KOMISJA EUROPEJSKA

Bruksela, dnia 25.1.2012 r.
COM(2012) 10 final

2012/0010 (COD)

Wniosek

DYREKTYWA PARLAMENTU EUROPEJSKIEGO I RADY

w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez właściwe organy do celów zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich i ścigania albo wykonywania kar kryminalnych oraz swobodnego przepływu tych danych

[…]

UZASADNIENIE

1. KONTEKST WNIOSKU

Niniejsze uzasadnienie zawiera dalsze szczegóły na temat podejścia do nowych ram prawnych ochrony danych osobowych w UE przedstawionego w komunikacie COM (2012) 9 wersja ostateczna. Na ramy prawne składają się dwa wnioski ustawodawcze:

– wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (ogólne rozporządzenie o ochronie danych), oraz

– wniosku dotyczącego 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 lub wykonywania kar kryminalnych oraz swobodnego przepływu takich danych

Niniejsze uzasadnienie dotyczy tego drugiego wniosku.

Podstawowy dokument ustanawiający obowiązujące unijne przepisy o ochronie danych, dyrektywa 95/46/WE[1], 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 Została ona uzupełniona przez szereg instrumentów przewidujących przepisy szczególne o ochronie danych w obszarze współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych[2] (były trzeci filar), w tym decyzję ramową 2008/977/WSiSW[3].

Rada Europejska wezwała Komisję do oceny funkcjonowania unijnych instrumentów o ochronie danych oraz przedstawienia, w razie potrzeby, dalszych inicjatyw ustawodawczych lub o charakterze nieustawodawczym[4]. W rezolucji w sprawie programu sztokholmskiego[5] 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[6] potrzebę zagwarantowania konsekwentnego stosowania podstawowego prawa do ochrony danych osobowych w kontekście wszystkich polityk UE. W planie działania podkreślono, że „w społeczeństwie globalnym charakteryzującym się szybkimi zmianami technologicznymi i nieograniczonym przepływem informacji szczególne znaczenie ma zachowanie ochrony prywatności. Unia musi zagwarantować spójne wykonywanie prawa do ochrony danych, będącego jednym z

---

1 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.

2 Zob. pełny wykaz w załączniku 3 do oceny skutków (SEC(2012)72)..

3 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.

4 W programie sztokholmskim - Dz. U. C 115 z 4.5.2010, s. 1

5 Zob. rezolucję Parlamentu Europejskiego w sprawie programu sztokholmskiego przyjętą w dniu 25 listopada 2009 r.

6 COM (2010) 171 wersja ostateczna.

praw podstawowych. Należy wzmocnić stanowisko UE dotyczące ochrony danych osobowych w kontekście wszystkich obszarów polityki UE, w tym w dziedzinie egzekwowania prawa i zapobiegania przestępstwom, a także w dziedzinie stosunków międzynarodowych".

W komunikacie w sprawie „Całościowego podejścia do kwestii ochrony danych osobowych w Unii Europejskiej"[7] Komisja stwierdziła, że UE potrzebuje bardziej całościowej i spójnej polityki w zakresie podstawowego prawa do ochrony danych osobowych.

Decyzja ramowa 2008/977/WSiSW ma ograniczony zakres zastosowania, ponieważ dotyczy wyłącznie transgranicznego przetwarzania danych, ale nie obejmuje ich przetwarzania przez organy policyjne i sądowe na szczeblu czysto krajowym. Może to powodować trudności dla policji i innych właściwych organów w obszarze współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej. Nie zawsze są w stanie łatwo rozróżnić między przetwarzaniem mającym charakter czysto wewnętrzny i transgraniczny czy też przewidzieć, czy określone dane staną się na późniejszym etapie przedmiotem transgranicznej wymiany (zob. pkt 2 poniżej). Ponadto ze względu na swój charakter i treść decyzja ramowa pozostawia państwom członkowskim dużą swobodę manewru, jeżeli chodzi o krajowe przepisy wdrażające przepisy decyzji. Poza tym nie zawiera ona żadnych mechanizmów ani nie przewiduje grupy doradczej podobnej do Grupy Roboczej Art. 29, które służyłyby promowaniu wspólnej wykładni przepisów decyzji ani też nie przewiduje żadnych uprawnień wykonawczych dla Komisji, aby zagwarantować wspólne podejście we wdrażaniu decyzji.

Artykuł 16 ust. 1 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE) ustanawia zasadę, że każdy ma prawo do ochrony danych osobowych. Ponadto w art. 16 ust. 2 TFUE traktat lizboński wprowadza szczególną podstawę prawną dla przyjmowania norm dotyczących ochrony danych osobowych, która znajduje zastosowanie także do współpracy wymiarów sprawiedliwości w sprawach karnych oraz współpracy policyjnej. W art. 8 Karty praw podstawowych UE zapisano ochronę danych osobowych jako jedno z praw podstawowych. Artykuł 16 TFUE nakłada na prawodawcę obowiązek ustanowienia przepisów dotyczących ochrony osób fizycznych w zakresie przetwarzania danych także w obszarze współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych, co obejmuje przetwarzanie danych zarówno na szczeblu transgranicznym, jak i krajowym. Umożliwi to ochronę podstawowych praw i wolności osób fizycznych, a w szczególności prawa do ochrony danych osobowych, gwarantując równocześnie wymianę danych osobowych do celów zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich i ścigania lub wykonywania kar kryminalnych. Przyczyni się to do ułatwienia współpracy w zwalczaniu przestępczości w Europie.

Ze względu na szczególny charakter współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych, w deklaracji 21[8] stwierdzono, że konieczne może okazać się wprowadzenie zasad szczególnych dotyczących ochrony danych osobowych i swobodnego przepływu tych danych w dziedzinach współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej, zapewnianej na podstawie artykułu 16 Traktatu o funkcjonowaniu Unii Europejskiej.

---

[7] Komunikat Komisji Europejskiej pt. „Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej", COM(2010) 609 wersja ostateczna z 4 listopada 2010 r.

[8] Deklaracja 21 w sprawie ochrony danych osobowych w dziedzinie współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej (dołączona do Akt końcowego konferencji międzyrządowej, która przyjęła Traktat z Lizbony z 13 grudnia 2007 r.).

2. WYNIKI KONSULTACJI Z ZAINTERESOWANYMI STRONAMI ORAZ OCENY SKUTKÓW

Niniejsza inicjatywa jest rezultatem szeroko zakrojonych konsultacji z wszystkimi głównymi zainteresowanymi stronami w sprawie przeglądu obowiązujących ram prawnych ochrony danych osobowych, obejmujących 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. Z opiniami niezaklasyfikowanymi jako poufne można się zapoznać na stronie internetowej Komisji[9].

– 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 organizacji biznesowych i pozarządowych. Z opiniami niesklasyfikowanymi jako poufne można się zapoznać na stronie internetowej Komisji[10].

Podczas gdy konsultacje te koncentrowały się głównie na przeglądzie dyrektywy 95/46/WE, przeprowadzono również specjalne konsultacje z najważniejszymi zainteresowanymi stronami reprezentującymi organy ścigania, w szczególności w dniu 29 czerwca 2010 r. zorganizowano warsztaty z organami państw członkowskich na temat stosowania norm ochrony danych do organów publicznych, w tym w obszarze współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych. Ponadto w 2 lutego 2011 r. Komisja zorganizowała warsztaty z organami państw członkowskich w celu omówienia kwestii wdrażania decyzji ramowej 2008/977/WSiSW oraz, bardziej ogólnie, zagadnień ochrony danych w współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych.

Konsultacje z obywatelami UE przeprowadzono za pośrednictwem kwestionariusza Eurobarometru w listopadzie-grudniu 2010 r.[11]. Zainicjowano również szereg analiz[12]. Grupa Robocza Art. 29[13] przedstawiła wiele opinii i wniosła cenny wkład w prace Komisji[14].

---

9 http://ec.europa.eu/justice/newsroom/data-protection/opinion/090709_en.htm.

10 http://ec.europa.eu/justice/newsroom/data-protection/opinion/090709_en.htm.

11 Specjalne wydanie Eurobarometru (EB) 359, *Ochrona danych i tożsamość elektroniczna w UE* (2011) http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf.

12 Zob. analizę korzyści ekonomicznych z technologii zwiększających ochronę prywatności (zob. przypis 2) lub *Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments*, styczeń 2010 r. (http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf).

13 Grupa robocza została ustanowiona w 1996 r. (na podstawie art. 29 dyrektywy) jako organ o charakterze doradczym, złożony z przedstawicieli krajowych organów nadzorczych w zakresie 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.

14 Zob. w szczególności następujące opinie: w sprawie „Przyszłości prywatności" (2009 r. WP 168), w sprawie pojęcia „administratora danych" i „podmiotu przetwarzającego dane" (1/2010, WP 169); w sprawie reklamy behawioralnej online (2/2010, WP 171); w sprawie zasady odpowiedzialności (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 pisma doradcze: w sprawie zawiadomień, w sprawie danych szczególnie chronionych oraz w sprawie praktycznego wdrożenia art. 28 ust. 6 dyrektywy

Również Europejski Inspektor Ochrony Danych wydał kompleksową opinię na temat zagadnień poruszonych w komunikacie Komisji z listopada 2010 r.[15].

Parlament Europejski zatwierdził swoją rezolucją z dnia 6 lipca 2011 r. sprawozdanie, w którym poparł podejście Komisji do reformy ram ochrony danych[16]. 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 ogólne dążenie Komisji do zagwarantowania spójniejszego stosowania unijnych norm ochrony danych we wszystkich państwach członkowskich oraz odpowiednią rewizję dyrektywy 95/46/WE[17].

Zgodnie ze swoją polityką dążenia do lepszych uregulowań prawnych Komisja przeprowadziła ocenę skutków alternatywnych wariantów politycznych[18]. Ocena skutków została oparta na trzech celach polityki zakładających poprawę wymiaru ochrony danych związanego z rynkiem wewnętrznym, zapewnienie osobom fizycznym możliwości skuteczniejszego wykonywania prawa do ochrony danych oraz stworzenie całościowych, spójnych ram obejmujących wszystkie obszary właściwości Unii, w tym współpracę policyjną i współpracę wymiarów sprawiedliwości w sprawach karnych. W szczególności w odniesieniu do tego ostatniego celu, oceniono dwa warianty polityki: pierwszy zakłada zwyczajne rozszerzenie zakresu norm ochrony danych na ten obszar oraz zaradzenie lukom i innym problemom związanym z decyzją ramową, a drugi, dalej sięgający, zakładający wprowadzenie bardzo ograniczających i rygorystycznych przepisów, co pociągałoby za sobą także niezwłoczną zmianę wszystkich innych instrumentów „trzeciego filaru". Trzeci „minimalistyczny" wariant, oparty w głównej mierze na komunikatach zawierających wykładnię i środkach wsparcia realizacji polityki, takich jak programy finansowania i narzędzia techniczne, przy minimalnej interwencji legislacyjnej, nie został uznany za właściwy by zaradzić problemom ustalonym w tym obszarze w odniesieniu do ochrony danych.

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 ekonomicznego 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 został włączony do obecnego wniosku. Zgodnie z oceną wdrażanie doprowadzi do dalszego wzmocnienia ochrony danych w tym obszarze polityki, w szczególności poprzez włączenie przetwarzania danych na szczeblu krajowym, zwiększając tym samym także

---

95/46/WE. Wszystkie one są dostępne na następującej stronie http://ec.europa.eu/justice/data-protection/article-29/documentation/index_en.htm.

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

16 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).

17 CESE 999/2011

18 SEC(2012)72.

pewność prawną dla właściwych organów w obszarze współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej.

Rada ds. ocen skutków przedstawiła opinię na temat projektu oceny skutków w dniu 9 września 2011 r. Po wydaniu opinii przez tę 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.

Komisja przygotowała również sprawozdanie z wdrażania związane z decyzją ramową 2008/977/WSiSW oparte na jej art. 29 ust. 2, które ma zostać przyjęte w ramach obecnego pakietu w zakresie ochrony danych[19]. Przy przygotowywaniu oceny skutków uwzględniono również ustalenia zawarte w sprawozdaniu, oparte na opiniach państw członkowskich.

3. ASPEKTY PRAWNE WNIOSKU

3.1. Podstawa prawna

Wniosek oparty jest na art. 16 ust. 2 TFUE będącym nową, szczególną podstawą prawną wprowadzoną traktatem lizbońskim dla przyjmowania przepisów dotyczących ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez instytucje, organy oraz jednostki organizacyjne i agencje Unii oraz przez państwa członkowskie w wykonywaniu działań wchodzących w zakres zastosowania prawa Unii, a także przepisów dotyczących swobodnego przepływu takich danych.

Wniosek zmierza do zapewnienia spójnego, wysokiego poziomu ochrony danych w tym obszarze, przyczyniając się tym samym do pogłębienia wzajemnego zaufania między organami policyjnymi i sądowymi różnych państw członkowskich oraz ułatwiając swobodny przepływ danych oraz współpracę między organami policyjnymi i sądowymi.

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 w obszarze współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych na podstawie następujących przesłanek:

– prawo do ochrony danych osobowych zapisane w art. 8 Karty praw podstawowych oraz w art. 16 ust. 1 TFUE wymaga tego samego poziomu ochrony danych w całej Unii; wymaga ono tego samego poziomu ochrony danych wymienianych i danych przetwarzanych na szczeblu krajowym;

---

[19] COM(2012)12.

– istnieje coraz większa potrzeba przetwarzania przez organy ścigania państwa członkowskich i prowadzenia wymiany szybko rosnącej liczby informacji do celów zapobiegania przestępczości transgranicznej i terroryzmowi oraz zwalczania tych zjawisk. W tym kontekście jasne i spójne normy ochrony danych na szczeblu UE pomogą promować współpracę między tymi organami.

– 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 przekazywanie danych osobowych przez granice na terytorium UE, przy równoczesnym zagwarantowaniu skutecznej ochrony dla wszystkich osób fizycznych w całej UE;

– proponowane działania legislacyjne UE będą przypuszczalnie bardziej skuteczne niż podobne działania na szczeblu państw członkowskich, ze względu na charakter i skalę problemów, które nie ograniczają się do szczebla jednego czy wielu 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 alternatywnych wariantów polityki, aż po sporządzenie wniosku ustawodawczego.

Dyrektywa jest zatem instrumentem najlepiej mogącym zapewnić harmonizację na szczeblu UE w tym obszarze, pozostawiając równocześnie państwom niezbędną elastyczność przy wdrażaniu zasad, przepisów i wyjątków od nich na szczeblu krajowym. Ze względu na złożoność obowiązujących przepisów krajowych dotyczących ochrony danych osobowych przetwarzanych w obszarze współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych oraz cel kompleksowej harmonizacji tych przepisów za pomocą niniejszej dyrektywy, Komisja będzie musiała wystąpić do państw członkowskich o przedłożenie dokumentów wyjaśniających związek między elementami dyrektywy i odpowiednimi częściami krajowych instrumentów służących transpozycji, by była zdolna do realizacji swoich zadań dotyczących nadzoru nad transpozycją dyrektywy.

3.3. Podsumowanie zagadnień praw podstawowych

Prawo do ochrony danych osobowych ustanowione jest art. 8 Karty praw podstawowych UE oraz art. 16 TFUE, jak również art. 8 EKPC. Jak podkreślił Trybunał Sprawiedliwości UE[20], prawo do ochrony danych osobowych nie jest prawem absolutnym i powinno być analizowane w kontekście funkcji, jaką pełni w społeczeństwie[21]. Ochrona danych jest ściśle

[20] Trybunał Sprawiedliwości UE, wyrok z dnia 9.11.2010 w sprawach C-92/09 i 93/09 „Schecke".

[21] Zgonie 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

powiązana z poszanowaniem życia prywatnego i rodzinnego chronionego przez 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 mieć potencjalnie wpływ, to zakaz dyskryminacji innych osób ze względu na takie czynniki jak: płeć, pochodzenie etniczne, cechy genetyczne, religię lub światopogląd, przekonania polityczne lub inne przekonania, niepełnosprawność lub orientację seksualną (art. 21); prawa dziecka (art. 24); prawo do skutecznego sądowego środka ochrony prawnej oraz prawo do rzetelnego procesu (art. 47).

3.4. Szczegółowe wyjaśnienie wniosku

3.4.1. ROZDZIAŁ I – PRZEPISY OGÓLNE

Artykuł 1 definiuje zakres przedmiotowy dyrektywy, tzn. przepisy dotyczące przetwarzania danych osobowych do celów zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich i ścigania lub wykonywania kar kryminalnych, jak również określa podwójny cel dyrektywy, jakim jest ochrona praw podstawowych i wolności osób fizycznych, w a szczególności ich prawa do ochrony danych osobowych, przy równoczesnym zagwarantowaniu wysokiego poziomu bezpieczeństwa publicznego, jak również zagwarantowanie wymiany danych osobowych między właściwymi organami na terytorium Unii.

Artykuł 2 określa zakres stosowania dyrektywy. Zakres dyrektywy nie ogranicza się do transgranicznego przetwarzania danych, lecz obejmuje wszystkie operacje przetwarzania realizowane przez „właściwe organy" (określone w art. 3 ust. 14) do celów dyrektywy. Dyrektywa nie ma zastosowania ani do przetwarzania w ramach działalności leżącej poza zakresem prawa unijnego, ani do przetwarzania przez instytucje, organy, biura i agencje Unii, które podlega rozporządzeniu (WE) nr 45/2001 i innym szczególnym przepisom.

Artykuł 3 zawiera definicje terminów używanych w dyrektywie. Podczas gdy część definicji przejęto z dyrektywy 95/46/WE i decyzji ramowej 2008/977/WSiSW, inne zostały zmienione, uzupełnione o dodatkowe lub nowo wprowadzone elementy. Nowe definicje dotyczą „naruszenia ochrony danych osobowych", „danych genetycznych" i „danych biometrycznych", „właściwych organów" (w oparciu o art. 87 TFUE i art. 2 lit. h) decyzji ramowej 2008/977/WSiSW oraz „dziecka" w oparciu Konwencję ONZ o prawach dziecka[22].

3.4.2. ROZDZIAŁ II – ZASADY

Artykuł 4 określa zasady dotyczące przetwarzania danych osobowych odpowiadające art. 6 dyrektywy 95/46/WE i art. 3 decyzji ramowej 2008/977/WSiSW, z dostosowaniem ich do szczególnego kontekstu niniejszej dyrektywy.

---

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

[22] Przywołana również w art. 2 lit. a) dyrektywy Parlamentu Europejskiego i Rady 2011/92/UE z dnia 13 grudnia 2011 r. w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej, zastępującej decyzję ramową Rady 2004/68/WSiSW, Dz.U. L 335 z 17.12.2011, s. 1.

Artykuł 5 wymaga rozróżnienia, na tyle, na ile to możliwe, między danymi osobowymi różnych kategorii podmiotów, których dane te dotyczą. To nowy przepis, którego nie było ani w dyrektywie 95/46/WE, ani w decyzji ramowej 2008/977/WSiSW, a który został zaproponowany przez Komisję w jej pierwotnym wniosku dotyczącym decyzji ramowej[23]. Inspirację dla niego stanowi rekomendacja nr R (87) 15. Podobne przepisy obowiązują już w odniesieniu do Europolu[24] i Eurojustu[25].

Artykuł 6 w sprawie różnych stopni dokładności i wiarygodności stanowi odzwierciedlenie pkt 3.2 rekomendacji Rady Europy nr R (87)15. Podobne przepisy, które także zawarto we wniosku Komisji dotyczącym decyzji ramowej, obowiązują wobec Europolu[26].

Artykuł 7 określa podstawy zgodnego z prawem przetwarzania: gdy jest ono potrzebne do wykonania przez właściwy organ zadania wynikającego z prawa krajowego lub do spełnienia przez administratora ciążących na nim obowiązków prawnych, w celu ochrony żywotnych interesów podmiotu danych lub w celu zapobieżenia poważnemu, bezpośredniemu zagrożeniu dla bezpieczeństwa publicznego. Inne podstawy przetwarzania zgodnie z prawem przewidziane w art. 7 dyrektywy 95/46/WE nie są odpowiednie w przypadku przetwarzania w sektorze policji i wymiaru sprawiedliwości w sprawach karnych.

Artykuł 8 wyraża ogólny zakaz przetwarzania szczególnych kategorii danych osobowych oraz określa wyjątki od tej ogólnej zasady, opierając się na art. 8 dyrektywy 95/46/EW, dodając przy tym dane genetyczne, w konsekwencji orzecznictwa EKPC[27].

Artykuł 9 ustanawia zakaz stosowania środków opartych wyłącznie na zautomatyzowanym przetwarzaniu danych osobowych, chyba że zezwalają na to przepisy przewidujące odpowiednie gwarancje, zgodnie z art. 7 decyzji ramowej 2008/977/WSiSW.

3.4.3. ROZDZIAŁ III – PRAWA PODMIOTU DANYCH

Artykuł 10 wprowadza obowiązek zapewnienia przez państwa członkowskie łatwo dostępnych i zrozumiałych informacji, czego inspirację stanowi w szczególności zasada 10 rezolucji madryckiej w sprawie międzynarodowych standardów ochrony danych osobowych i prywatności[28], oraz zobowiązuje administratorów danych do zapewnienia procedur i mechanizmów ułatwiających osobom, których dane dotyczą, korzystanie z przysługujących im praw. Obejmuje to wymóg, by korzystanie z praw nie wymagało zasadniczo ponoszenia opłat.

Artykuł 11 precyzuje zobowiązanie państw członkowskich do zapewnienia informacji podmiotom danych. Obowiązki te opierają się na art. 10 i 11 dyrektywy 95/46/WE, przy czym nie ma osobnego artykułu wprowadzającego rozróżnienie pod kątem tego, czy dane zbierane są od podmiotu, którego dotyczą, oraz rozszerzają zakres informacji, których należy udzielić. Ustanawia on wyjątki od obowiązku informowania, przy czym muszą być one proporcjonalne i konieczne w demokratycznym społeczeństwie na potrzeby wykonywania zadań przez

---

23 COM(2005) 475 wersja ostateczna.

24 Artykuł 14 decyzji o ustanowieniu Europolu 2009/371/WSiSW.

25 Artykuł 15 decyzji ustanawiającej Eurojust 2009/426/WSiSW.

26 Artykuł 14 decyzji o ustanowieniu Europolu 2009/371/WSiSW.

27 Wyrok Europejskiego Trybunału Praw Człowieka z 4.12.2008, S i Marper przeciwko Zjednoczonemu Królestwu (skargi nr 30562/04 i 30566/04).

28 Przyjęta przez międzynarodową konferencję inspektorów ochrony danych w dniu 5 listopada 2009 r.

właściwe organy (inspirację stanowi tutaj art. 13 dyrektywy 95/46/WE oraz art. 17 decyzji ramowej 2008/977/WSiSW).

Artykuł 12 przewiduje obowiązek dopilnowania przez państwa członkowskie, by podmioty danych mogły korzystać z prawa dostępu do swoich danych osobowych. Opiera się on na art. 12 lit. a) dyrektywy 95/46/WE, przy czym dodano nowe elementy, o których trzeba poinformować osoby, których dane dotyczą (okres przechowywania, przysługujące im prawo do poprawienia, usunięcia oraz ograniczenia danych oraz złożenia skargi).

Artykuł 13 przewiduje, że państwa członkowskie mogą przyjąć środki legislacyjne ograniczające ich prawo dostępu, jeżeli wymaga tego szczególny charakter przetwarzania w sektorze policji i wymiaru sprawiedliwości w sprawach karnych, jak również środki dotyczące informowania osób, których dane dotyczą o ograniczeniach dostępu, w oparciu o art. 17 ust. 2 i 3 decyzji ramowej 2008/977/WSiSW.

Artykuł 14 wprowadza przepis stanowiący, że w przypadku ograniczenia bezpośredniego dostępu podmiot danych musi zostać poinformowany o możliwości pośredniego dostępu przy pomocy organu nadzorczego, który powinien skorzystać z tego prawa w jego imieniu i musi poinformować daną osobę w wynikach weryfikacji.

Artykuł 15 o prawie do poprawienia danych opiera się na art. 12 lit. b) dyrektywy 95/46/WE i, w odniesieniu do obowiązków powstających w przypadku odmowy, na art. 18 ust. 1 decyzji ramowej 2008/977/WSiSW.

Artykuł 16 o prawie do usunięcia danych opiera się na art. 12 lit. b) dyrektywy 95/46 i, w odniesieniu do obowiązków powstających w przypadku odmowy, na art. 18 ust. 1 decyzji ramowej 2008/977/WSiSW. Obejmuje on także prawo do ograniczenia przetwarzania w określonych przypadkach, zastępując tym samym niejednoznaczny termin „blokowanie" użyty w art. 12 lit. b) dyrektywy 95/46/WE i art. 18 ust. 1 decyzji ramowej 2008/977/WSiSW.

Artykuł 17 o prawie do poprawienia, usunięcia i ograniczenia przetwarzania w postępowaniu sądowym wyjaśnia przepisy, w oparciu o art. 4 ust. 4 decyzji ramowej 2008/977/WSiSW.

3.4.4. ROZDZIAŁ IV – ADMINISTRATOR I PODMIOT PRZETWARZAJĄCY

3.4.4.1. SEKCJA 1 – OBOWIĄZKI OGÓLNE

Artykuł 18 opisuje obowiązek przestrzegania przez administratora przepisów niniejszej dyrektywy oraz zapewnienia zgodności z nią, w tym poprzez przyjmowanie służących temu polityk i mechanizmów.

Artykuł 19 stanowi, że państwa członkowskie muszą zapewnić przestrzeganie przez administratora obowiązków wynikających z zasad ochrony danych już w fazie projektowania oraz domyślnej ochrony danych.

Artykuł 20 w sprawie współadministratorów wyjaśnia status współadministratorów w odniesieniu do ich stosunków wewnętrznych.

Artykuł 21 wyjaśnia status i obowiązki podmiotów przetwarzających dane, 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 22 dotyczący przetwarzania pod nadzorem administratora i podmiotu przetwarzającego opiera się na art. 16 dyrektywy 95/46/WE.

Artykuł 23 wprowadza dla administratorów danych i podmiotów przetwarzających dane obowiązek prowadzenia dokumentacji dotyczącej wszystkich systemów i procedur przetwarzania podlegających ich odpowiedzialności.

Artykuł 24 dotyczy prowadzenia rejestru, zgodnie z art. 10 ust. 1 decyzji ramowej 2008/977, przy czym doprecyzowano treść przepisu.

Artykuł 25 wyjaśnia obowiązki administratora i podmiotu przetwarzającego w zakresie współpracy z organem nadzorczym.

Artykuł 26 dotyczy przypadków, w których powstaje obowiązek konsultacji z organem nadzorczym przed przetwarzaniem, w oparciu o art. 23 decyzji ramowej 2008/977/WSiSW.

3.4.4.2. SEKCJA 2 – BEZPIECZEŃSTWO DANYCH

Artykuł 27 w sprawie bezpieczeństwa przetwarzania opiera się na obecnym art. 17 ust. 1 dyrektywy 95/46 dotyczącym bezpieczeństwa przetwarzania oraz art. 22 decyzji ramowej 2008/977/WSiSW, rozszerza powiązane obowiązki na podmioty przetwarzające dane, niezależnie od ich umowy z administratorem danych.

Artykuły 28 i 29 wprowadzają obowiązek zawiadamiania o naruszeniach ochrony danych osobowych, do czego inspirację stanowił taki obowiązek określony w art. 4 ust. 3 dyrektywy w sprawie e-prywatności 2002/58/WE, wyjaśniają i rozdzielają obowiązki zawiadomienia organu nadzorczego (art. 28) i przekazania informacji, w kwalifikowanych okolicznościach, podmiotowi danych (art. 29). Artykuł 29 przewiduje także wyjątki, przez odniesienie do art. 11 ust. 4.

3.4.4.3. SEKCJA 3 – INSPEKTOR OCHRONY DANYCH

Artykuł 30 wprowadza obowiązek powołania przez administratora inspektora ochrony danych, który powinien wypełniać zadania wyszczególnione w art. 32. W przypadku gdy wiele właściwych organów działa pod nadzorem organu centralnego, pełniącego funkcję administratora, przynajmniej ten centralny organ powinien wyznaczyć takiego inspektora ochrony danych. Artykuł 18 ust. 2 dyrektywy 95/46/WE przewidywał możliwość wprowadzenia przez państwo członkowskie takiego wymogu w ramach zastąpienia ogólnego obowiązku zawiadomienia przewidzianego w tej dyrektywie.

Artykuł 31 określa status inspektora ochrony danych.

Artykuł 32 opisuje zadania inspektora ochrony danych.

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

Artykuł 33 określa ogólne zasady przekazywania danych do państw trzecich lub organizacji międzynarodowych w obszarze współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych, w tym wtórnego przekazywania. Wyjaśnia on, że przekazywanie do państw trzecich może mieć miejsce jedynie wtedy, gdy jest to niezbędne do

celów zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich lub ścigania i w celu wykonywania kar kryminalnych.

Artykuł 34 stanowi, że można dokonać przekazania danych do państw trzecich w odniesieniu do których Komisja przyjęła decyzję stwierdzającą odpowiedni poziom ochrony na mocy rozporządzenia …./../201X lub albo konkretnie dotyczącą obszaru współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych lub, w przypadku braku takiej decyzji, gdy obowiązują odpowiednie gwarancje. Do czasu przyjęcia decyzji o odpowiednim stopniu ochrony dyrektywa gwarantuje możliwość dalszego przekazania na podstawie odpowiednich gwarancji i derogacji. Ponadto określa on kryteria, na podstawie których Komisja dokonuje oceny odpowiedniego stopnia ochrony, zaznaczając wyraźnie, że obejmują one praworządność, sądowe środki ochrony prawnej oraz niezależny nadzór. Artykuł ten przewiduje także możliwość oceny przez Komisję poziomu ochrony zapewnianego na terytorium państwa trzeciego lub w tym państwie w określonym sektorze, w którym odbywa się przetwarzanie. Wprowadza on zasadę, że ogólna decyzja w sprawie stopnia ochrony przyjęta w ramach procedury wynikającej z art. 38 ogólnej dyrektywy o ochronie danych jest objęta zakresem obowiązywania niniejszej dyrektywy. Alternatywnie Komisja może przyjąć decyzję w sprawie odpowiedniego stopnia ochrony wyłącznie do celów niniejszej decyzji.

Artykuł 35 określa odpowiednie gwarancje, które należy zapewnić przed dokonaniem międzynarodowego przekazania, w przypadku braku decyzji Komisji w sprawie odpowiedniego stopnia ochrony. Gwarancje te mogę być wprowadzone w prawnie wiążącym instrumencie, takim jak umowa międzynarodowa. Administrator może też, na podstawie oceny okoliczności towarzyszących przekazaniu danych stwierdzić, że gwarancje takie są zapewnione.

Artykuł 36 określa wyjątki dotyczące przekazania danych w oparciu o art. 26 dyrektywy 95/46/WE i art. 13 decyzji ramowej 2008/977/WSiSW.

Artykuł 37 zobowiązuje państwa członkowskie do ustanowienia przepisów nakazujących administratorowi danych informowanie odbiorcy o wszelkich ograniczeniach przetwarzania oraz podjęcie wszystkich rozsądnych kroków na rzecz zapewnienia, by odbiorcy danych osobowych w państwie trzecim lub organizacji międzynarodowej stosowali się do tych ograniczeń.

Artykuł 38 wyraźnie przewiduje mechanizmy współpracy międzynarodowej w celu ochrony danych osobowych między Komisją a organami nadzorczymi państw trzecich, w szczególności takie, 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.

ROZDZIAŁ VI – NIEZALEŻNE ORGANY NADZORCZE

3.4.5.1. SEKCJA 1 – NIEZALEŻNY STATUS

Artykuł 39 zobowiązuje państwa członkowskie, na podstawie art. 28 ust. 1 dyrektywy 95/46/WE i art. 25 decyzji ramowej 2008/977/WSiSW, do ustanowienia organów nadzorczych, którymi mogą być organy nadzorcze ustanowione na mocy ogólnego rozporządzenia o ochronie danych, rozszerzając zakres powierzonych im zadań o przyczynianie się do spójnego stosowania dyrektywy na terytorium całej Unii.

Artykuł 40 wyjaśnia warunki niezależności organów nadzorczych, co stanowi wdrożenie orzecznictwa Trybunału Sprawiedliwości Unii Europejskiej[29], inspirowane także art. 44 rozporządzenia (WE) nr 45/2001[30].

Artykuł 41 określa ogólne warunki członkostwa w organie nadzorczym, co stanowi wdrożenie odpowiedniego orzecznictwa[31], inspirowane także art. 42 ust. 2-6 rozporządzenia (WE) 45/2001.

Artykuł 42 podaje zasady ustanawiania organu nadzorczego, w tym warunki dotyczące jego członków, które określać mają przepisy państwa członkowskiego.

Artykuł 43 dotyczy tajemnicy służbowej obowiązującej członków i personel organu nadzorczego na podstawie art. 28 ust. 7 dyrektywy 95/46/WE i art. 25 ust. 4 decyzji ramowej 2008/977/WSiSW.

3.4.5.2. SEKCJA 2 – OBOWIĄZKI I UPRAWNIENIA

Artykuł 44 określa kompetencje organów nadzorczych, na podstawie art. 28 ust. 6 dyrektywy 95/46/WE i art. 25 ust. 1 decyzji ramowej 2008/977/WSiSW. Sądy, w zakresie sprawowanych funkcji sądowniczych, są zwolnione z kontroli organu nadzorczego, lecz nie są zwolnione ze stosowania materialnych przepisów dotyczących ochrony danych.

Artykuł 45 stanowi, że państwa członkowskie mają ustanowić przepisy określające obowiązki organów nadzorczych, w tym dotyczące wysłuchiwania skarg i prowadzenia postępowań w ich sprawie oraz szerzenia w społeczeństwie wiedzy na temat ryzyka, przepisów, gwarancji i praw. Szczególnym obowiązkiem organów nadzorczych w kontekście niniejszej dyrektywy jest, w przypadku odmowy lub ograniczenia bezpośredniego dostępu, korzystanie z prawa dostępu w imieniu podmiotu danych oraz sprawdzanie zgodności z prawem przetwarzania danych.

Artykuł 46 określa kompetencje organu nadzorczego, w oparciu o art. 28 ust. 3 dyrektywy 95/46/WE i art. 25 ust. 2 i 3 decyzji ramowej 2008/977/WSiSW. Artykuł 47 nakłada na organy nadzorcze obowiązek sporządzania rocznych sprawozdań z działalności, na podstawie art. 28 ust. 5 dyrektywy 95/46/WE.

3.4.6. ROZDZIAŁ VII - WSPÓŁPRACA

Artykuł 48 wprowadza przepisy dotyczące obowiązkowej pomocy wzajemnej, podczas gdy art. 28 ust. 6 akapit drugi dyrektywy 95/46/WE przewidywał jedynie ogólny obowiązek współpracy, bez określenia dalszych szczegółów.

Artykuł 49 przewiduje, że Europejska Rada Ochrony Danych ustanowiona ogólnym rozporządzeniem o ochronie danych wypełnia swoje zadania także w odniesieniu do operacji przetwarzania objętych zakresem niniejszej dyrektywy. Aby zapewnić dodatkowe wsparcie, Komisja będzie zasięgać porady przedstawicieli organów odpowiedzialnych za zapobieganie

---

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

30 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.

31 *Op. cit*, przypis 27.

przestępstwom, prowadzenie dochodzeń w ich sprawie, wykrywanie ich lub ściganie i wykonywanie kar w państwach członkowskich, jak również przedstawicieli Europolu i Eurojustu, za pośrednictwem grupy ekspertów ds. aspektów ochrony danych związanych z egzekwowaniem prawa.

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

Artykuł 50 przewiduje uprawnienie każdej podmiotu danych do zgłaszania organowi nadzorczemu skarg, na podstawie art. 28 ust. 4 dyrektywy 95/46/WE, i dotyczy wszelkich naruszeń dyrektywy związanych ze skargą. Wymienia on ponadto organy, organizacje lub stowarzyszenia, które mogą zgłaszać skargi w imieniu podmiotu danych lub, w przypadku naruszenia ochrony danych osobowych, niezależnie od skargi podmiotu danych.

Artykuł 51 dotyczy prawa do skorzystania z sądowego środka ochrony prawnej przeciwko organowi nadzorczemu. Opiera się on na ogólnym przepisie art. 28 ust. 3 dyrektywy 95/46/WE i zawiera szczegółowe uregulowanie stanowiące, że podmiot danych, może wszcząć postępowanie sądowe w celu zobowiązania organu nadzorczego do zareagowania na skargę.

Artykuł 52 dotyczy prawa do sądowego środka ochrony prawnej przeciwko administratorowi lub podmiotowi przetwarzającemu , w oparciu o art. 22 dyrektywy 95/46/WE i art. 20 decyzji ramowej 2008/977/WSiSW.

Artykuł 53 wprowadza wspólne przepisy dotyczące postępowań sądowych, w tym praw organów, organizacji lub zrzeszeń reprezentujących podmioty danych przed sądem, oraz prawa organów nadzorczych do udziału w postępowaniach prawnych. Obowiązek zapewnienia przez państwa członkowskie szybkich postępowań sądowych został zainspirowany art. 18 ust. 1 dyrektywy 2000/31/WE o handlu elektronicznym[32].

Artykuł 54 zobowiązuje państwa członkowskie do ustanowienia przepisów dotyczących prawa do odszkodowania. Opiera się on na art. 23 dyrektywy 95/46/WE i art. 19 ust. 1 decyzji ramowej, rozciągając to prawo na szkody spowodowane przez podmioty przetwarzające dane i wyjaśniając zasady odpowiedzialności współadministratorów i podmioty współprzetwarzających dane.

Artykuł 55 zobowiązuje państwa członkowskie do ustanowienia przepisów dotyczących sankcji, nakładania sankcji za naruszenia dyrektywy oraz zapewnienia wdrożenia jej przepisów.

3.4.8. ROZDZIAŁ IX – AKTY DELEGOWANE I WYKONAWCZE

Artykuł 56 zawiera standardowe przepisy dotyczące wykonywania przekazanych uprawnień zgodnie z art. 290 TFUE. Dzięki temu prawodawca może przekazywać Komisji uprawnienia do przyjmowania aktów o charakterze nieustawodawczym o powszechnym zakresie zastosowania, które uzupełniają lub zmieniają niektóre, inne niż zasadnicze elementy aktu ustawodawczego (akty quasi-ustawodawcze).

---

[32] Dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 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.

Artykuł 57 zawiera przepis 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.

3.4.9. ROZDZIAŁ X – POSTANOWIENIA KOŃCOWE

Artykuł 58 uchyla decyzję ramową 2008/977/WSiSW

Artykuł 59 stanowi, że dyrektywa nie wpływa na przepisy szczególne dotyczące przetwarzania danych osobowych przez właściwe organy na potrzeby zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich i ścigania oraz wykonywania kar kryminalnych zawarte w aktach Unii i regulujące przetwarzanie danych osobowych lub dostęp do systemów informacyjnych w zakresie obowiązywania dyrektywy, które zostały przyjęte przed przyjęciem niniejszej dyrektywy.

Artykuł 60 wyjaśnia stosunek niniejszej dyrektywy do umów międzynarodowych wcześniej zawartych przez państwa członkowskie w dziedzinie współpracy wymiarów sprawiedliwości w sprawach karnych oraz współpracy policyjnej.

Artykułu 61 przewiduje obowiązek dokonania przez Komisję oceny wdrażania dyrektywy, a następnie złożenia z tego sprawozdania, w celu oceny potrzeby uzgodnienia uprzednio przyjętych przepisów szczególnych, o których mowa w art. 59, z niniejszą dyrektywą.

Artykuł 62 stanowi o obowiązku transpozycji przez państwa członkowskie dyrektywy do ich prawa krajowego i zawiadomienia Komisji o przepisach przyjętych na mocy dyrektywy.

Artykuł 63 określa datę wejścia w życie dyrektywy.

Artykuł 64 wskazuje adresatów niniejszej dyrektywy.

4. WPŁYW NA BUDŻET

Ocena finansowych skutków regulacji towarzysząca wnioskowi dotyczącemu ogólnego rozporządzenia o ochronie danych obejmuje wpływ na budżet zarówno rozporządzenia, jak i niniejszej dyrektywy.

2012/0010 (COD)

Wniosek

DYREKTYWA PARLAMENTU EUROPEJSKIEGO I RADY

w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez właściwe organy do celów zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich i ścigania albo wykonywania kar kryminalnych oraz swobodnego przepływu tych danych

PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ,

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

uwzględniając wniosek Komisji Europejskiej,

po przekazaniu projektu aktu ustawodawczego parlamentom narodowym,

po zasięgnięciu opinii Europejskiego Inspektora Ochrony Danych[33],

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 o funkcjonowaniu Unii Europejskiej stanowią, iż każda osoba ma prawo do ochrony danych osobowych jej dotyczących.

(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 zamieszkania osób fizycznych, respektować ich podstawowe prawa i wolności, szczególnie prawo do ochrony danych osobowych. Powinno ono również przyczyniać się do stworzenia obszaru wolności, bezpieczeństwa i sprawiedliwości.

(3) Szybki rozwój technologiczny i globalizacja przyniosły nowe wyzwania w zakresie ochrony danych osobowych. Niezwykle wzrosła skala wymiany i zbierania danych. Technologia umożliwia właściwym organom wykorzystywanie danych osobowych do wykonywania powierzonych im zadań na niespotykaną dotąd skalę.

(4) Wymaga to ułatwienia swobodnego przepływu danych między właściwymi organami na terytorium Unii oraz przekazywania danych do państw trzecich i organizacji

---

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

międzynarodowych, przy równoczesnym zagwarantowaniu wysokiego poziomu ochrony danych osobowych. Przemiany te wymagają budowy mocnych i bardziej spójnych ram ochrony danych w Unii, popartych zdecydowanym egzekwowaniem.

(5) Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych[34] ma zastosowanie do wszystkich operacji przetwarzania danych w państwach członkowskich, odbywających się zarówno w sektorze publicznym, jak i prywatnym. Nie ma ona jednak zastosowania do przetwarzania danych osobowych „w ramach działalności wykraczającej poza zakres prawa Wspólnoty", takiej jak działalność prowadzona w ramach współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej.

(6) Decyzja ramowa Rady 2008/977/JHA z dnia 27 listopada 2008 r. w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych[35] ma zastosowanie w obszarze współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej. Zakres zastosowania tej decyzji ramowej jest ograniczony do przetwarzania danych osobowych przekazywanych lub udostępnianych pomiędzy państwami członkowskimi.

(7) Zapewnienie spójnego, wysokiego poziomu ochrony danych osobowych osób fizycznych oraz ułatwienie wymiany danych osobowych między właściwymi organami państw członkowskich ma zasadnicze znaczenie dla zagwarantowania skutecznej współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej. Aby osiągnąć ten cel konieczne jest zapewnienie we wszystkich państwach członkowskich równorzędnego poziomu ochrony praw i wolności osób fizycznych w zakresie przetwarzania danych osobowych przez właściwe organy w celu zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich lub ścigania i w celu wykonywania kar kryminalnych oraz swobodnego przepływu tych danych. Skuteczna ochrona danych osobowych w całej Unii wymaga wzmocnienia praw podmiotów danych oraz obowiązków podmiotów, które przetwarzają dane osobowe, lecz także równorzędnych uprawnień w zakresie monitorowania i zapewnienia zgodności z przepisami o ochronie danych osobowych w państwach członkowskich.

(8) Artykuł 16 ust. 2 Traktatu o funkcjonowaniu Unii Europejskiej stanowi, że Parlament Europejski i Rada powinny ustanowić przepisy dotyczące ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu takich danych.

(9) Na tej podstawie rozporządzenie UE …../2012 Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych przetwarzania związku z przetwarzaniem danych osobowych i swobodnego przepływu takich danych (ogólne rozporządzenie o ochronie danych) ustanawia ogólne przepisy służące ochronie osób fizycznych w zakresie przetwarzania danych osobowych oraz zagwarantowaniu swobodnego przepływu danych osobowych na terytorium Unii.

---

[34] Dz.U. L 281 z 23.11.1995, s. 31.
[35] Dz.U. L 350 z 30.12.2008, s. 60.

(10) W deklaracji 21 w sprawie ochrony danych osobowych w dziedzinie współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej załączonej do Aktu końcowego konferencji międzyrządowej, która przyjęła Traktat z Lizbony, konferencja uznała fakt, że konieczne może okazać się przyjęcie szczególnych przepisów dotyczących ochrony danych osobowych i swobodnego przepływu tych danych w dziedzinach współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej, opartych na art. 16 Traktatu o funkcjonowaniu Unii Europejskiej, ze względu na szczególny charakter tych dziedzin.

(11) Dlatego też osobna dyrektywa powinna uwzględniać szczególnych charakter tych dziedzin, ustanawiając przepisy dotyczące ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez właściwe organy do celów zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich lub ścigania i wykonywania kar kryminalnych.

(12) Aby zagwarantować jednakowy poziom ochrony osób fizycznych poprzez prawnie egzekwowalne prawa obowiązujące na terytorium całej Unii oraz zapobiec różnicom utrudniającym wymianę danych osobowych między właściwymi organami, dyrektywa powinna przewidywać zharmonizowane przepisy dotyczące ochrony i swobodnego przepływu danych w obszarze współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej.

(13) Niniejsza dyrektywa umożliwia uwzględnienie zasady publicznego dostępu do dokumentów urzędowych przy stosowaniu przepisów w niej ustanowionych.

(14) Ochrona zapewniana na mocy niniejszej dyrektywy powinna dotyczyć osób fizycznych, niezależnie od ich obywatelstwa lub miejsca zamieszkania, w zakresie przetwarzania danych osobowych.

(15) Ochrona osób fizycznych powinna być neutralna pod względem technologicznym i nie powinna zależeć od zastosowanych 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 niniejszej dyrektywy. Dyrektywa nie powinna mieć zastosowania do przetwarzania danych w toku działalności leżącej poza zakresem prawa Unii, w szczególności dotyczącej bezpieczeństwa narodowego, ani do przetwarzania danych przez instytucje, organy, biura i agencje Unii, takie jak Europol czy Eurojust.

(16) Zasady ochrony powinny być stosowane do wszelkich informacji dotyczących zidentyfikowanych lub możliwych do zidentyfikowania osób fizycznych. Aby ustalić, czy można zidentyfikować daną osobę fizyczną, należy wziąć pod uwagę wszystkie sposoby, jakimi może 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.

(17) Za dane osobowe dotyczące zdrowia powinny być uznawane w szczególności wszelkie dane dotyczące stanu zdrowia podmiotu danych informacje na temat

rejestracji osoby fizycznej w celu świadczenia na jej rzecz usług zdrowotnych; informacje o płatnościach danej osoby za opiekę zdrowotną lub kwalifikowaniu się danej osoby do korzystania z opieki zdrowotnej; numer, symbol lub oznaczenie przypisane danej osobie wyłącznie w celu identyfikowanie jej dla potrzeb świadczenia opieki zdrowotnej; wszelkie informacje na temat danej osoby zebrane w okresie świadczenia usług 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 nienależnie od ich źródła, którym może być np. lekarz lub inny pracownik służby zdrowia, szpital, urządzenie medyczne, badanie diagnostyczne *in vitro*.

(18) Wszelkie operacje przetwarzania danych osobowych powinny być zgodne z prawem i prowadzone rzetelnie wobec zainteresowanych osób fizycznych. W szczególności należy wyraźnie określić konkretne cele, dla których dane są przetwarzane.

(19) Zapobieganie przestępstwom, prowadzenie dochodzeń w ich sprawie i ściganie ich wymaga zatrzymywania i przetwarzania przez właściwe organy danych osobowych, zgromadzonych w kontekście zapobiegania konkretnym przestępstwom, prowadzenia dochodzeń w ich sprawie i ścigania ich, poza tym kontekstem, by lepiej rozumieć istotę przestępstw i tendencje w tym zakresie, zebrania informacji na temat zorganizowanych sieci kryminalnych oraz powiązania różnych wykrytych przestępstw.

(20) Dane osobowe nie powinny być przetwarzane do celów niezgodnych z celem , w którym zostały zebrane. Dane osobowe powinny być prawidłowe, właściwe i nie wykraczać poza zakres odpowiadający celowi, dla którego są przetwarzane. Należy podjąć wszelkie stosowne kroki gwarantujące poprawienie lub usunięcie niedokładnych danych osobowych.

(21) Zasadę dokładności danych należy stosować, uwzględniając charakter i cel danej operacji przetwarzania. W szczególności w postępowaniach sądowych oświadczenia zawierające dane osobowe oparte są na subiektywnym osądzie osób fizycznych i w pewnych przypadkach nie zawsze można je zweryfikować. Zatem wymóg dokładności danych nie powinien odnosić się do dokładności oświadczenia, lecz jedynie do faktu, że dane oświadczenie zostało złożone.

(22) W toku wykładni i stosowania ogólnych zasad dotyczących przetwarzania danych osobowych przez właściwe organy do celów zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, ścigania ich i wykrywania oraz wykonywania kar kryminalnych, należy uwzględnić specyfikę tego sektora, w tym szczególne cele w nim realizowane.

(23) Nieodłączną cechę przetwarzania danych osobowych w obszarze współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej jest to, że przetwarzane są dane osobowe należące do różnych kategorii osób, których dane dotyczą. Należy zatem wprowadzić w możliwie największym stopniu rozróżnienie między danymi osobowymi dotyczącymi różnych kategorii osób, takich jak podejrzani, osoby skazane za przestępstwo, pokrzywdzeni i osoby trzecie, takie jak

świadkowie, osoby posiadające istotne informacje lub kontakty oraz wspólnicy podejrzanych i skazanych przestępców.

(24) Na tyle na ile to możliwe należy rozróżniać dane osobowe ze względu na stopień ich dokładności i wiarygodności. Fakty należy rozróżnić od osobistych osądów, w celu zagwarantowania zarówno ochrony osób fizycznych, jak i jakości i wiarygodności informacji przetwarzanych przez właściwe organy.

(25) Aby przetwarzanie danych osobowych było zgodne z prawem, musi być ono konieczne dla spełnienia przez administratora ciążących na nim obowiązków prawnych, w celu wykonania przez właściwy organ, w oparciu o przepisy prawa, zadania realizowanego w interesie publicznym lub w celu ochrony żywotnych interesów osoby, które dane dotyczą, lub innej osoby lub w celu zapobieżenia poważnemu zagrożeniu dla bezpieczeństwa publicznego.

(26) Dane osobowe, które z racji swego charakteru są szczególnie newralgiczne w kontekście podstawowych praw lub prywatności, w tym dane genetyczne, zasługują na szczególną ochronę. Dane te nie powinny być przetwarzane, chyba że przepisy wyraźnie na to zezwalają, przewidując przy tym odpowiednie środki służące zabezpieczeniu słusznych interesów podmiotów danych; lub też gdy przetwarzanie jest niezbędne do ochrony żywotnych interesów podmiotu danych, lub innej osoby; lub też gdy przetwarzane mają być dane wyraźnie udostępnione publicznie podmiot danych.

(27) Każda osoba fizyczna powinna mieć prawo niepodlegania środkom opartym wyłącznie na automatycznym przetwarzaniu, jeżeli wywołują one negatywne skutki prawne dla tej osoby, chyba że prawo zezwala na automatyczne przetwarzanie, przewidując przy tym odpowiednie środki służące zabezpieczeniu słusznych interesów podmiotu danych.

(28) Aby podmioty danych mogły korzystać ze swoich praw, wszelkie informacje do nich kierowane powinny być łatwo dostępne i zrozumiałe, w tym napisane w jednoznacznym, prostym języku.

(29) Należy opracować sposoby ułatwienia podmiotowi danych korzystania z praw przysługujących mu na mocy niniejszej dyrektywy, włączając mechanizmy składania wniosków, wolnych od opłat, dotyczących w szczególności dostępu do danych, poprawiania ich i usunięcia. Administrator powinien być zobowiązany do odpowiedzi na wniosek podmiotu danych bez nieuzasadnionej zwłoki.

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

(31) 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 tej osoby, w momencie ich rejestrowania lub rozsądnym terminie po zebraniu danych, zależnie od okoliczności, w jakich dane są przetwarzane.

(32) Każdej osobie powinno przysługiwać prawo dostępu do zebranych danych 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 uzyskania wiedzy, w szczególności informacji na temat celów, dla których dane są przetwarzane, przez jaki okres i jacy odbiorcy otrzymują dane, w tym w państwach trzecich. Podmioty danych powinny otrzymać kopię ich danych osobowych, które są przetwarzane.

(33) Państwom członkowskim należy zezwolić na przyjęcie środków legislacyjnych umożliwiających opóźnienie, ograniczenie lub odstąpienie od informowania osób, których dane dotyczą o dostępie do ich danych osobowych, w zakresie i w czasie, w jakim takie częściowe lub kompletne ograniczenie stanowi konieczny i proporcjonalny środek w demokratycznym społeczeństwie, przy należytym uwzględnieniu słusznych interesów danej osoby, aby zapobiec utrudnianiu urzędowych lub prawnych dochodzeń, śledztw lub procedur, aby zapobiec utrudnieniom w zapobieganiu przestępstw, ich wykrywaniu, prowadzeniu dochodzeń w ich sprawie i ściganiu lub wykonywaniu kar kryminalnych, by chronić bezpieczeństwo publiczne lub narodowe lub chronić osobę, które dane dotyczą, lub prawa i wolności innych osób.

(34) Podmiot danych powinien zostać zawiadomiony o wszelkich ograniczeniach dostępu na piśmie, w tym o faktycznych i prawnych przyczynach ograniczenia.

(35) Jeżeli państwa członkowskie przyjęły środki legislacyjne ograniczające całkowicie lub częściowo prawo dostępu, podmiot danych powinien mieć prawo wystąpienia do właściwego krajowego organu nadzorczego o sprawdzenie zgodności z prawem przetwarzania. Podmiot danych powinien zostać poinformowany o tym prawie. Jeżeli organ nadzorczy uzyskuje dostęp w imieniu podmiotu danych, podmiot ten powinien zostać poinformowany przez organ nadzorczy przynajmniej o tym, że organ ten przeprowadził wszystkie niezbędne weryfikacje oraz o ich wynikach, jeżeli chodzi o zgodność z prawem przedmiotowych operacji przetwarzania.

(36) Każda osoba powinna mieć prawo do poprawienia niedokładnych danych osobowych jej dotyczących oraz prawo do ich usunięcia, jeżeli przetwarzanie takich danych jest niezgodne z głównymi zasadami ustanowionymi w niniejszej dyrektywie. Jeżeli dane osobowe przetwarzane są w toku dochodzenia i postępowania karnego, poprawianie, prawa do informacji, dostępu, usunięcia i ograniczenia przetwarzania mogą być wykonywane godnie z przepisami krajowej procedury sądowej

(37) Należy obciążyć administratora całkowitą odpowiedzialnością za przetwarzanie danych osobowych prowadzone przez niego samego lub w jego imieniu. W szczególności administrator powinien zapewnić zgodność operacji przetwarzania z przepisami przyjętymi na mocy niniejszej dyrektywy.

(38) Ochrona prawa i wolności osób, których dane dotyczą w zakresie przetwarzania danych osobowych wymaga podjęcia odpowiednich środków technicznych i organizacyjnych w celu zagwarantowania spełnienia wymogów dyrektywy. By zapewnić zgodność z przepisami przyjętymi na mocy niniejszej dyrektywy, administrator powinien przyjąć polityki i wdrożyć odpowiednie środki, które są w szczególności zgodne z zasadą uwzględnienia ochrony danych już w fazie projektowania oraz zasadą domyślnej ochrony danych.

(39) Ochrona praw i wolności podmiotów danych a także zobowiązania i odpowiedzialność administratorów i podmiotów przetwarzających wymaga dokonania w niniejszej dyrektywie jasnego podziału obowiązków, w tym w przypadku gdy administrator określa cele, warunki i sposoby przetwarzania wspólnie z innymi administratorami danych oraz gdy operacja przetwarzania jest dokonywana w imieniu administratora.

(40) Działalność związana z przetwarzaniem danych powinna być udokumentowana przez administratora lub podmiot przetwarzający w celu zapewnienia lepszej zgodności z niniejszą dyrektywą. Każdy administrator i podmiot przetwarzający powinien być zobowiązany do współpracy z organem nadzorczym oraz do udostępniania mu, na żądanie, dokumentacji, tak by mogła ona służyć do monitorowania operacji przetwarzania. .

(41) W celu zagwarantowania skutecznej ochrony praw i wolności osób, których dane dotyczą poprzez działania prewencyjne, administrator lub podmiot przetwarzający powinien w określonych przypadkach konsultować się z organem nadzorczym przed przetwarzaniem.

(42) Naruszenie ochrony danych osobowych, w braku odpowiedniej i szybkiej reakcji, może spowodować poważne szkody, w tym dla reputacji danej osoby. Z tego względu, administrator, niezwłocznie po powzięciu wiadomości o naruszeniu, powinien powiadomić o nim organ nadzorczy. Osoby, których dane osobowe lub prywatność mogłyby ucierpieć wskutek takiego naruszenia, powinny być niezwłocznie powiadamiane, aby umożliwić im podjęcie niezbędnych środków ostrożności. Naruszenie powinno być uznawane za mające niekorzystny wpływ na dane osobowe lub prywatność osoby fizycznej, jeżeli jego skutkiem mogą być np. kradzież lub sfałszowanie tożsamości, uszkodzenie ciała, poważne upokorzenie lub naruszenie dobrego imienia w związku z przetwarzaniem danych osobowych.

(43) Przy określaniu szczegółowych przepisów dotyczących formy i procedur mających zastosowanie przy zgłaszaniu naruszeń ochrony danych osobowych należy odpowiednio uwzględnić okoliczności naruszenia, w tym zbadać, czy dane osobowe były zabezpieczone właściwymi technicznymi środkami ochrony, skutecznie ograniczającymi prawdopodobieństwo niewłaściwego wykorzystania danych. W tych przepisach i procedurach należy ponadto uwzględnić słuszne interesy właściwych organów, w przypadkach gdy przedwczesne ujawnienie mogłoby niepotrzebnie utrudnić badanie okoliczności naruszenia.

(44) Administrator lub podmiot przetwarzający powinien wyznaczyć osobę, która będzie pomagać danemu administratorowi lub podmiotowi w monitorowaniu zgodności przepisów przyjętych na mocy niniejszej dyrektywy. Inspektor ochrony danych może zostać wyznaczony wspólnie przez szereg jednostek właściwego organu. Inspektorzy ochrony danych muszą być w stanie wykonywać swoje obowiązki i zadania niezależnie i skutecznie.

(45) Państwa członkowskie powinny zadbać o to, by przekazywanie danych dokonywane było wyłącznie w przypadku, gdy jest to konieczne do zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich i ścigania albo wykonywania kar kryminalnych oraz gdy administrator w państwie trzecim lub organizacji międzynarodowej jest właściwym organem w rozumieniu niniejszej dyrektywy. Przekazywanie może mieć miejsce w przypadkach, w których Komisja zdecydowała,

że dane państwo trzecie lub organizacja międzynarodowa zapewnia odpowiedni poziom ochrony lub gdy wprowadzono odpowiednie gwarancje.

(46) Komisja może podjąć decyzję, która będzie obowiązywać w całej Unii, że niektóre państwa trzecie lub też jakieś terytorium lub sektor przetwarzający dane w państwie trzecim bądź organizacja międzynarodowa oferują odpowiedni poziom ochrony danych, gwarantując tym samym pewność prawną i jednolitość w całej Unii co do państw trzecich lub organizacji międzynarodowych uznawanych za zapewniające taki poziom ochrony. W takich przypadkach przekazywanie danych osobowych do tych państw może odbywać się bez potrzeby uzyskania dalszego zezwolenia.

(47) Zgodnie z podstawowymi wartościami, na których opiera się Unia, w szczególności ochroną praw człowieka, 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.

(48) Komisja powinna mieć również możliwość uznania, że państwo trzecie lub terytorium bądź sektor przetwarzający dane w państwie trzecim lub organizacja międzynarodowa nie oferują odpowiedniego poziomu ochrony danych. W związku z tym przekazywanie danych osobowych do tego państwa trzeciego powinno być zakazane, chyba że opiera się ono na umowie międzynarodowej, odpowiednich gwarancjach lub odstępstwie. Należy przewidzieć możliwość odbywania konsultacji między Komisją a tymi państwami trzecimi lub organizacjami międzynarodowymi. Taka decyzja Komisji pozostaje jednak bez uszczerbku dla możliwości dokonywania przekazania na podstawie odpowiednich gwarancji lub odstępstwa ustanowionego w dyrektywie.

(49) Przekazanie, które nie jest dokonane w oparciu o taką decyzję stwierdzającą odpowiedni stopień ochrony powinno być dopuszczalne jedynie wtedy, gdy w prawnie wiążącym instrumencie prawnym wprowadzono odpowiednie gwarancje, zapewniające ochronę danych osobowych lub gdy administrator lub podmiot przetwarzający ocenili wszystkie okoliczności towarzyszące operacji przekazywania danych lub zestawowi takich operacji i, na podstawie tej oceny uznaje, że obowiązują odpowiednie gwarancje w zakresie ochrony danych osobowych. W przypadkach, w których brakuje podstawy do dokonywania przekazania należy umożliwić zastosowanie odstępstwa w celu ochrony żywotnych interesów podmiotu danych, lub innej osoby, lub ochrony słusznych interesów podmiotu danych, jeżeli prawo państwa członkowskiego przekazującego dane osobowe tak stanowi lub też jeżeli jest to konieczne dla zapobieżenia bezpośredniemu, poważnemu zagrożeniu dla bezpieczeństwa publicznego państwa członkowskiego lub państwa trzeciego, lub też, w indywidualnych przypadkach, na potrzeby zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich lub ścigania lub w celu wykonywania kar kryminalnych, lub też, w indywidualnych przypadkach, do celów ustanowienia roszczeń prawnych, ich realizacji lub bronienia ich.

(50) Przenoszenie danych osobowych ponad granicami może wiązać się z jeszcze większym ryzykiem niemożności wykonywania przez osoby fizyczne praw do ochrony danych osobowych, by chronić się przed niezgodnym z prawem wykorzystaniem lub ujawnieniem tych danych. 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 oraz niespójne systemy prawne. Z tego względu należy promować ściślejszą współpracę między organami nadzorczymi w zakresie ochrony danych, by pomagać im w wymianie informacji z ich międzynarodowymi odpowiednikami.

(51) Utworzenie w państwach członkowskich organów nadzorczych, wykonujących swoje funkcje w sposób całkowicie niezależny jest koniecznym elementem ochrony osób fizycznych w zakresie przetwarzania danych osobowych. Organy nadzorcze powinny monitorować stosowanie przepisów w sposób zgodny z niniejszą dyrektywą oraz przyczyniać się do ich spójnego stosowania w całej Unii, w celu ochrony osób fizycznych w zakresie przetwarzania ich danych osobowych. W tym celu organu nadzorcze powinny współpracować ze sobą oraz z Komisją.

(52) Państwa członkowskie mogą powierzyć organowi nadzorczemu już wcześniej ustanowionemu w państwach członkowskich na mocy rozporządzenia (UE) …./2012 odpowiedzialność za zadania spoczywające na organach nadzorczych, które mają zostać ustanowione na mocy niniejszej dyrektywy.

(53) Państwa członkowskie mogą ustanowić więcej niż jeden organu nadzorczy, w odzwierciedleniu swojej struktury konstytucyjnej, organizacyjnej i administracyjnej. 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.

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

(55) Niniejsza dyrektywa 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 zadań sądowych w sprawach sądowych i nie powinien mieć zastosowania do innych działań, w których sędziowie mogą brać udział, zgodnie z prawem krajowym.

(56) Aby zapewnić spójne monitorowanie i wykonanie niniejszej dyrektywy 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 wiążących interwencji, podejmowania decyzji i nakładania sankcji, w szczególności w sprawach skarg od osób fizycznych oraz do udziału w postępowaniu sądowym.

(57) Każdy organ nadzorczy powinien rozpatrywać skargi zgłoszone 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 przeprowadzenia dalszego dochodzenia lub koordynacji z innym organem nadzorczym, podmiot danych, powinien zostać o tym niezwłocznie poinformowany.

(58) Organy nadzorcze powinny wspierać się wzajemnie w wykonywaniu swoich zadań oraz świadczyć sobie wzajemną pomoc, by zapewnić spójne stosowanie i egzekwowanie przepisów przyjętych na mocy niniejszej dyrektywy.

(59) Europejska Rada Ochrony Danych ustanowiona rozporządzeniem (UE) …./2012 powinna przyczyniać się do spójnego stosowania niniejszej dyrektywy na terytorium całej Unii, w tym poprzez doradzanie Komisji i promowanie współpracy organów nadzorczych na terytorium całej Unii.

(60) Każdy podmiot danych, powinien mieć prawo do złożenia skargi organowi nadzorczemu w dowolnym państwie członkowskim oraz do skorzystania z sądowego środka ochrony prawnej, jeśli uzna, że jego prawa wynikające z niniejszej dyrektywy są naruszane lub jeśli organ nadzorczy nie zareaguje na skargę albo nie podejmuje działania, pomimo iż jest ono niezbędne do ochrony praw podmiotu danych.

(61) 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, powinny mieć prawo do złożenia skargi organowi nadzorczemu lub skorzystania z prawa do sądowego środka ochrony prawnej w imieniu podmiotów danych jeśli zostały przez nich należycie umocowane, lub też złożenia, niezależnie od skargi podmiotu danych własnej skargi, jeśli uzna, iż doszło do naruszenia ochrony danych osobowych.

(62) 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.

(63) W celu zapewnienia skuteczności postępowań sądowych państwa członkowskie powinny zagwarantować szybkie przyjmowanie środków mających zaradzić lub zapobiec naruszeniom niniejszej dyrektywy.

(64) Szkoda, jaką dana osoba może ponieść wskutek niezgodnego z prawem przetwarzania danych, powinna zostać wyrównana 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.

(65) Na wszystkie osoby fizyczne i prawne, która nie przestrzegają niniejszej dyrektywy, 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.

(66) Aby spełnić cele niniejszej dyrektywy, a 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. W szczególności należy przyjąć akty delegowane dotyczące zawiadamiania organu nadzorczego o naruszeniach ochrony danych osobowych. 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.

(67) Aby zagwarantować jednolite warunki wdrażania niniejszej dyrektywy w zakresie dotyczącym dokumentacji przez administratorów danych i podmioty przetwarzające dane, zwłaszcza w odniesieniu do norm szyfrowania, zgłaszania organowi nadzorczemu naruszeń ochrony danych osobowych oraz odpowiedniego poziomu ochrony zapewnianego przez państwo trzecie lub terytorium lub sektor, w którym odbywa się przetwarzanie w tym państwie trzecim, lub też organizację międzynarodową, Komisji należy powierzyć kompetencje wykonawcze. 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[36].

(68) Środki dotyczące prowadzenia dokumentacji przez administratorów i podmioty przetwarzające, bezpieczeństwa przetwarzania, zgłaszania organowi nadzorczego naruszeń ochrony danych osobowych oraz odpowiedniego poziomu ochrony zapewnianego przez państwo trzecie albo terytorium lub sektor, w którym odbywa się przetwarzanie w tym państwie trzecim, lub też organizację międzynarodową powinny być przyjmowane w trybie procedury sprawdzającej, ze względu na powszechny zakres zastosowania tych aktów.

(69) Komisja powinna przyjąć akty wykonawcze mające natychmiastowe zastosowanie, jeśli, w należycie 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, jest to bezwzględnie konieczne ze względu na potrzebę pilnych działań.

(70) Ponieważ cele niniejszego rozporządzenia, mianowicie ochrona podstawowych praw i wolności osób fizycznych, w szczególności ich prawa do ochrony danych osobowych, oraz zapewnienie swobodnego przepływu danych osobowych 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 niniejsza dyrektywa nie wychodzi poza zakres niezbędny do osiągnięcia tego celu.

(71) Decyzję ramową 2008/977/WSiSW należy uchylić niniejszą dyrektywą.

---

[36] Dz.U. L 55 z 28.2.2011, s. 13.

(72) Dyrektywa nie powinna wpływać na przepisy szczególne dotyczące przetwarzania danych osobowych przez właściwe organy na potrzeby zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich lub ścigania lub w celu wykonywania kar kryminalnych zawarte w aktach Unii przyjętych przed datą przyjęcia niniejszej dyrektywy, regulujące przetwarzanie danych osobowych między państwami członkowskimi lub dostęp wyznaczonych organów państw członkowskich do systemów informacyjnych ustanowionych na mocy Traktatów. Komisja powinna ocenić sytuację pod kątem stosunku niniejszej dyrektywy do aktów przyjętych przed datą przyjęcia niniejszej dyrektywy regulujących przetwarzanie danych osobowych między państwami członkowskimi lub dostęp wyznaczonych organów państw członkowskich do systemów informacyjnych ustanowionych na mocy Traktatów, w celu oceny potrzeby uzgodnienia tych przepisów szczególnych z niniejszą dyrektywą.

(73) Aby zagwarantować całościową i spójną ochronę danych osobowych w Unii umowy międzynarodowe zawarte przez państwa członkowskie przed wejściem w życie niniejszej dyrektywy powinny zostać zmienione zgodnie z niniejszą dyrektywą.

(74) Niniejsza dyrektywa pozostaje bez uszczerbku dla przepisów dotyczących zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej ustanowionych w dyrektywie 2011/93/UE Parlamentu Europejskiego i Rady z dnia 13 grudnia 2011 r.[37].

(75) Zgodnie z art. 6a Protokołu w sprawie stanowiska Zjednoczonego Królestwa i Irlandii w odniesieniu do przestrzeni wolności, bezpieczeństwa i sprawiedliwości załączonego do Traktatu o Unii Europejskiej i Traktatu o funkcjonowaniu Unii Europejskiej, Zjednoczone Królestwo i Irlandia nie są związane przepisami ustanowionymi w niniejszej dyrektywie w przypadkach, w których państwa te nie są związane przepisami regulującymi formy współpracy wymiarów sprawiedliwości w sprawach karnych lub współpracy policyjnej, które wymagają przestrzegania przepisów ustanowionych na podstawie art. 16 Traktatu o funkcjonowaniu Unii Europejskiej.

(76) Zgodnie z art. 2 i 2a Protokołu w sprawie stanowiska Danii załączonego do Traktatu o Unii Europejskiej i Traktatu o funkcjonowaniu Unii Europejskiej, Dania nie jest związana niniejszą dyrektywą ani nie ma ona do niej zastosowania. Ze względu na to, że niniejsza dyrektywa stanowi rozwinięcie dorobku Schengen w rozumieniu postanowień tytułu V Traktatu o funkcjonowaniu Unii Europejskiej Dania, zgodnie z art. 4 tego protokołu, w terminie sześciu miesięcy od daty przyjęcia niniejszej dyrektywy podejmuje decyzję czy dokona transpozycji dyrektywy do swojego prawa krajowego.

(77) W odniesieniu do Norwegii i Islandii, niniejsza dyrektywa stanowi rozwinięcie przepisów dorobku Schengen 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[38].

(78) W odniesieniu do Szwajcarii, niniejsza dyrektywa stanowi rozwinięcie przepisów dorobku Schengen w rozumieniu Umowy zawartej między Unią Europejską i

---

37 Dz.U. L 335 z 17.12.2011, s. 1.

38 Dz.U. L 176 z 10.7.1999, s. 36.

Wspólnotą Europejską a Konfederacją Szwajcarską w sprawie włączenia Konfederacji Szwajcarskiej we wprowadzanie w życie, stosowanie i rozwój dorobku Schengen[39].

(79) W odniesieniu do Lichtensteinu, niniejsza dyrektywa stanowi rozwinięcie przepisów dorobku Schengen 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[40].

(80) Niniejsza dyrektywa respektuje prawa podstawowe i jest zgodna z zasadami uznanymi w Karcie praw podstawowych Unii Europejskiej utrwalonej w Traktacie, w szczególności prawem do poszanowania życia prywatnego i rodzinnego, prawem do ochrony danych osobowych oraz prawem do skutecznego środka ochrony prawnej i rzetelnego procesu. Ograniczenia tych praw są zgodne z art. 52 ust. 1 karty, ponieważ są niezbędne do realizacji celów leżących w interesie ogólnym uznanych przez Unię lub ze względu na potrzebę ochrony praw i wolności innych osób.

(81) Zgodnie ze wspólną deklaracją polityczną państw członkowskich i Komisji dotyczącą dokumentów wyjaśniających z dnia 28 września 2011 r., państwa członkowskie zobowiązały w uzasadnionych przypadkach dołączyć do zawiadomienia o swoich środkach transpozycji przynajmniej jeden dokument wyjaśniający związek między elementami dyrektywy a odpowiadającymi im częściami krajowych instrumentów transpozycyjnych. W odniesieniu do niniejszej dyrektywy prawodawca uznaje przekazanie tych dokumentów za uzasadnione,

(82) Niniejsza dyrektywa nie powinna stanowić dla państw członkowskich przeszkody we wdrażaniu w krajowych przepisach o postępowaniu karnym środków zapewniających możliwość korzystania przez podmioty danych z prawa do informacji, dostępu, poprawienia, usunięcia i ograniczenia ich danych osobowych w toku postępowania karnego oraz ewentualnych ograniczeń tych praw.

PRZYJMUJĄ NINIEJSZĄ DYREKTYWĘ:

ROZDZIAŁ I
PRZEPISY OGÓLNE

Artykuł 1
Przedmiot i cele

1. Niniejsza dyrektywa ustanawia przepisy dotyczące ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez właściwe organy do celów zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich lub ścigania i wykonywania kar kryminalnych.

---

39 Dz.U. L 53 z 27.2.2008, s. 52.
40 Dz.U. L 160 z 18.6.2011, s. 19.

2. Zgodnie z niniejszą dyrektywą państwa członkowskie:

a) chronią prawa podstawowe i wolności osób fizycznych, w szczególności ich prawo do ochrony danych osobowych; oraz

b) zapewniają, by wymiana danych osobowych przez właściwe organy w Unii nie była ani ograniczana, ani zakazywana z przyczyn związanych z ochroną osób fizycznych w zakresie przetwarzania danych osobowych.

Artykuł 2
Zakres

1. Niniejsza dyrektywa ma zastosowania do przetwarzania danych osobowych przez właściwe organy do celów, o których mowa w art. 1 ust. 1.

2. Niniejsza dyrektywa ma zastosowanie do przetwarzania danych osobowych w sposób zautomatyzowany w całości lub w części oraz innych rodzajów przetwarzania danych osobowych, stanowiących część zbioru danych lub mających stanowić część zbioru danych.

3. Niniejsza dyrektywa 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.

Artykuł 3
Definicje

Do celów niniejszej dyrektywy:

(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 też 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 przekazywanie, rozpowszechnianie lub udostępnianie w inny sposób, dopasowywanie lub łączenie, ograniczanie usuwanie lub niszczenie;

(4) „ograniczenie przetwarzania” oznacza oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przetwarzania w przyszłości;

(5) „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;

(6) „administrator” oznacza właściwy organ publiczny, który samodzielnie lub wspólnie z innymi organami ustala cele, warunki i sposoby przetwarzania danych osobowych; w przypadkach, w których cele, warunki i sposoby przetwarzania ustalane są prawem Unii lub państwa członkowskiego, administrator lub szczególne kryteria wyznaczania go mogą zostać określone w prawie Unii lub państwa członkowskiego;

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

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

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

(14) „właściwe organy” oznaczają każdy organ publiczny właściwy do celów zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich lub ścigania oraz wykonywania kar kryminalnych;

(15) „organ nadzorczy” oznacza organ publiczny ustanowiony przez państwo członkowskie zgodnie z art. 39.

ROZDZIAŁ II
ZASADY

Artykuł 4
Zasady dotyczące przetwarzania danych osobowych

Państwa członkowskie stanowią przepisy nakazujące, by dane osobowe były:

a) przetwarzane rzetelnie i zgodnie z prawem;

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

c) prawidłowe, właściwe oraz by nie wykraczały poza zakres niezbędny do celów, dla których są przetwarzane;

d) dokładne i, w razie potrzeby, aktualne; należy podjąć wszelkie zasadne działania, by zapewnić niezwłoczne usunięcie lub poprawienie niedokładnych 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;

f) przetwarzane pod nadzorem i na odpowiedzialność administratora, który zapewnia zgodność z przepisami przyjętymi na mocy niniejszej dyrektywy.

.

Artykuł 5
Rozróżnianie poszczególnych kategorii osób , których danych dotyczą

1. Państwa członkowskie stanowią przepisy wymagające od administratorów, by w możliwym zakresie rozróżniali dane osobowe poszczególnych kategorii podmiotów danych takich jak:

a) osoby, w stosunku do których istnieją poważne podstawy by przypuszczać, że popełniły lub zamierzają popełnić przestępstwo;

b) osoby skazane za przestępstwo;

c) osób, które padły ofiarą przestępstwa lub w przypadku których określone fakty wskazują, że mogły paść ofiarą przestępstwa;

d) osoby trzecie w stosunku do przestępstwa, takie jak osoby, które mogą być wezwane do złożenia zeznań w ramach dochodzenia dotyczącego przestępstwa lub dalszych etapów postępowania karnego lub osoby mogące dostarczyć

informacji o przestępstwach albo osoby mające kontakt z jedną z osób wymienionych w lit. a) lub b) albo wspólnicy tych osób; oraz

e) osoby, które nie należą do żadnej z wyżej wymienionych kategorii.

Artykuł 6
Różne stopnie dokładności i wiarygodności danych osobowych

1. Państwa członkowskie zapewniają by, na ile to możliwe, różne kategorie danych osobowych poddawanych przetwarzaniu były rozróżniane według stopnia ich dokładności i wiarygodności.

2. Państwa członkowskie zapewniają, na ile to możliwe, rozróżnienie między danymi osobowymi opartymi na faktach i danymi osobowymi opartymi na indywidualnej ocenie.

Artykuł 7
Zgodność z prawem przetwarzania

Państwa członkowskie stanowią przepisy przewidujące, że przetwarzanie danych osobowych jest zgodne z prawem jedynie wtedy o ile jest ono niezbędne:

a) do wykonania zadania realizowanego przez właściwy organ, w oparciu o prawo, do celów określonych w art. 1 ust. 1; lub

b) do wypełnienia obowiązku prawnego ciążącego na administratorze; lub

c) w celu ochrony żywotnych interesów podmiotu danych lub innej osoby; lub

d) dla zażegnania bezpośredniego i poważnego zagrożenia dla bezpieczeństwa publicznego.

Artykuł 8
Przetwarzanie szczególnych kategorii danych osobowych

1. Państwa członkowskie zabraniają przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, wierzenia religijne lub przekonania filozoficzne, przynależność do związków zawodowych, jak również przetwarzania danych genetycznych lub danych dotyczących zdrowia i życia seksualnego.

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

   a) na przetwarzanie zezwala prawo przewidujące odpowiednie gwarancje; lub

   b) przetwarzanie jest niezbędne w celu ochrony żywotnych interesów podmiotu danych lub innej osoby; lub

   c) przetwarzanie dotyczy danych osobowych, które zostały wyraźnie podane do publicznej wiadomości przez podmiot danych.

Artykuł 9

Środki oparte na profilowaniu i automatycznym przetwarzaniu

1. Państwa członkowskie stanowią przepisy przewidujące, że środki wywołujące niekorzystne skutki prawne dla podmiotu danych, lub mające na tę osobę istotny wpływ i oparte wyłącznie na automatycznym przetwarzaniu danych mającym służyć ocenie niektórych aspektów o charakterze osobistym podmiotu danych, jest zakazane, chyba że zostanie dopuszczone prawem, które przewiduje również gwarancje słusznych interesów podmiotu danych.

2. 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. 8.

ROZDZIAŁ III

PRAWA PODMIOTU DANYCH

Artykuł 10

Tryby wykonywania praw przez podmiot danych

1. Państwa członkowskie stanowią przepisy przewidujące, że administrator podejmuje wszystkie rozsądne kroki, aby dysponować przejrzystymi i łatwo dostępnymi politykami w zakresie przetwarzania danych osobowych i wykonywania praw przez podmioty danych.

2. Państwa członkowskie stanowią przepisy przewidujące, że wszelkie informacje i komunikaty dotyczące przetwarzania danych osobowych mają być przekazywane przez administratora podmiotowi danych w czytelnej formie, w jasnym i prostym języku.

3. Państwa członkowskie stanowią przepisy przewidujące, że administrator podejmuje wszystkie rozsądne kroki w celu ustanowienia procedur dostarczenia informacji, o których mowa w art. 11 i wykonywania praw podmiotów danych o których mowa w art. 12-17.

4. Państwa członkowskie stanowią przepisy przewidujące, że administrator niezwłocznie informuje podmiot danych o sposobie reakcji na jego wniosek.

5. Państwa członkowskie stanowią przepisy przewidujące, że informacje oraz wszelkie czynności podjęte przez administratora w odpowiedzi na wniosek, o którym mowa w ust. 3 i 4, są zwolnione z opłat. Jeśli wnioski są dokuczliwe, w szczególności ze względu na składanie ich w sposób uporczywy albo ze względu na zakres wniosku, administrator może pobrać opłatę za udzielenie informacji lub podjęcie wnioskowanych czynności lub też może nie wykonać wnioskowanych czynności. W takim przypadku na administratorze spoczywa ciężar udowodnienia dokuczliwego charakteru wniosku.

Artykuł 11

Informacje o podmiocie danych

1. Jeżeli zbierane są dane osobowe odnoszące się do podmiotu danych państwa członkowskie zapewniają podejmowanie przez administratora wszelkich stosownych środków w celu udzielenia podmiotowi danych co najmniej następujących informacji dotyczących:

   a) tożsamości i danych kontaktowych administratora i inspektora ochrony danych;

   b) celów przetwarzania danych, do których dane są przeznaczone;

   c) okresu przechowywania danych osobowych;

   d) istnienia prawa do wystąpienia do administratora o uzyskanie wglądu do danych, poprawienie ich, usunięcie lub ograniczenie przetwarzania danych osobowych odnoszących się podmiotu danych;

   e) prawa do złożenia skargi do organu nadzorczego, o którym mowa w art. 39, jak również jego danych kontaktowych;

   f) odbiorcy lub kategorii odbiorców danych osobowych, w tym w państwach trzecich lub organizacjach międzynarodowych;

   g) wszelkich dalszych informacji o ile są one potrzebne do zagwarantowania rzetelnego przetwarzania danych w stosunku do podmiotu danych uwzględniając szczególne okoliczności, w których dane osobowe są przetwarzane.

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 braku przekazania tych danych.

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

   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 osobowe są przetwarzane.

4. Państwa członkowskie mogą przyjąć środki legislacyjnej opóźniające, ograniczające, lub uchylające udzielenie informacji podmiotowi danych, o ile takie częściowe lub całkowite ograniczenie stanowi konieczny i proporcjonalny środek w demokratycznym społeczeństwie, przy należytym uwzględnieniu słusznych interesów danej osoby:

   a) aby zapobiec utrudnianiu urzędowych lub innych prawnych dochodzeń, śledztw lub procedur;

b) aby zapobiec negatywnemu wpływowi na zapobieganie przestępstwom, wykrywanie ich, prowadzenie dochodzeń w ich sprawie i ich ściganie lub wykonywanie kar kryminalnych;

c) aby chronić bezpieczeństwo publiczne;

d) aby chronić bezpieczeństwo narodowe;

e) aby chronić prawa i wolności innych osób.

5. Państwa członkowskie mogą ustalić kategorie przetwarzania danych, które mogą zostać objęte w całości lub części wyjątkami przewidzianymi w ust. 4.

Artykuł 12
Prawo podmiotu danych do dostępu do danych

1. Państwa członkowskie stanowią przepisy przewidujące prawo podmiotów danych do uzyskania od administratora potwierdzenia, czy przetwarzane są dane osobowe odnoszące się do nich. 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 zostały ujawnione, w szczególności odbiorcy w państwach trzecich;

d) okresu przechowywania danych osobowych;

e) istnienie prawa do wystąpienia do administratora o poprawienie, usunięcie lub ograniczenie przetwarzania danych osobowych odnoszących się do podmiotu danych;

f) prawo do złożenia skargi do organu nadzorczego oraz dane kontaktowe organu nadzorczego;

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

2. Państwa członkowskie stanowią przepisy przewidujące prawo podmiotu danych do uzyskania od administratora kopii danych osobowych poddawanych przetwarzaniu.

Artykuł 13
Ograniczenia prawa do dostępu

1. Państwa członkowskie mogą przyjąć środki legislacyjnej ograniczające, w całości lub w części, prawo dostępu podmiotu danych o ile takie częściowe lub całkowite ograniczenie stanowi konieczny i proporcjonalny środek w demokratycznym społeczeństwie, przy należytym uwzględnieniu słusznych interesów danej osoby:

a) aby zapobiec utrudnianiu urzędowych lub innych prawnych dochodzeń, śledztw lub procedur;

b) aby zapobiec negatywnemu wpływowi na zapobieganie przestępstwom, wykrywanie ich, prowadzenie dochodzeń w ich sprawie i ich ściganie lub wykonywanie kar kryminalnych;

c) aby chronić bezpieczeństwo publiczne;

d) aby chronić bezpieczeństwo narodowe;

e) aby chronić prawa i wolności innych osób.

2. Państwa członkowskie mogą ustalić przepisami prawa kategorie przetwarzania danych, które mogą zostać objęte w całości lub części wyjątkami przewidzianymi w ust. 1.

3. W przypadkach, o których mowa w ust. 1 i 2, państwa członkowskie stanowią przepisy przewidujące, że administrator informuje podmiot danych, na piśmie o wszelkich odmowach lub ograniczeniu dostępu, o przyczynach odmowy oraz możliwości złożenia skargi do organu nadzorczego i wystąpienia o sądowy środek ochrony prawnej. Można nie podawać informacji o faktycznych i prawnych przyczynach wydania decyzji jeżeli ich udzielenie utrudniłoby realizację celu wynikającego z ust. 1.

4. Państwa członkowskie zapewniają, by administrator dokumentował przyczyny nieprzekazania informacji o faktycznych lub prawnych przyczynach wydania decyzji.

Artykuł 14

Tryby korzystania z prawa do dostępu

1. Państwa członkowskie stanowią przepisy przewidujące że podmiot danych, ma prawo do zwrócenia się, w szczególności w przypadkach, o których mowa w art. 13, do organu nadzorczego o sprawdzenie zgodności z prawem przetwarzania.

2. Państwa członkowskie stanowią, że administrator informuje podmiot danych o prawie od zwrócenia się do organu nadzorczego o interwencję na mocy ust. 1.

3. W przypadku skorzystania z prawa, o którym mowa w ust. 1, organ nadzorczy informuje podmiot danych przynajmniej o dokonaniu przez ten organ wszystkich niezbędnych weryfikacji oraz o ich wynikach w odniesieniu do zgodności z prawem danej operacji przetwarzania.

Artykuł 15

Prawo do poprawienia

1. Państwa członkowskie stanowią przepisy przewidujące, że podmiot danych, ma prawo do uzyskania od administratora poprawienia niedokładnych danych

osobowych, które go dotyczą. Podmiot danych, ma prawo do uzyskania uzupełnienia niekompletnych danych osobowych, w szczególności w drodze sprostowania.

2. Państwa członkowskie stanowią przepisy przewidujące, że administrator informuje podmiot danych, na piśmie, o wszelkich odmowach poprawienia danych, o przyczynach odmowy oraz możliwości złożenia skargi do organu nadzorczego i wystąpienia o sądowy środek ochrony prawnej.

Artykuł 16
Prawo do usunięcia

1. Państwa członkowskie stanowią przepisy przewidujące, że podmiot danych ma prawo uzyskania od administratora usunięcia danych osobowych odnoszących się do niego, jeżeli przetwarzanie jest niezgodne z przepisami przyjętymi na mocy art. 4 lit. a)-e), art. 7 i 8 niniejszej dyrektywy.

2. Administrator usuwa dane niezwłocznie.

3. Zamiast usunąć je, administrator oznacza dane osobowe jeżeli:

   a) podmiot danych kwestionuje ich dokładność, przez okres pozwalający administratorowi danych na sprawdzenie dokładności danych; lub

   b) dane osobowe muszą być zachowane do celów dowodowych;

   c) podmiot danych sprzeciwia się ich usunięciu, występując w zamian o ograniczenie ich używania.

4. Państwa członkowskie stanowią przepisy przewidujące, że administrator informuje podmiot danych, na piśmie o wszelkich odmowach usunięcia lub oznaczenia danych, o przyczynach odmowy oraz możliwości złożenia skargi do organu nadzorczego i wystąpienia o sądowy środek ochrony prawnej.

Artykuł 17
Prawa podmiotu danych w dochodzeniu i postępowaniu karnym

Państwa członkowskie mogą ustanowić przepisy przewidujące, że prawa do informacji, dostępu, poprawienia, usunięcia i ograniczenia przetwarzania, o których mowa w art. 11-16 wykonywane są zgodnie z krajowymi przepisami postępowania karnego, jeżeli dane osobowe zawarte są w orzeczeniu lub protokole sądowym przetwarzanym w toku dochodzenia i postępowania karnego.

ROZDZIAŁ IV – ADMINISTRATOR I PODMIOT PRZETWARZAJĄCY

SEKCJA 1
OBOWIĄZKI OGÓLNE

Artykuł 18
Odpowiedzialność administratora

1. Państwa członkowskie stanowią przepisy przewidujące, że administrator przyjmuje polityki i realizuje odpowiednie środki w celu zapewnienia, by przetwarzanie danych osobowych odbywało się zgodnie z przepisami przyjętymi na mocy niniejszej dyrektywy.

2. Środki, o których mowa w ust. 1 obejmują w szczególności:

   a) prowadzenie dokumentacji, o której mowa w art. 23;

   b) spełnianie wymogu wcześniejszej konsultacji wynikającego z art. 26;

   c) realizację wymogów bezpieczeństwa danych ustanowionych w art. 27;

   d) wyznaczenie inspektora ochrony danych na mocy art. 30.

3. Administrator wdraża mechanizmy służące zapewnieniu weryfikacji skuteczności środków, o których mowa w ust. 1 niniejszego artykułu. Jeżeli jest to proporcjonalne, weryfikacja ta prowadzona jest przez niezależnych wewnętrznych lub zewnętrznych audytorów.

Artykuł 19
Uwzględnienie ochrony danych już w fazie projektowania oraz ochrona danych jako opcja domyślna

1. Państwa członkowskie stanowią przepisy przewidujące, że administrator wdraża odpowiednie środki i procedury techniczne i organizacyjne, uwzględniając najnowsze osiągnięcia techniczne oraz koszty wdrożenia, tak by przetwarzanie odpowiadało wymogom przepisów przyjętych na mocy niniejszej dyrektywy oraz gwarantowało ochronę praw osób, których dane dotyczą.

2. Kontroler wdraża mechanizmy służące zapewnieniu, by domyślnie przetwarzane były jedynie te dane osobowe, które są niezbędne do realizacji celów przetwarzania.

Artykuł 20
Współadministratorzy

Państwa członkowskie stanowią przepisy przewidujące, że gdy administrator określa cele, warunki i środki przetwarzania danych osobowych wspólnie z innymi administratorami, współadministratorzy muszą ustalić zakres odpowiedzialności za zgodność z obowiązkami wynikającymi z niniejszego rozporządzenia spoczywającej na każdym z nich, w

szczególności w odniesieniu do procedur i mechanizmów wykonywania praw podmiotu danych w drodze wspólnych uzgodnień.

Artykuł 21
Podmiot przetwarzający

1. Państwa członkowskie stanowią przepisy przewidujące, że gdy operacja przetwarzania realizowana jest w imieniu administratora, administrator musi wybrać podmiot przetwarzający dający wystarczające gwarancje wdrożenia odpowiednich środków i procedur technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom przepisów przyjętych na mocy niniejszej dyrektywy oraz gwarantowało ochronę praw osób, których dane dotyczą.

2. Państwa członkowskie stanowią przepisy przewidujące, że przetwarzanie przez podmiot przetwarzający musi być regulowane aktem prawnym wiążącym podmiot przetwarzający z administratorem i zawierającym w szczególności zapis, że podmiot przetwarzający działa wyłącznie na polecenie administratora, w szczególności gdy przekazywanie danych osobowych jest zakazane.

3. 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. 20.

Artykuł 22
Przetwarzanie z upoważnienia administratora i podmiotu przetwarzającego

Państwa członkowskie stanowią przepisy przewidujące, że podmiot przetwarzający oraz wszelkie osoby działające z upoważnienia administratora lub podmiotu przetwarzającego, które mają dostęp do danych osobowych, mogą je przetwarzać tylko na polecenie administratora, lub gdy wymaga tego prawo Unii lub państwa członkowskiego.

Artykuł 23
Dokumentacja

1. Państwa członkowskie przyjmują przepisy przewidujące, że każdy administrator i podmiot przetwarzający prowadzą dokumentację wszystkich systemów i procedur 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;

   b) celów przetwarzania;

   c) odbiorców lub kategorii odbiorców danych osobowych;

d) przekazywania danych do państw trzecich lub organizacji międzynarodowej, łącznie z określeniem tego państwa trzeciego lub organizacji międzynarodowej.

3. Administrator i podmiot przetwarzający udostępniają dokumentację, na żądanie, organowi nadzorczemu.

Artykuł 24
Prowadzenie ewidencji

1. Państwa członkowskie zapewniają ewidencjonowanie przynajmniej następujących operacji przetwarzania: zbieranie, zmiana, wgląd, ujawnianie, łączenie i usuwanie. W ewidencji uzyskiwania wglądu i ujawniania podaje się w szczególności cel, datę i godzinę takich operacji oraz, w możliwym zakresie, oznaczenie osoby, która uzyskała wgląd do danych osobowych lub ujawniła je.

2. Ewidencja wykorzystywana jest wyłącznie w celu weryfikacji zgodności z prawem przetwarzania danych, monitorowania własnej działalności oraz zagwarantowania integralności i bezpieczeństwa danych.

Artykuł 25
Współpraca z organem nadzorczym

1. Przepisy państw członkowskich przewidują, że administrator i podmiot przetwarzający na żądanie organu nadzorczego współpracują z nim w wykonywaniu jego obowiązków, w szczególności poprzez dostarczanie wszelkich informacji potrzebnych organowi nadzorczemu do wykonywania jego obowiązków.

2. Administrator i podmiot przetwarzający udzielają odpowiedzi na zapytanie organu nadzorczego wykonującego uprawnienia przekazane mu na podstawie art. 46 lit. a) i b) w rozsądnym terminie. Odpowiedź na uwagi organu nadzorczego zawiera opis podjętych środków i osiągniętych rezultatów.

Artykuł 26
Uprzednia konsultacja z organem nadzorczym

1. Państwa członkowskie zapewniają, by – przed przetworzeniem danych osobowych, które będą stanowić część mającego powstać nowego zbioru danych – administrator lub podmiot przetwarzający przeprowadzili konsultacje z organem nadzorczym, jeżeli:

   a) przetwarzane mają być szczególne kategorie danych, o których mowa w art. 8;

   b) rodzaj przetwarzania, w szczególności stosowanie nowych technologii, mechanizmów lub procedur, niesie ze sobą w innym przypadku szczególne ryzyko dla podstawowych praw i wolności podmiotu danych, a zwłaszcza ochrony danych osobowych.

2. Państwa członkowskie mogą ustanowić przepisy przewidujące, że organ nadzorczy ustanawia wykaz operacji przetwarzania, w przypadku których wymagana jest wcześniejsza konsultacja na mocy ust. 1.

SEKCJA 2
BEZPIECZEŃSTWO DANYCH

Artykuł 27
Bezpieczeństwo przetwarzania

1. Państwa członkowskie stanowią przepisy przewidujące, że 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 wprowadzenia.

2. W odniesieniu do automatycznego przetwarzania danych każde państwo członkowskie stanowi przepisy przewidujące, że administrator lub podmiot przetwarzający, po ocenie ryzyk, wdraża środki służące:

   a) uniemożliwieniu osobom nieupoważnionym dostępu do sprzętu używanego do przetwarzania danych osobowych (kontrola dostępu do sprzętu);

   b) zapobieżenia nieupoważnionemu odczytywaniu, kopiowaniu, zmienianiu lub usuwaniu nośników danych (kontrola nośników danych);

   c) zapobieżeniu nieupoważnionemu wprowadzaniu danych oraz nieupoważnionemu kontrolowaniu, zmienianiu lub usuwaniu przechowywanych danych osobowych (kontrola przechowywania);

   d) uniemożliwienia korzystania z systemów automatycznego przetwarzania danych przez osoby nieuprawnione, używające sprzętu do przekazywania danych (kontrola użytkowników);

   e) zapewnieniu, aby osoby uprawnione do korzystania z systemu automatycznego przetwarzania danych miały dostęp wyłącznie do danych objętych posiadanym przez siebie upoważnieniem (kontrola dostępu do danych);

   f) zapewnieniu możliwości zweryfikowania i stwierdzenia, jakim organom dane osobowe zostały lub mogą zostać przesłane lub udostępnione za pomocą sprzętu do przekazywania danych (kontrola przesyłania danych);

   g) zapewnieniu możliwości następczego zweryfikowania i stwierdzenia, jakie dane osobowe zostały wprowadzone do systemów automatycznego przetwarzania danych, kiedy i przez kogo (kontrola wprowadzania danych);

   h) przeciwdziałaniu nieautoryzowanemu odczytowi, kopiowaniu, modyfikowaniu lub usuwaniu danych osobowych podczas przekazywania danych osobowych lub podczas przenoszenia nośników danych (kontrola transportu);

i) zapewnieniu możliwości przywrócenia zainstalowanego systemu w przypadku awarii (przywracalność);

j) zapewnieniu wykonywania przez system swoich funkcji i zgłaszania występujących w nich błędów (niezawodność) oraz zapobieżeniu uszkodzeniom przechowywanych danych spowodowanym błędnym działaniem systemu (integralność).

3. 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 standardów szyfrowania. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 57 ust. 2.

Artykuł 28

Zgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu

1. Państwa członkowskie stanowią przepisy przewidujące, że w przypadku naruszenia ochrony danych osobowych, administrator zgłasza organowi nadzorczemu takie naruszenie bez nieuzasadnionej zwłoki i, w jeśli to możliwe, nie później niż w ciągu 24 godzin od momentu dowiedzenia się o tym naruszeniu. Na żądanie organu nadzorczego administrator dostarcza umotywowane wyjaśnienie w przypadkach, w których zgłoszenie nie zostało przekazane w ciągu 24 godzin.

2. Podmiot przetwarzający ostrzega i informuje administratora niezwłocznie po uzyskaniu wiadomości o naruszeniu ochrony danych osobowych.

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

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

b) imię i nazwisko oraz dane kontaktowe inspektora ochrony danych, o którym mowa w art. 30, lub innego punktu kontaktowego, w którym można uzyskać więcej informacji;

c) zalecenia dotyczące środków mające na celu zmniejszenie ewentualnych negatywnych skutków naruszenia ochrony danych osobowych;

d) opis potencjalnych konsekwencji naruszenia ochrony danych osobowych;

e) opis środków proponowanych lub podjętych przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych.

4. Państwa członkowskie stanowią przepisy przewidujące, że 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. 56 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 zawiadomić o naruszeniu ochrony danych osobowych.

6. Komisja może ustanowić standardowe formularze zawiadomienia przekazywanego organowi nadzorczemu, procedury mające zastosowanie do wymogu zawiadomienia, 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. 57 ust. 2.

Artykuł 29

Zawiadomienie podmiotu danych o naruszeniu ochrony danych osobowych

1. Państwa członkowskie stanowią przepisy przewidujące, że gdy istnieje prawdopodobieństwo, że naruszenie ochrony danych osobowych może niekorzystnie wpłynąć na ochronę danych osobowych lub prywatność osoby, administrator, po dokonaniu zawiadomienia, o którym mowa w art. 28, 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. 28 ust. 3 lit. b) i c).

3. Zawiadomienie 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. Zawiadomienie podmiotu danych może zostać opóźnione, ograniczone lub zaniechane z przyczyn, o których mowa w art. 11 ust. 4.

SEKCJA 3
INSPEKTOR OCHRONY DANYCH

Artykuł 30

Wyznaczenie inspektora ochrony danych

1. Państwa członkowskie stanowią przepisy przewidujące, że administrator lub podmiot przetwarzający wyznaczają inspektora ochrony danych.

2. Inspektor ochrony danych wyznaczany jest na podstawie kwalifikacji zawodowych, a w szczególności specjalistycznej wiedzy na temat przepisów i praktyk w zakresie ochrony danych, jak również zdolność do pełnienia zadań, o których mowa w art. 32.

3. Inspektor ochrony danych może być wyznaczony dla szeregu jednostek organizacyjnych, przy uwzględnieniu struktury organizacyjnej właściwego organu.

Artykuł 31

Status inspektora ochrony danych

1. Państwa członkowskie stanowią przepisy przewidujące, że 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 inspektorowi ochrony danych dostarczono środki umożliwiające wykonywanie spoczywających na nim obowiązków i zadań, o których mowa w art. 32, skutecznie i niezależnie i nie otrzymywał on żadnych instrukcji dotyczących pełnienia swojej funkcji.

Artykuł 32

Zadania inspektora ochrony danych

Państwa członkowskie stanowią przepisy przewidujące, że administrator lub podmiot przetwarzający powierzają inspektorowi ochrony danych przynajmniej poniższe zadania:

a) informowanie administratora lub podmiotu przetwarzającego o ich obowiązkach wynikających z przepisów przyjętych na mocy niniejszej dyrektywy oraz dokumentowanie tej działalności i uzyskiwanych odpowiedzi;

b) monitorowanie wykonania i stosowanie polityk w zakresie ochrony danych osobowych, w tym przydziału obowiązków, szkolenia personelu zaangażowanego w operacje przetwarzania oraz powiązane kontrole;

c) monitorowanie wdrażania i stosowania przepisów przyjętych na mocy niniejszej dyrektywy, 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 ich wniosków składanych w ramach wykonywania praw przysługujących im mocy przepisów niniejszej dyrektywy;

d) zapewnienie prowadzenia dokumentacji, o której mowa w art. 23;

e) monitorowanie dokumentacji, zgłoszeń i zawiadomień dotyczących naruszeń ochrony danych osobowych na mocy art. 28 i 29;

f) monitorowanie stosowania przepisów dotyczących uprzedniej konsultacji z organem nadzorczym, jeśli jest ona wymagana na mocy art. 26;

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 pojedynczego punktu kontaktowego organu nadzorczego w kwestiach związanych z przetwarzaniem oraz zasięganie opinii organu nadzorczego, w razie potrzeby, z inicjatywy inspektora ochrony danych.

ROZDZIAŁ V
PRZEKAZYWANIE DANYCH OSOBOWYCH DO PAŃSTW TRZECICH LUB ORGANIZACJI MIĘDZYNARODOWYCH

Artykuł 33
Ogólne zasady przekazywania danych osobowych

Państwa członkowskie stanowią przepisy przewidujące, że wszelkie operacje przekazywania przez właściwe organy danych osobowych poddawanych przetwarzaniu lub mających być poddawane przetwarzaniu po przekazaniu do państwa trzeciego lub do organizacji międzynarodowej, w tym operacje wtórnego przekazywania do innych państw trzecich lub organizacji międzynarodowych, mogą mieć miejsce wyłącznie gdy:

a) przekazanie jest konieczne do zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich lub ścigania albo do wykonywania kar kryminalnych; oraz

b) administrator i podmiot przetwarzający spełniają warunki ustanowione w niniejszym rozdziale.

Artykuł 34
Przekazywanie na podstawie decyzji stwierdzającej odpowiedni poziom ochrony

1. Państwa członkowskie stanowią przepisy przewidujące, że dane osobowe mogą być przekazywane do państwa trzeciego lub organizacji międzynarodowej, jeżeli Komisja wydała decyzję zgodnie z art. 41 rozporządzenia (UE) ..../2012 lub zgodnie z ust. 3 niniejszego artykułu, w której uznała, że państwo trzecie, terytorium lub sektor przetwarzania w tym państwie trzecim lub dana organizacja międzynarodowa zapewniają odpowiedni poziom ochrony. Takie operacje przekazywania nie wymagają żadnego dodatkowego zezwolenia.

2. W przypadku braku przyjęcia decyzji zgodnie z art. 41 rozporządzenia (UE) …./2012 Komisja ocenia, czy zapewniono odpowiedni poziom ochrony danych, uwzględniając następujące elementy:

   a) praworządność, ogólne i sektorowe przepisy obowiązujące w tym zakresie, w tym dotyczące bezpieczeństwa publicznego, obronności, bezpieczeństwa narodowego i prawa karnego, jak również środki 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 osobom 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, odpowiedzialnych 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 państwo trzecie lub organizację międzynarodową.

3. Komisja może zdecydować, w zakresie, niniejszej dyrektywy, że państwo trzecie, terytorium lub sektor przetwarzający dane w państwie trzecim lub organizacja międzynarodowa zapewniają odpowiedni poziom ochrony w rozumieniu ust. 2. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 57 ust. 2.

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

5. Komisja może zdecydować, w zakresie niniejszej dyrektywy, że państwo trzecie, terytorium lub sektor przetwarzający dane w państwie trzecim lub organizacja międzynarodowa nie zapewniają odpowiedniego poziomu ochrony w rozumieniu ust. 2, 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 podmiotom danych mającym miejsce zamieszkania w Unii, których dane osobowe są przekazywane. Te akty wykonawcze są przyjmowane zgodnie z procedurą sprawdzającą, o której mowa w art. 57 ust. 2 lub, w wyjątkowo naglących przypadkach w odniesieniu do osób fizycznych w zakresie ich prawa do ochrony danych osobowych, zgodnie z procedurą, o której mowa w art. 57 ust. 3.

6. Państwa członkowskie zapewniają, by, w przypadku gdy Komisja podejmie decyzję na mocy art. 5, wszelkie operacje przekazywania danych osobowych do państwa trzeciego, terytorium lub do sektora przetwarzającego dane w tym państwie lub do organizacji międzynarodowej były zakazane, przy czym decyzja ta obowiązuje bez uszczerbku dla operacji przekazywania na mocy art. 35 ust 1 lub zgodnie z art. 36. We właściwym czasie Komisja przystępuje do konsultacji z państwem trzecim lub organizacją międzynarodową w celu zaradzenia sytuacji wynikającej z decyzji podjętej na mocy ust. 5 niniejszego artykułu.

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

8. Komisja monitoruje stosowanie aktów wykonawczych, o których mowa w ust. 3 i 5.

Artykuł 35

Operacje przekazywania dzięki odpowiednim gwarancjom

1. W przypadkach, w których Komisja nie podjęła decyzji na mocy art. 34, państwa członkowskie stanowią przepisy przewidujące, że dane osobowe mogą być przekazywane do odbiorców w państwie trzecim lub organizacji międzynarodowej, jeżeli:

a) w prawnie wiążącym instrumencie zapewniono odpowiednie gwarancje w zakresie ochrony danych osobowych; lub

b) administrator lub podmiot przetwarzający ocenili wszystkie okoliczności towarzyszące przekazaniu danych osobowych, stwierdzając, że istnieją odpowiednie gwarancje w zakresie ochrony danych osobowych.

2. Decyzja o przekazaniu danych na mocy ust. 1 lit. b) musi zostać podjęta przez należycie upoważnionych pracowników. Te operacje przekazywania muszą być dokumentowane a dokumentacja musi być udostępniana na wniosek organowi nadzorczemu.

Artykuł 36
Odstępstwa

W drodze odstępstwa od art. 34 i 35 państwa członkowskie stanowią przepisy przewidujące, że dane osobowe mogą być przekazywane do państwa trzeciego lub organizacji międzynarodowej wyłącznie pod warunkiem, że:

a) przekazanie jest niezbędne dla ochrony żywotnych interesów podmiotu danych lub innej osoby; lub

b) przekazanie jest niezbędne dla zabezpieczenia słusznych interesów podmiotu danych, jeżeli prawo państwa członkowskiego przekazującego dane osobowe tak stanowi; lub

c) przekazanie danych jest konieczne dla zapobieżenia bezpośredniemu i poważnemu zagrożeniu dla bezpieczeństwa publicznego państwa członkowskiego lub państwa trzeciego; lub

d) przekazanie jest konieczne w indywidualnych przypadkach do zapobiegania przestępstwom, prowadzenia śledztw i dochodzeń w ich sprawie, wykrywania ich lub ścigania albo do wykonywania kar kryminalnych; lub

e) przekazanie jest konieczne w indywidualnych przypadkach dla ustalenia, wykonania lub obrony roszczeń prawnych dotyczących zapobieżenia konkretnemu przestępstwu, prowadzenia dochodzenia w jego sprawie, wykrycia go lub ścigania albo wykonania konkretnej kary kryminalnej.

Artykuł 37
Szczególne warunki przekazania danych osobowych

Państwa członkowskie stanowią, że administrator informuje odbiorcę danych osobowych o wszelkich ograniczeniach przetwarzania oraz podejmuje wszystkie rozsądne kroki na rzecz zapewnienia, by ograniczenia te były przestrzegane.

Artykuł 38
Międzynarodowa współpraca na rzecz ochrony danych osobowych

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

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

   b) zapewnienia międzynarodowej wzajemnej pomocy 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 działania 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. 34 ust. 3.

ROZDZIAŁ VI
NIEZALEŻNE ORGANY NADZORCZE

SEKCJA 1
NIEZALEŻNY STATUS

Artykuł 39
Organ nadzorczy

1. Każde państwo członkowskie stanowi przepisy przewidujące, że przynajmniej jeden organ publiczny odpowiada za monitorowanie stosowania przepisów przyjętych na mocy niniejszej dyrektywy oraz przyczynianie się do jej spójnego stosowania na terytorium całej Unii, w celu ochrony podstawowych praw i wolności osób fizycznych w zakresie przetwarzania ich danych osobowych oraz ułatwienia swobodnego przepływu danych osobowych na terytorium Unii. W tym celu organy nadzorcze współpracują ze sobą oraz z Komisją.

2. Państwa członkowskie mogą ustanowić przepisy przewidujące, że organ nadzorczy ustanowiony w państwie członkowskim na mocy rozporządzenia (UE)..../2012 przyjmuje odpowiedzialność za zadania organu nadzorczego, który ma zostać ustanowiony na mocy ust. 1 niniejszego artykułu.

3. Jeżeli w państwie członkowskim ustanowiono więcej niż jeden organ nadzorczy, to dane państwo członkowskie wyznacza organ nadzorczy pełniący rolę punktu kontaktowego na potrzeby faktycznego udziału tych organów w Europejskiej Radzie Ochrony Danych.

Artykuł 40
Niezależność

1. Państwa członkowskie zapewniają, by organ nadzorczy przy wykonywaniu powierzonych mu zadań i kompetencji działał w warunkach pełnej niezależności.

2. Każde państwo członkowskie stanowi przepisy przewidujące, że członkowie organu nadzorczego przy wykonywaniu swoich obowiązków nie zwracają się do nikogo o instrukcje ani nie wypełniają niczyich instrukcji.

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

4. Członkowskie organu nadzorczego po zakończeniu swojej kadencji postępują w sposób uczciwy i ostrożny, jeżeli chodzi o przyjmowanie stanowisk i korzyści.

5. Każde państwo członkowskie zapewnia, by organ nadzorczy otrzymał odpowiednie zasoby ludzkie, techniczne i finansowe, a także pomieszczenia i infrastrukturę niezbędne do skutecznego wykonywania jego obowiązków i kompetencji, w tym tych, która mają być realizowane w kontekście wzajemnej pomocy, współpracy i aktywnego udziału w Europejskiej Radzie Ochrony Danych.

6 Każde państwo członkowskie zapewnia, by organ nadzorczy dysponował własnym personelem wyznaczanym przez dyrektora organu nadzorczego i podlegającym jego kierownictwu.

7. Państwa członkowskie zapewniają, by organ nadzorczy podlegał kontroli finansowej, która nie narusza jego niezależności. Państwa członkowskie zapewniają, by organy nadzorcze miały odrębne budżety roczne. Budżety te są podawane do wiadomości publicznej.

Artykuł 41
Ogólne warunki dotyczące członków organu nadzorczego

1. Państwa członkowskie stanowią przepisy przewidujące, że członkowie organu nadzorczego muszą być wyznaczani albo przez parlament albo przez rząd danego państwa członkowskiego.

2. Członkowie wybierani są spośród osób o niepodważalnej niezależności, mających wykazane doświadczenie i umiejętności niezbędne do pełnienia ich obowiązków, zwłaszcza w obszarze ochrony danych osobowych oraz zapobieganiu przestępstwom, prowadzeniu dochodzeń w ich sprawie, wykrywaniu ich lub ściganiu albo wykonywaniu kar kryminalnych.

3. Obowiązki członka wygasają wraz z zakończeniem kadencji oraz w przypadku rezygnacji lub przymusowego pozbawienia funkcji zgodnie z ust. 5.

4. Członek może zostać zdymisjonowany lub pozbawiony prawa do świadczeń emerytalnych lub innych alternatywnych świadczeń przez właściwy sąd krajowy, jeżeli przestał on spełniać warunki niezbędne do pełnienia obowiązków lub też dopuścił się poważnego uchybienia zawodowego.

5. W przypadku wygaśnięcia kadencji lub rezygnacji członka pełni on nadal swoje obowiązki do czasu wyznaczenia nowego członka.

Artykuł 42
Przepisy dotyczące ustanawianie organu nadzorczego

Każde państwo członkowskie określa w drodze ustawy:

a) tryb ustanowienia i status organu nadzorczego, zgodnie z art. 39 i 40;

b) kwalifikacje, doświadczenie i umiejętności wymagane do pełnienia obowiązków członka organu nadzorczego;

c) przepisy i procedury wyznaczania członków organu nadzorczego, jak również przepisy dotyczące działań lub funkcji nie dających się pogodzić z pełnionymi obowiązkami;

d) długość kadencji członków organu nadzorczego, która nie może być krótsza niż cztery lata, z wyjątkiem pierwszego powołania po wejściu w życie niniejszej dyrektywy, które może częściowo dotyczyć krótszego okresu;

e) czy członek organu nadzorczego może być wyznaczony ponownie;

f) regulaminy i wspólne warunki regulujące obowiązki członków i personelu organu nadzorczego;

g) przepisy i procedury dotyczące ustania pełnienia obowiązków przez członka organu nadzorczego, w tym przypadków, w których przestają oni spełniać warunki niezbędne do pełnienia obowiązków lub gdy dopuszczą się poważnego uchybienia zawodowego.

Artykuł 43
Tajemnica służbowa

Państwa członkowskie stanowią przepisy przewidujące, że członkowie i personel organu nadzorczego, zarówno podczas pełnienia obowiązków służbowych, jak i po zaprzestaniu ich pełnienia, podlegają obowiązkowi zachowania tajemnicy służbowej w odniesieniu do wszelkich poufnych informacji, które uzyskali w toku pełnienia swoich obowiązków służbowych.

SEKCJA 2
OBOWIĄZKI I UPRAWNIENIA

Artykuł 44
Kompetencje

1. Państwa członkowskie stanowią przepisy przewidujące, że każdy organ nadzorczy wykonuje, na terytorium swojego państwa członkowskiego, uprawnienia powierzone mu zgodnie z niniejszą dyrektywą.

2. Państwa członkowskie stanowią przepisy przewidujące, że organ nadzorczy nie ma właściwości do nadzorowania operacji przetwarzania dokonywanych przez sądy w toku wykonywania funkcji sądowych.

Artykuł 45
Obowiązki

1. Państwa członkowskie stanowią przepisy przewidujące, że organ nadzorczy:

   a) monitoruje i zapewnia stosowanie przepisów przyjętych na mocy niniejszej dyrektywy oraz środków służących jej wdrożeniu;

   b) rozpatruje skargi złożone przez podmioty danych lub jakiekolwiek zrzeszenie reprezentujące podmiot danych i należycie przez niego upoważnione, zgodnie z art. 50; prowadzi, w odpowiednim zakresie, dochodzenie w danej sprawie oraz informuje podmiot danych lub zrzeszenie o postępach oraz sposobie rozstrzygnięcia skargi w rozsądnym terminie, w szczególności gdy niezbędne jest dalsze dochodzenie lub koordynacja z innym organem nadzorczym;

   c) weryfikuje zgodność z prawem przetwarzania na mocy art. 14 oraz informuje podmiot danych w rozsądnym terminie o rezultatach tej weryfikacji lub o przyczynach, dla których weryfikacji nie przeprowadzono;

   d) zapewnia wzajemną pomoc innym organom nadzorczym oraz dopilnowuje ścisłego stosowania i egzekwowania przepisów przyjętych na mocy niniejszej dyrektywy;

   e) prowadzi postępowania bądź z własnej inicjatywy, bądź na podstawie skargi, lub też na wniosek innego organu nadzorczego oraz informuje podmiot danych, jeżeli złożył on skargę, o rezultatach dochodzenia w rozsądnym terminie;

   f) monitoruje zmiany w odpowiednich dziedzinach w zakresie, w jakim mają one wpływ na ochronę danych osobowych, w szczególności rozwój technologii informacyjno-komunikacyjnych;

   g) jest konsultowany przez instytucje i organy państwa członkowskiego w sprawie środków legislacyjnych i administracyjnych dotyczących ochrony praw i wolności osób fizycznych w zakresie przetwarzania danych osobowych;

h) jest konsultowany w sprawie operacji przetwarzania przeprowadzanych na mocy art. 26;

i) uczestniczy w działalności Europejskiej Rady Ochrony Danych.

2. Każdy organ nadzorczy prowadzi działania na rzecz pogłębiania w społeczeństwie wiedzy na temat zagrożeń, przepisów, gwarancji i 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 ustanowionych w przepisach przyjętych na mocy niniejszej dyrektywy i, w odpowiednich 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 zostać wypełniony elektronicznie, przy czym dostępne są także inne środki łączności.

5. Państwa członkowskie stanowią przepisy przewidujące, że obowiązki pełnione przez organ nadzorczy nie wiążą się z opłatami dla podmiotu danych.

6. W przypadku gdy wnioski mają charakter dokuczliwy, w szczególności ze względu na ich uporczywy charakter, organ nadzorczy może nałożyć opłatę lub nie podjąć działania, o które zwrócił się podmiot danych. Na organie nadzorczym spoczywa ciężar udowodnienia dokuczliwego charakteru wniosku.

Artykuł 46
Uprawnienia

Państwa członkowskie stanowią przepisy przewidujące, że każdy organ nadzorczy musi posiadać w szczególności:

a) uprawnienia dochodzeniowe, takie jak prawo do dostępu do danych, które stanowią przedmiot operacji przetwarzania, oraz prawo do gromadzenia wszelkich informacji potrzebnych mu do wykonywania swoich funkcji nadzorczych;

b) skuteczne uprawnienia interwencyjne, takie jak wydawanie opinii przed przeprowadzeniem przetwarzania oraz zapewnienie odpowiedniej publikacji takich opinii; nakazywanie ograniczenia dostępu do danych, ich usunięcia lub zniszczenia; nakładanie czasowego lub ostatecznego zakazu przetwarzania danych; wydawanie administratorowi danych ostrzeżeń lub upomnień lub przekazywanie sprawy parlamentowi narodowemu państwa członkowskiego lub innym instytucjom politycznym;

c) uprawnienie do wszczynania postępowań prawnych w przypadku naruszenia przepisów przyjętych na mocy niniejszej dyrektywy lub do powiadamiania organów sądowych o takich naruszeniach.

Artykuł 47
Sprawozdanie z działalności

Państwa członkowskie stanowią przepisy przewidujące, że każdy organ nadzorczy sporządza roczne sprawozdanie z działalności. Sprawozdanie to udostępniane jest Komisji i Europejskiej Radzie Ochrony Danych.

ROZDZIAŁ VII
WSPÓŁPRACA

Artykuł 48
Wzajemna pomoc

1. Państwa członkowskie stanowią przepisy przewidujące, że organy nadzorcze świadczą sobie wzajemną pomoc w celu spójnego wdrażania i stosowania przepisów przyjętych na mocy niniejszej dyrektywy oraz wprowadzają środki na rzecz zapewnienia skutecznej wzajemnej współpracy. Wzajemna pomoc obejmuje w szczególności wnioski o udzielenie informacji oraz środki nadzorcze, takie jak wnioski o przeprowadzenie uprzednich konsultacji, kontroli i dochodzenia.

2. Państwa członkowskie stanowią przepisy przewidujące, że organ nadzorczy podejmuje wszystkie właściwe środki niezbędne, by odpowiedzieć na wniosek innego organu nadzorczego.

3. Organ nadzorczy, do którego skierowano wniosek, informuje organ nadzorczy, od którego wniosek pochodzi, o rezultatach lub, w odpowiednich przypadkach, o postępach albo środkach podjętych w celu realizacji wniosku skierowanego przez ten organ.

Artykuł 49
Zadania Europejskiej Rady Ochrony Danych

1. Europejska Rada Ochrony Danych ustanowiona rozporządzeniem (UE) …./2012 wykonuje następujące zadania w odniesieniu do przetwarzania w zakresie zastosowania niniejszej dyrektywy:

   a) doradzanie Komisji we wszelkich sprawach związanych z ochroną danych osobowych w Unii, w tym na temat wszelkich proponowanych zmian w niniejszej dyrektywie;

   b) badanie, na wniosek Komisji, albo z inicjatywy własnej lub jednego ze swych członków, wszelkich kwestii dotyczących stosowania przepisów przyjętych na mocy niniejszej dyrektywy oraz wydawanie wytycznych, zaleceń i najlepszych praktyk skierowanych do organów nadzorczych w celu zachęcenia do spójnego stosowania tych przepisów;

   c) kontrola praktycznego stosowania wytycznych, zaleceń i najlepszych praktyk, o których mowa w lit. b), oraz składanie Komisji regularnych sprawozdań na ich temat;

d) wydawanie Komisji opinii na temat poziomu ochrony w państwach trzecich lub organizacjach międzynarodowych;

e) wspieranie współpracy i skutecznej dwustronnej i wielostronnej wymiany informacji i praktyk między organami nadzorczymi;

f) wspieranie wspólnych programów szkoleniowych i ułatwianie wymiany personelu między organami nadzorczymi, jak również w odpowiednich przypadkach z organami nadzorczymi państw trzecich lub organizacji międzynarodowych;

g) wspieranie wymiany wiedzy i dokumentacji z organami nadzorującymi ochronę danych na całym świecie, w tym przepisów o ochronie danych i praktyk.

2. Jeżeli Komisja zwraca się o opinię doradczą do Europejskiej Rady Ochrony Danych, może wyznaczyć limit, w którym Europejska Rada Ochrony Danych wydaje taką opinię, przy uwzględnieniu stopnia pilności danej sprawy.

3. Europejska Rada Ochrony Danych przekazuje swoje opinie, wytyczne, zalecenia i najlepsze praktyki Komisji oraz komitetowi, o którym mowa w art. 57 ust. 1 oraz udostępnia je publicznie.

4. Komisja informuje Europejską Radę Ochrony Danych o działaniach podjętych w reakcji na opinię, wytyczne, zalecenia i najlepsze praktyki przedstawione przez Europejską Radę Ochrony Danych.

ROZDZIAŁ VIII
ŚRODKI OCHRONY PRAWNEJ, ODPOWIEDZIALNOŚĆ I SANKCJE

Artykuł 50
Prawo do złożenia skargi do organu nadzorczego

1. Bez uszczerbku dla wszelkich innych administracyjnych lub sądowych środków ochrony prawnej, państwa członkowskie stanowią przepisy przewidujące prawo wszystkich podmiotów danych do złożenia skargi do organu nadzorczego w dowolnym państwie członkowskim, jeżeli uważają one, że przetwarzanie danych osobowych ich dotyczących, nie jest zgodne z przepisami przyjętymi na mocy niniejszej dyrektywy.

2. Państwa członkowskie stanowią przepisy przewidujące dla każdego organu, organizacji lub zrzeszenia, których celem jest ochrona praw i interesów podmiotów danych w zakresie ochrony ich danych osobowych, i które zostały odpowiednio ustanowione zgodnie z prawem państwa członkowskiego, prawo do złożenia skargi do organu nadzorczego w dowolnym państwie członkowskim w imieniu jednego podmiotu danych lub większej liczby tych podmiotów, jeżeli uznają one, że doszło do naruszenia praw podmiotów danych wynikających z niniejszej dyrektywy w rezultacie przetwarzania danych osobowych. Organizacja lub zrzeszenie muszą być należycie upoważnione przez podmiot lub podmioty danych.

3. Państwa członkowskie stanowią przepisy przewidujące dla każdego organu, organizacji lub zrzeszenia, o których mowa w ust. 2, prawo do złożenia, niezależnie od skargi podmiotu danych, skargi do organu nadzorczego w dowolnym państwie członkowskim, jeżeli uznają one, że doszło do naruszenia ochrony danych osobowych.

Artykuł 51

Prawo do sądowego środka ochrony prawnej przeciwko organowi nadzorczemu

1. Państwa członkowskie stanowią przepisy przewidujące prawo od sądowego środka ochrony prawnej od decyzji organu nadzorczego.

2. Każdy podmiot danych ma prawo do sądowego środka ochrony prawnej w celu zobowiązania organu nadzorczego do działania na podstawie skargi, w przypadku braku decyzji niezbędnej do ochrony jego praw lub gdy organ nadzorczy nie poinformuje podmiotu danych w ciągu trzech miesięcy o postępach w rozpatrywania skargi lub rezultatach jej rozpatrzenia zgodnie z art. 45 ust. 1 lit. b).

3. Państwa członkowskie stanowią przepisy przewidujące, że postępowanie przeciwko organowi nadzorczemu wszczynane jest przed sądem państwa członkowskiego, w którym organ nadzorczy ma siedzibę.

Artykuł 52

Prawo do sądowego środka ochrony prawnej przeciwko administratorowi lub podmiotowi przetwarzającemu

Bez uszczerbku dla jakichkolwiek dostępnych administracyjnych środków ochrony prawnej, w tym prawa do złożenia skargi do organu nadzorczego, państwa członkowskie stanowią przepisy przewidujące dla każdej osoby fizycznej prawo do sądowego środka ochrony prawnej, jeżeli uważa ona, że jej prawa ustanowione w przepisach przyjętych na mocy niniejszej dyrektywy zostały naruszone w rezultacie przetwarzania jej danych osobowych niezgodnie z tymi przepisami.

Artykuł 53

Wspólne przepisy dotyczące postępowań sądowych

1. Państwa członkowskie stanowią przepisy przewidujące dla każdego organu, organizacji lub zrzeszenia, o których mowa w art. 50 ust. 2, uprawnienie do korzystania z praw, o których mowa w art. 51 i 52 w imieniu podmiotu danych lub większej liczby takich podmiotów.

2. Każdy organ nadzorczy ma prawo do wszczęcia postępowania prawnego i wszczęcia postępowania przed sądem w celu egzekwowania przepisów przyjętych na mocy niniejszej dyrektywy oraz zagwarantowania spójnej ochrony danych osobowych na terytorium Unii.

3. Państwa członkowskie zapewniają, by skargi przewidziane w prawie krajowym umożliwiały szybkie podjęcie środków, łącznie ze środkami tymczasowymi

mającymi doprowadzić do zaprzestania każdego domniemanego naruszenia oraz zapobieżenia jakiemukolwiek dalszemu naruszeniu przedmiotowych interesów.

Artykuł 54
Odpowiedzialność i prawo do odszkodowania

1. Państwa członkowskie zapewniają, by każdej osobie, która poniosła szkodę wskutek niezgodnej z prawem operacji przetwarzania danych lub innej czynności niezgodnej z przepisami krajowymi przyjętymi na mocy niniejszej dyrektywy, przysługiwało prawo do uzyskania odszkodowania od administratora lub podmiotu przetwarzającego 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 od tej odpowiedzialności w całości lub w części, jeżeli wykaże, że nie jest odpowiedzialny za zdarzenie, które spowodowało szkodę.

Artykuł 55
Kary

Państwa członkowskie ustanawiają przepisy dotyczące kar mających zastosowanie w przypadku naruszenia przepisów przyjętych na mocy niniejszej dyrektywy i podejmują wszelkie niezbędne środki w celu zapewnienia ich wdrożenia. Przewidziane kary muszą być skuteczne, proporcjonalne i odstraszające.

ROZDZIAŁ IX
AKTY DELEGOWANE I WYKONAWCZE

Artykuł 56
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. 28 ust. 5, powierza się Komisji na czas nieokreślony od dnia wejścia w życie niniejszej dyrektywy.

3. Przekazanie uprawnień, o którym mowa w art. 28 ust. 5, 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. 28 ust. 5 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 2 miesiące z inicjatywy Parlamentu Europejskiego lub Rady.

Artykuł 57
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 X
PRZEPISY KOŃCOWE

Artykuł 58
Uchylenie

1. Uchyla się decyzję ramową Rady 2008/977/WSiSW.

2. Odniesienia do uchylonej decyzji ramowej, o której mowa w ust. 1 traktuje się jako odniesienia do niniejszej dyrektywy.

Artykuł 59
Stosunek do uprzednio przyjętych aktów Unii dotyczących współpracy wymiarów sprawiedliwości w sprawach karnych oraz współpracy sądowej

Dyrektywa nie wpływa na przepisy szczególne dotyczące ochrony danych osobowych w zakresie przetwarzania danych osobowych przez właściwe organy na potrzeby zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich lub ścigania albo w celu wykonywania kar kryminalnych zawarte w aktach Unii przyjętych przed datą przyjęcia niniejszej dyrektywy, regulujące przetwarzanie danych osobowych między państwami członkowskimi lub dostęp wyznaczonych organów państw członkowskich do systemów informacyjnych ustanowionych na mocy Traktatów w zakresie zastosowania niniejszej dyrektywy.

Artykuł 60

Stosunek do uprzednio zawartych umów międzynarodowych dotyczących współpracy wymiarów sprawiedliwości w sprawach karnych oraz współpracy sądowej

Umowy międzynarodowe zawarte przez państwa członkowskie przed wejściem w życie niniejszej dyrektywy zostają zmienione, w razie potrzeby, w ciągu pięciu lat od daty wejście w życie niniejszej dyrektywy.

Artykuł 61

Ocena

1. Komisja ocenia stosowanie niniejszej dyrektywy.

2. W ciągu trzech lat po wejściu w życie niniejszej dyrektywy Komisja dokonuje przeglądu innych aktów przyjętych przez Unię Europejską, które regulują przetwarzanie danych osobowych przez właściwe organy, do celów zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich lub ścigania albo wykonywania kar kryminalnych, w szczególności aktów przyjętych przez Unię, o których mowa w art. 59, w celu oceny potrzeby uzgodnienia ich z niniejszą dyrektywą oraz przedstawienia, w razie potrzeby, niezbędnych propozycji dotyczących zmiany tych aktów celem zapewnienia spójnego podejścia do ochrony danych osobowych w zakresie zastosowania niniejszej dyrektywy.

3. Komisja w regularnych odstępach czasu przedkłada sprawozdania z oceny i przeglądu niniejszej dyrektywy na mocy ust. 1 Parlamentowi Europejskiemu i Radzie. Pierwsze sprawozdania zostaną przedłożone najpóźniej cztery lata po wejściu w życie niniejszej dyrektywy. Kolejne sprawozdania przedkłada się następnie co cztery lata. Komisja przedkłada, w razie potrzeby, odpowiednie propozycje dotyczące zmiany niniejszej dyrektywy oraz uzgodnienia innych instrumentów prawnych. Sprawozdanie jest udostępniane publicznie.

Artykuł 62

Wdrażanie

1. Państwa członkowskie przyjmują i publikują, najpóźniej do dnia [data/dwa lata po wejściu w życie], przepisy ustawowe, wykonawcze i administracyjne niezbędne do wykonania niniejszej dyrektywy. Niezwłocznie przekazują Komisji tekst tych przepisów oraz tabelę korelacji pomiędzy tymi przepisami a niniejszą dyrektywą.

   Państwa członkowskie stosują te przepisy od dnia xx.xx.201x [data/dwa lata po wejściu w życie].

   Przepisy przyjęte przez państwa członkowskie zawierają odniesienie do niniejszej dyrektywy lub odniesienie takie towarzyszy ich urzędowej publikacji. Metody dokonywania takiego odniesienia określane są przez państwa członkowskie.

2. Państwa członkowskie przekazują Komisji tekst podstawowych przepisów prawa krajowego, przyjętych w dziedzinie objętej niniejszą dyrektywą.

Artykuł 63
Wejście w życie i stosowanie

Niniejsza dyrektywa wchodzi w życie pierwszego dnia po jej opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

Artykuł 64
Adresaci

Niniejsza dyrektywa skierowana jest do państw członkowskich.

Sporządzono w Brukseli, dnia 25.1.2012 r.

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