludzkie								
Pozostałe wydatki administracyjne								
Poza DZIAŁEM 5 wieloletnich ram finansowych – suma cząstkowa								

OGÓŁEM	**3,477**	**3,477**	**3,477**	**3,477**	**3,477**	**3,477**	**3,477**	**24,339**

62 Rok N jest rokiem, w którym rozpoczyna się wprowadzanie w życie wniosku/inicjatywy.

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

3.2.3.2. Szacowane zapotrzebowanie na zasoby ludzkie

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

11. ☑ Wniosek/inicjatywa wiąże się z koniecznością wykorzystania zasobów ludzkich, jak określono poniżej:

Wartości szacunkowe należy wyrazić w pełnych kwotach (lub najwyżej z dokładnością do jednego miejsca po przecinku)

		Rok **2014**	Rok **2015**	Rok **2016**	Rok **2017**	Rok **2018**	Rok **2019**	Rok **2020**
• Stanowiska przewidziane w planie zatrudnienia (stanowiska urzędników i pracowników zatrudnionych na czas określony)								
XX 01 01 01 (w centrali i w biurach przedstawicielstw Komisji)		22	22	22	22	22	22	22
XX 01 01 02 (w delegaturach)								
• Personel zewnętrzny (w ekwiwalentach pełnego czasu pracy)[64]								
XX 01 02 01 (AC, END, INT z globalnej koperty finansowej)		2	2	2	2	2	2	2
XX 01 02 02 (AC, AL, END, INT i JED w delegaturach)								
XX 01 04 ***yy***[65]	- w centrali[66]							
	- w delegaturach							
XX 01 05 02 (AC, END, INT - pośrednie badania naukowe)								
10 01 05 02 (AC, END, INT – bezpośrednie badania naukowe)								
Inna pozycja w budżecie (określić)								
OGÓŁEM		**24**	**24**	**24**	**24**	**24**	**24**	**24**

XX oznacza odpowiednią dziedzinę polityki lub odpowiedni tytuł w budżecie

W związku z reformą Komisja będzie musiała wykonywać nowe zadania w obszarze ochrony osób fizycznych w odniesieniu do przetwarzania danych osobowych poza tymi, które są wykonywane obecnie. Dodatkowe zadania dotyczą głównie wdrożenia nowego mechanizmu zgodności, który zapewni spójne stosowanie zharmonizowanych przepisów prawa o ochronie danych, oceny odpowiedniego poziomu ochrony danych zapewnianej przez państwa trzecie, za które Komisja będzie ponosić wyłączną odpowiedzialność i przygotowania środków wykonawczych oraz aktów delegowanych. Inne zadania obecnie wykonywane przez

64 AC= pracownik kontraktowy; INT= pracownik tymczasowy; JED= młodszy oddelegowany ekspert AL= członek personelu miejscowego; END= oddelegowany ekspert krajowy;

65 W ramach pułapu na personel zewnętrzny ze środków operacyjnych (dawne pozycje „BA”).

66 Przede wszystkim fundusze strukturalne, Europejski Fundusz Rolny na rzecz Rozwoju Obszarów Wiejskich (EFRROW) oraz Europejski Fundusz Rybacki.

Komisję (np. rozwój polityki, monitorowanie transpozycji, podnoszenie świadomości, skargi itp.) będą nadal wykonywane.

Potrzeby w zakresie zasobów ludzkich zostaną pokryte z zasobów DG 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	Osoby odpowiedzialne za obsługę spraw: obsługujące mechanizm zgodności ochrony danych, aby zapewnić jednolitość stosowania przepisów UE w zakresie ochrony danych. Zadania obejmują prowadzenie dochodzeń i badanie spraw przedłożonych przez organy państw członkowskich w celu podjęcia decyzji, negocjacje z państwami członkowskimi i przygotowywanie decyzji Komisji. Z dotychczasowych doświadczeń wynika, że załatwienia w ramach mechanizmu zgodności może wymagać od 5 do 10 spraw rocznie. Obsługa wniosków o stwierdzenie odpowiedniego poziomu ochrony wymaga bezpośredniego współdziałania z państwem, które wystąpiło z takim wnioskiem, ewentualnego zarządzania ekspertyzami dotyczącymi sytuacji w tym państwie, oceny tej sytuacji, przygotowania odpowiednich decyzji Komisji i procedury, w tym także przez komitet wspomagający Komisję i każdy organ ekspercki, w stosownych przypadkach. W oparciu o ostatnio zdobyte doświadczenia można oczekiwać, że rocznie zostanie złożonych do 4 wniosków o stwierdzenie odpowiedniego poziomu ochrony. Proces przyjmowania środków wykonawczych obejmuje środki przygotowawcze, takie jak dokumenty dotyczące kwestii problemowych, badania i konsultacje społeczne, jak również sporządzenie samego instrumentu i zarządzanie negocjacjami w odpowiednich komitetach i innych grupach oraz ogólnie utrzymywanie kontaktu z zainteresowanymi podmiotami. W obszarach wymagających bardziej szczegółowych wytycznych możliwa jest obsługa do trzech środków wykonawczych na rok, podczas gdy proces taki, w zależności od intensywności konsultacji, może trwać nawet do 24 miesięcy.
Personel zewnętrzny	Wsparcie administracyjne i obsługa sekretariatu

3.2.4. Zgodność z obowiązującymi wieloletnimi ramami finansowymi

12. ☐ Wniosek/inicjatywa jest zgodny/zgodna z kolejnymi wieloletnimi ramami finansowymi.

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

W poniższej tabeli wskazano kwoty środków finansowych, które są corocznie potrzebne EIOD, aby mógł wykonywać swoje nowe zadania związane z obsługą sekretariatu Europejskiej Rady Ochrony Danych i z odnośnymi procedurami i narzędziami przez okres następnej perspektywy finansowej poza tymi, które zostały już uwzględnione w planowaniu.

Rok	2014	2015	2016	2017	2018	2019	2020	Ogółem
Personel	1,555	1,555	1,543	1,543	1,543	1,543	1,543	10,823

itp.								
Operacje	0,850	1,500	1,900	1,900	1,500	1,200	1,400	10,250
Ogółem	**2,405**	**3,055**	**3,443**	**3,443**	**3,043**	**2,743**	**2,943**	**21,073**

14. ☐ Wniosek/inicjatywa wymaga zastosowania instrumentu elastyczności lub zmiany wieloletnich ram finansowych[67]

3.2.5. Udział osób trzecich w finansowaniu

15. ☑Wniosek/inicjatywa nie przewiduje współfinansowania ze strony osób trzecich

16. ☐Wniosek/inicjatywa przewiduje współfinansowanie szacowane zgodnie z poniższym:

Środki w mln EUR (do 3 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

17. ☑ Wniosek/inicjatywa nie ma wpływu finansowego na dochody.

18. ☐ Wniosek/inicjatywa ma wpływ finansowy określony poniżej:

- ☐ wpływ na zasoby własne
- ☐ wpływ na dochody różne

w mln EUR (do 3 miejsc po przecinku)

Pozycja w budżecie dotycząca dochodów	Środki zapisane w budżecie na bieżący rok budżetowy	Wpływ wniosku/inicjatywy[68]						
		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)		

W przypadku wpływu na dochody różne, należy wskazać pozycję(-e) wydatków w budżecie, którą(-e) ten wpływ obejmie.
Należy określić metodę obliczania wpływu na dochody.

[67] Zob. pkt 19 i 24 porozumienia międzyinstytucjonalnego.

[68] 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.

Załącznik do oceny skutków finansowych regulacji odnoszącej się do wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem tych danych.

Zastosowana metodologia oraz główne założenia

Koszty związane z nowymi zadaniami, które będzie wykonywał Europejski Inspektor Ochrony Danych (EIOD), wynikającymi z dwóch wniosków ustawodawczych, zostały oszacowane dla wydatków na personel na podstawie kosztów ponoszonych obecnie przez Komisję na realizację podobnych zadań.

EIOD zapewni obsługę sekretariatu Europejskiej Rady Ochrony Danych zastępującej Grupę Roboczą Art. 29. Zważywszy na obecne obciążenie pracą Komisji związane z realizacją tego zadania, oznacza to, że niezbędne jest zatrudnienie trzech dodatkowych osób na pełnym etacie oraz przeznaczenie odpowiednich środków administracyjnych i operacyjnych. To obciążenie pracą rozpocznie się od momentu wejścia w życie rozporządzenia.

Ponadto EIOD będzie odgrywał rolę w mechanizmie zgodności, co będzie prawdopodobnie wymagać zatrudnienia pięciu osób na pełnym etacie, a także w opracowaniu i obsługiwaniu wspólnego narzędzia informatycznego dla krajowych organów ds. ochrony danych, co z kolei będzie się wiązać z potrzebą zatrudnienia kolejnych dwóch pracowników.

Obliczenia dotyczące zwiększenia środków w budżecie przeznaczonych na personel przez pierwsze siedem lat przedstawiono w bardziej szczegółowy sposób w poniższej tabeli. Druga tabela pokazuje wymagany budżet operacyjny. Będzie to odzwierciedlone w budżecie UE w sekcji IX „EIOD”.

Rodzaj kosztów	Obliczenia	Kwota (w tys.)							
		2014	2015	2016	2017	2018	2019	2020	Ogółem
Wynagrodzenie i dodatki									
- przewodniczący EROD		0,300	0,300	0,300	0,300	0,300	0,300	0,300	2,100
- urzędnicy i pracownicy zatrudnieni na czas określony	=7*0,127	0,889	0,889	0,889	0,889	0,889	0,889	0,889	6,223
- z czego END	=1*0,073	0,073	0,073	0,073	0,073	0,073	0,073	0,073	0,511
- z czego pracownicy kontraktowi	=2*0,064	0,128	0,128	0,128	0,128	0,128	0,128	0,128	0,896
Wydatki związane z rekrutacją	=10*0,005	0,025	0,025	0,013	0,013	0,013	0,013	0,013	0,113
Koszty delegacji		0,090	0,090	0,090	0,090	0,090	0,090	0,090	0,630
Pozostałe wydatki, szkolenia	=10*0,005	0,050	0,050	0,050	0,050	0,050	0,050	0,050	0,350
Wydatki administracyjne ogółem		**1,555**	**1,555**	**1,543**	**1,543**	**1,543**	**1,543**	**1,543**	**10,823**

Opis zadań do wykonania:

Urzędnicy i pracownicy zatrudnieni na czas określony	Osoby odpowiedzialne za obsługę sekretariatu Europejskiej Rady Ochrony Danych. Oprócz wsparcia logistycznego, w tym kwestii budżetowych i umownych, ich zadania obejmują przygotowanie porządków obrad i zaproszeń dla ekspertów, badania dotyczące tematów objętych porządkiem obrad grupy, zarządzanie dokumentami dotyczącymi prac grupy, z uwzględnieniem odpowiednich wymogów ochrony danych, poufności i publicznego dostępu. Włączając wszystkie podgrupy i grupy eksperckie, rocznie może zajść potrzeba przygotowania do 50 posiedzeń i procedur podejmowania decyzji. Osoby odpowiedzialne za obsługę spraw: obsługujące mechanizm zgodności ochrony danych, aby zapewnić jednolitość stosowania przepisów UE w zakresie ochrony danych. Ich zadania obejmują prowadzenie dochodzeń i badanie spraw przedłożonych przez organy państw członkowskich w celu podjęcia decyzji, negocjacje z państwami członkowskimi i przygotowywanie decyzji Komisji. Z dotychczasowych doświadczeń wynika, że załatwienia w ramach mechanizmu zgodności może wymagać od 5 do 10 spraw rocznie. Narzędzie informatyczne uprości współpracę operacyjną między krajowymi organami ds. ochrony danych a administratorami danych zobowiązanymi do dzielenia się informacjami z organami publicznymi. Odpowiedzialni członkowie personelu zapewnią kontrolę jakości, zarządzanie projektami i monitorowanie kwestii budżetowych w zakresie procesów informatycznych pod kątem specyfikacji wymogów, wdrażania i obsługi systemów.
Personel zewnętrzny	Wsparcie administracyjne i obsługa sekretariatu

Wydatki EIOD odnoszące się do konkretnych zadań

Określić cele i realizacje			Rok **N=2014**		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**	
	REALIZACJA																	
⇩	Rodzaj[69]	Średni koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba całkowita	Koszt całkowity
CEL SZCZEGÓŁOWY nr 1[70]			Sekretariat Rady Ochrony Danych															
Realizacja	Sprawy[71]	0,010	30	0,300	40	0,400	50	0,500	50	0,500	50	0,500	50	0,500	50	0,500	320	3,200
Cel szczegółowy nr 1 - suma cząstkowa			30	0,300	40	0,400	50	0,500	50	0,500	50	0,500	50	0,500	50	0,500	320	3,200
CEL SZCZEGÓŁOWY nr 2			Mechanizm zgodności															
Realizacja	Akta[72]	0,050	5	0,250	10	0,500	10	0,500	10	0,500	8	0,400	8	0,400	8	0,400	59	2,950
Cel szczegółowy nr 2 - suma cząstkowa			5	0,250	10	0,500	10	0,500	10	0,500	8	0,400	8	0,400	8	0,400	59	2,950
CEL SZCZEGÓŁOWY nr 3			Wspólne narzędzie IT dla organów ds. ochrony danych (EIOD)															
Realizacja	Sprawy[73]	0,100	3	0,300	6	0,600	9	0,900	9	0,900	6	0,600	3	0,300	5	0,500	41	4,100
Cel szczegółowy nr 3 - suma cząstkowa			3	0,300	6	0,600	9	0,900	9	0,900	6	0,600	3	0,300	5	0,500	41	4,100
KOSZT OGÓŁEM			38	0,850	56	1,500	69	1,900	69	1,900	64	1,500	61	1,200	63	1,400	420	10,250

69 Realizacje odnoszą się do produktów i usług, które zostaną zapewnione (np. liczba sfinansowanych wymian studentów, liczba kilometrów zbudowanych dróg itp.).

70 Zgodnie z opisem w pkt 1.4.2 „Cel(e) szczegółowy(-e) …”

71 Sprawy rozpatrywane w ramach mechanizmu zgodności.

72 Opinie, decyzje, posiedzenia Rady dotyczące procedur.

73 Na podstawie łącznej liczby na każdy rok szacuje się wysiłek na opracowanie i obsługę narzędzi IT.