Dziennik Urzędowy C 158
Unii Europejskiej

Wydanie polskie

Informacje i zawiadomienia

Tom 59

3 maja 2016

Spis treści

PL

III

(Akty przygotowawcze)

RADA

STANOWISKO RADY (UE) NR 5/2016 W PIERWSZYM CZYTANIU

w sprawie przyjęcia dyrektywy Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylającej decyzję ramową Rady 2008/997/WSiSW

Przyjęte przez Radę w dniu 8 kwietnia 2016 r.

(2016/C 158/01)

PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ,

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

uwzględniając wniosek Komisji Europejskiej,

po przekazaniu projektu aktu ustawodawczego parlamentom narodowym,

uwzględniając opinię Komitetu Regionów [1],

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą [2],

a także mając na uwadze, co następuje:

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

(2) Zasady i przepisy dotyczące ochrony osób fizycznych w związku z przetwarzaniem ich danych osobowych powinny – niezależnie od ich obywatelstwa czy miejsca zamieszkania – przestrzegać ich podstawowych praw i wolności, zwłaszcza prawa do ochrony danych osobowych. Niniejsza dyrektywa ma przyczyniać się do tworzenia przestrzeni wolności, bezpieczeństwa i sprawiedliwości.

(3) Szybki postęp techniczny i globalizacja przyniosły nowe wyzwania w dziedzinie ochrony danych osobowych. Skala zbierania i wymiany danych osobowych znacznie wzrosła. Technologia pozwala na przetwarzanie danych osobowych na niespotykaną dotąd skalę w celu prowadzenia takich czynności jak zapobieganie przestępczości, prowadzenie postępowań przygotowawczych, wykrywanie i ściganie czynów zabronionych lub wykonywanie kar.

(4) Należy ułatwić swobodny przepływ danych osobowych między właściwymi organami do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w tym do celów ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania

[1] Dz.U. C 391 z 18.12.2012, s. 127.

[2] Stanowisko Parlamentu Europejskiego z dnia 12 marca 2014 r. (dotychczas nieopublikowane w Dzienniku Urzędowym) i stanowisko Rady w pierwszym czytaniu z dnia 8 kwietnia 2016 r. Stanowisko Parlamentu Europejskiego z dnia … i decyzja Rady z dnia ….

takim zagrożeniom na terytorium Unii oraz przekazywania takich danych osobowych do państw trzecich i organizacji międzynarodowych, zapewniając przy tym wysoki stopień ochrony danych osobowych. Przemiany te wymagają stworzenia stabilnych i spójniejszych ram dla ochrony danych osobowych w Unii oraz zdecydowanego egzekwowania ich przepisów.

(5) Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady ([1]) ma zastosowanie do całości przetwarzania danych osobowych w państwach członkowskich, 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 działania w ramach współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej.

(6) Decyzja ramowa Rady 2008/977/WSiSW ([2]) ma zastosowanie do współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej. Jednak zakres zastosowania tej decyzji ramowej jest ograniczony do przetwarzania danych osobowych przesyłanych lub udostępnianych pomiędzy państwami członkowskimi.

(7) Zapewnienie spójnego, wysokiego stopnia ochrony danych osobowych osób fizycznych oraz ułatwienie wymiany danych osobowych między właściwymi organami państw członkowskich ma zasadnicze znaczenie dla zapewnienia skutecznej współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej. W tym celu należy we wszystkich państwach członkowskich zapewnić równorzędny stopień ochrony praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w tym do celów ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom. Aby ochrona danych osobowych w Unii była skuteczna, należy wzmocnić prawa osób, których dane dotyczą, oraz obowiązki podmiotów, które przetwarzają dane osobowe, jak i odpowiadające im uprawnienia w zakresie monitorowania i egzekwowania przepisów o ochronie danych osobowych w państwach członkowskich.

(8) Artykuł 16 ust. 2 TFUE powierza Parlamentowi Europejskiemu i Radzie określenie zasad ochrony osób fizycznych w związku z przetwarzaniem danych osobowych oraz zasad swobodnego przepływu takich danych.

(9) Na tej podstawie rozporządzenie Parlamentu Europejskiego i Rady UE 2016/… ([3]) (*) ustanawia ogólne przepisy mające chronić osoby fizyczne w związku z przetwarzaniem danych osobowych oraz zapewnić swobodny przepływ danych osobowych w Unii.

(10) W deklaracji nr 21 w sprawie ochrony danych osobowych w dziedzinie współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej – załączonej do Aktu końcowego konferencji międzyrządowej, która przyjęła Traktat z Lizbony – konferencja uznała, że ze względu na szczególny charakter współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej konieczne może okazać się przyjęcie – na podstawie art. 16 TFUE – szczególnych przepisów o ochronie danych osobowych i swobodnym przepływie danych osobowych w tych dziedzinach.

(11) Należy zatem odnieść się do tych dziedzin w odrębnej dyrektywie, która stanowi szczególne przepisy o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w tym do celów ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom, 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]) 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).

([3]) Rozporządzenie (UE) 2016/… Parlamentu Europejskiego i Rady z dnia … w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylające dyrektywę 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. L …).

(*) Rozporządzenie w st 5419/16 (Dz.U. C 159 z 3.5.2016, s. 1).

zachowaniem szczególnego charakteru takich czynności. Do takich właściwych organów mogą należeć nie tylko organy publiczne – takie jak organy sądowe, policja lub inne organy ścigania – ale też wszelkie inne organy lub podmioty, którym prawo państwa członkowskiego powierza sprawowanie władzy publicznej i wykonywanie uprawnień publicznych do celów niniejszej dyrektywy. Jeżeli taki organ lub podmiot przetwarza dane osobowe do celów innych niż cele niniejszej dyrektywy, zastosowanie ma rozporządzenie (UE) 2016/… (*). Rozporządzenie (UE) 2016/… (*) ma zatem zastosowanie wtedy, gdy organ lub podmiot zbiera dane osobowe do innych celów, a następnie dalej te dane przetwarza w celu realizacji obowiązku prawnego, któremu podlega. Przykładowo do celów postępowania przygotowawczego, wykrywania lub ścigania czynów zabronionych określone instytucje finansowe zatrzymują przetwarzane przez siebie dane osobowe i udostępniają takie dane osobowe tylko właściwym organom krajowym w konkretnych sytuacjach i w zgodzie z prawem państwa członkowskiego. Organ lub podmiot, który w imieniu takich organów przetwarza dane osobowe w ramach niniejszej dyrektywy, powinien podlegać umowie lub innemu aktowi prawnemu oraz przepisom mającym zgodnie z niniejszą dyrektywą zastosowanie do podmiotu przetwarzającego, podczas gdy w odniesieniu do przetwarzania danych osobowych przez podmiot przetwarzający spoza zakresu niniejszej dyrektywy zastosowanie rozporządzenia (UE) 2016/… (*) pozostaje niezmienione.

(12) Czynności policji lub innych organów ścigania koncentrują się na zapobieganiu przestępczości, prowadzeniu postępowań przygotowawczych, wykrywaniu i ściganiu czynów zabronionych, wraz z czynnościami policji podejmowanymi, gdy nie wiadomo, czy dane zdarzenie jest czynem zabronionym. Czynności te mogą też polegać na sprawowaniu władzy poprzez stosowanie środków przymusu takich jak czynności policji podczas demonstracji, dużych imprez sportowych czy zamieszek. Czynności te obejmują również utrzymywanie prawa i porządku jako zadanie powierzone policji lub innym organom ścigania, gdy jest to konieczne do ochrony przed zagrożeniami dla bezpieczeństwa publicznego i dla prawnie chronionych podstawowych interesów społecznych i do zapobiegania takim zagrożeniom, które mogą prowadzić do popełnienia czynu zabronionego. Państwa członkowskie mogą powierzyć właściwym organom inne zadania, które niekoniecznie służą zapobieganiu przestępczości, prowadzeniu postępowań przygotowawczych, wykrywaniu i ściganiu czynów zabronionych, w tym ochronie przed zagrożeniami dla bezpieczeństwa publicznego i zapobieganiu takim zagrożeniom, tak by przetwarzanie danych osobowych w związku z tymi innymi zadaniami – o ile mieści się w zakresie prawa Unii – wchodziło w zakres rozporządzenia (UE) 2016/… (*).

(13) Czyn zabroniony w rozumieniu niniejszej dyrektywy powinien być autonomicznym pojęciem prawa unijnego, zgodnie z wykładnią Trybunału Sprawiedliwości Unii Europejskiej (zwanego dalej „Trybunałem Sprawiedliwości").

(14) Niniejsza dyrektywa nie powinna mieć zastosowania do przetwarzania danych osobowych w toku działalności wykraczającej poza zakres prawa Unii, dlatego czynności w zakresie bezpieczeństwa narodowego, czynności agencji lub jednostek zajmujących się bezpieczeństwem narodowym ani przetwarzania danych osobowych przez państwa członkowskie podczas czynności, które wchodzą w zakres zastosowania tytułu V rozdział 2 Traktatu o Unii Europejskiej (TUE), nie należy uznawać za czynności wchodzące w zakres niniejszej dyrektywy.

(15) Aby zapewnić jednakowy stopień ochrony osób fizycznych poprzez prawnie wykonalne prawa obowiązujące w całej Unii oraz aby zapobiec różnicom utrudniającym wymianę danych osobowych między właściwymi organami, niniejsza dyrektywa powinna przewidywać zharmonizowane zasady ochrony i swobodnego przepływu danych osobowych przetwarzanych do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w tym do celów ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom. Zbliżenie przepisów państw członkowskich nie powinno skutkować osłabieniem gwarantowanej przez nie ochrony danych osobowych, a wręcz przeciwnie – powinno służyć zapewnieniu wysokiego stopnia ochrony w całej Unii. Państwa członkowskie powinny także móc ustanawiać gwarancje wyższe od przewidzianych w niniejszej dyrektywie dla ochrony praw i wolności osoby, której dane dotyczą, w związku z przetwarzaniem danych osobowych przez właściwe organy.

(16) Niniejsza dyrektywa nie narusza zasady publicznego dostępu do dokumentów urzędowych. W myśl rozporządzenia (UE) 2016/… (*) dane osobowe zawarte w dokumentach urzędowych, które posiada organ lub podmiot publiczny lub prywatny w celu wykonania zadania realizowanego w interesie publicznym, mogą zostać przez ten organ lub podmiot ujawnione zgodnie z prawem Unii lub prawem państwa członkowskiego, któremu podlegają ten organ lub podmiot, dla pogodzenia publicznego dostępu do dokumentów urzędowych z prawem do ochrony danych osobowych.

(17) Ochrona przyznana niniejszą dyrektywą powinna być stosowana do osób fizycznych, bez względu na obywatelstwo czy miejsca zamieszkania, w związku z przetwarzaniem ich danych osobowych.

(*) Rozporządzenie w st 5419/16.

(18) W celu zapobieżenia wystąpieniu poważnego ryzyka obchodzenia prawa, ochrona osób fizycznych powinna być technologiczne neutralna i nie powinna zależeć od stosowanych technik. Ochrona osób fizycznych powinna mieć zastosowanie do zautomatyzowanego przetwarzania danych osobowych oraz do przetwarzania ręcznego, jeżeli dane osobowe znajdują się lub mają się znaleźć w zbiorze danych. Zbiory lub zestawy zbiorów, jak i ich strony tytułowe, które nie są uporządkowane według określonych kryteriów, nie powinny wchodzić w zakres stosowania niniejszej dyrektywy.

(19) Do przetwarzania danych osobowych przez instytucje, organy i jednostki organizacyjne Unii ma zastosowanie rozporządzenie (WE) nr 45/2001 ([1]) Parlamentu Europejskiego i Rady. Rozporządzenie (WE) nr 45/2001 oraz inne unijne akty prawne mające zastosowanie do takiego przetwarzania danych osobowych należy dostosować do zasad i przepisów przyjętych w rozporządzeniu (UE) 2016/… (*).

(20) Niniejsza dyrektywa nie powinna stanowić dla państw członkowskich przeszkody w określaniu – w krajowym prawie karnym procesowym – operacji i procedur przetwarzania danych osobowych przez sądy i inne organy wymiaru sprawiedliwości, zwłaszcza danych osobowych ujmowanych w orzeczeniach sądowych lub aktach związanych z postępowaniem karnym.

(21) Zasady ochrony danych powinny mieć zastosowanie do wszelkich informacji o zidentyfikowanych lub możliwych do zidentyfikowania osobach fizycznych. Aby stwierdzić, czy daną osobę fizyczną można zidentyfikować, należy wziąć pod uwagę wszelkie sposoby, takie jak wyodrębnienie, w stosunku do których istnieje uzasadnione prawdopodobieństwo, iż zostaną wykorzystane przez administratora lub inną osobę w celu bezpośredniego lub pośredniego zidentyfikowania osoby fizycznej. Aby stwierdzić, czy dany sposób może być z uzasadnionym prawdopodobieństwem wykorzystany do zidentyfikowania danej osoby fizycznej, należy wziąć pod uwagę wszelkie obiektywne czynniki, takie jak koszt i czas potrzebne do jej zidentyfikowania, oraz uwzględnić technologię dostępną w momencie przetwarzania danych i postęp technologiczny. Zasady ochrony danych nie powinny więc mieć zastosowania do informacji anonimowych, mianowicie do informacji, które nie wiążą się ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną, ani do danych osobowych zanonimizowanych w taki sposób, że osoby, której dane osobowe dotyczą, nie można już zidentyfikować.

(22) Organy publiczne, którym ujawnia się dane osobowe w związku z ich prawnym obowiązkiem sprawowania funkcji publicznej, takich jak organy podatkowe, organy celne, jednostki analityki finansowej, niezależne organy administracyjne czy organy rynków finansowych regulujące i nadzorujące rynki papierów wartościowych, nie powinny być traktowane jako odbiorcy, jeżeli otrzymane przez nie dane osobowe są im niezbędne do przeprowadzenia określonych czynności w interesie ogólnym zgodnie z prawem Unii lub prawem państwa członkowskiego. Żądanie o ujawnienie danych, z którym występują takie organy publiczne, powinno zawsze mieć formę pisemną, posiadać uzasadnienie, mieć charakter wyjątkowy i nie powinien dotyczyć całego zbioru danych ani prowadzić do połączenia zbiorów danych. Przetwarzając dane osobowe, takie organy publiczne powinny przestrzegać mających zastosowanie przepisów o ochronie danych, zgodnie z celami przetwarzania.

(23) Dane genetyczne należy zdefiniować jako dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby fizycznej i wynikające z analizy próbki biologicznej danej osoby, a w szczególności z analizy chromosomów, kwasu dezoksyrybonukleinowego (DNA) lub kwasu rybonukleinowego (RNA) lub z analizy wszelkich innych materiałów umożliwiających pozyskanie równoważnych informacji. Biorąc pod uwagę złożoność i wrażliwość informacji genetycznych, istnieje wysokie ryzyko niewłaściwego i ponownego ich wykorzystania do nieuprawnionych celów przez administratora. Wszelka dyskryminacja oparta na danych genetycznych powinna być co do zasady zakazana.

(24) Do danych osobowych dotyczących zdrowia należy zaliczyć wszelkie dane o stanie zdrowia osoby, której dane dotyczą, ujawniające informacje o przeszłym, obecnym lub przyszłym stanie zdrowia fizycznego lub psychicznego osoby, której dane dotyczą. Do danych tych należą informacje o osobie fizycznej zebrane podczas jej rejestracji na potrzeby usług opieki zdrowotnej lub podczas świadczenia usług opieki zdrowotnej takiej osobie, jak to określa dyrektywa 2011/24/UE Parlamentu Europejskiego i Rady ([2]); numer, symbol lub oznaczenie przypisane danej osobie fizycznej w celu zidentyfikowania tej osoby fizycznej do celów zdrowotnych; informacje pochodzące

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

(*) Rozporządzenie w st 5419/16.

([2]) Dyrektywa Parlamentu Europejskiego i Rady 2011/24/UE z dnia 9 marca 2011 r. w sprawie stosowania praw pacjentów w transgranicznej opiece zdrowotnej (Dz.U. L 88 z 4.4.2011, s. 45).

z laboratoryjnych lub lekarskich badań części ciała lub płynów ustrojowych, w tym danych genetycznych i próbek biologicznych; oraz wszelkie inne informacje, przykładowo, o chorobie, niepełnosprawności, ryzyku choroby, historii medycznej, leczeniu szpitalnym lub o stanie fizjologicznym lub biomedycznym osoby, której dane dotyczą, niezależnie od ich źródła, którym może być na przykład lekarz lub inny pracownik służby zdrowia, szpital, urządzenie medyczne lub badanie diagnostyczne in vitro.

(25) Wszystkie państwa członkowskie należą do Międzynarodowej Organizacji Policji Kryminalnej (Interpol). Aby wypełnić swoją misję, Interpol otrzymuje, przechowuje i przekazuje dane osobowe w celu wspierania właściwych organów w zapobieganiu i zwalczaniu przestępczości międzynarodowej. W związku z tym należy wzmocnić współpracę między Unią a Interpolem poprzez promowanie sprawnej wymiany danych osobowych, jednocześnie zapewniając poszanowanie podstawowych praw i wolności w przypadku automatycznego przetwarzania danych osobowych. Gdy dane osobowe są przekazywane przez Unię Interpolowi oraz państwom, które oddelegowały swoich przedstawicieli do Interpolu, zastosowanie powinna mieć niniejsza dyrektywa, w szczególności przepisy o międzynarodowym przekazywaniu danych. Niniejsza dyrektywa nie powinna wpływać na stosowanie przepisów szczegółowych określonych we wspólnym stanowisku Rady 2005/69/WSiSW ([1]) oraz w decyzji Rady 2007/533/WSiSW ([2]).

(26) Wszelkie przetwarzanie danych osobowych musi być zgodne z prawem, rzetelne i przejrzyste względem zainteresowanej osoby fizycznej oraz służyć wyłącznie konkretnym celom określonym prawem. Nie stanowi to dla organów ścigania przeszkody w prowadzeniu czynności takich jak nadzór niejawny lub monitoring wizyjny. Czynności takie można prowadzić do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w tym do celów ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom, jeżeli czynności te są określone prawem i stanowią środek niezbędny i proporcjonalny w społeczeństwie demokratycznym, z należytym uwzględnieniem uzasadnionych interesów danej osoby fizycznej. Zasada rzetelnego przetwarzania obowiązująca w ochronie danych jest pojęciem odrębnym względem prawa do rzetelnego procesu, które jest zdefiniowane w art. 47 Karty i w art. 6 europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności (zwanej dalej „EKPC"). Osobom fizycznym należy uświadomić ryzyko, zasady, zabezpieczenia i prawa związane z przetwarzaniem ich danych osobowych oraz sposoby wykonywania praw przysługujących im w związku z takim przetwarzaniem. Wyraźne, uzasadnione i określone w momencie zbierania danych osobowych powinny być w szczególności konkretne cele ich przetwarzania. Dane osobowe powinny być adekwatne i właściwe w stosunku do celów przetwarzania. Należy w szczególności zapewnić, by zebrane dane osobowe nie były nadmierne i by okres ich przechowywania był nie dłuższy, niż jest to niezbędne do osiągnięcia celu ich przetwarzania. Dane osobowe powinny być przetwarzane tylko wtedy, gdy celu przetwarzania nie można rozsądnie osiągnąć innymi sposobami. Aby zapobiec przechowywaniu danych przez okres dłuższy, niż jest to niezbędne, administrator powinien ustalić termin ich usuwania lub okresowego przeglądu. Państwa członkowskie powinny ustanowić odpowiednie zabezpieczenia dla danych osobowych przechowywanych dłużej w celu archiwizacji w interesie publicznym, wykorzystania do celów naukowych, statystycznych lub historycznych.

(27) Zapobieganie przestępczości, prowadzenie postępowań przygotowawczych, wykrywanie i ściganie czynów zabronionych wymaga, aby właściwe organy przetwarzały dane osobowe – zebrane w kontekście zapobiegania konkretnym czynom zabronionym, prowadzenia postępowań przygotowawczych w ich sprawie, wykrywania ich lub ścigania – w kontekście szerszym, dla lepszego zrozumienia działalności przestępczej oraz ustalenia powiązań pomiędzy różnymi wykrytymi czynami zabronionymi.

(28) Aby zapewnić bezpieczeństwo w stosunku do przetwarzania i zapobiegać przetwarzaniu z naruszeniem niniejszej dyrektywy, dane osobowe należy przetwarzać tak, by zapewnić odpowiedni stopień bezpieczeństwa i poufności, w tym chronić przed nieuprawnionym dostępem do takich danych i do sprzętu służącego ich przetwarzaniu lub przed nieuprawnionym korzystaniem z takich danych i sprzętu, z uwzględnieniem stanu wiedzy technicznej w odnośnej dziedzinie, technologii i kosztów wdrożenia w stosunku do ryzyka naruszenia i charakteru danych osobowych wymagających ochrony.

(29) Dane osobowe należy zbierać w konkretnych, wyraźnych i prawnie uzasadnionych celach mieszczących się w zakresie zastosowania niniejszej dyrektywy i nie należy ich przetwarzać w celach niezgodnych z zapobieganiem przestępczości, prowadzeniem postępowań przygotowawczych, wykrywaniem i ściganiem czynów zabronionych i wykonywaniem kar, w tym z ochroną przed zagrożeniami dla bezpieczeństwa publicznego i zapobieganiem takim zagrożeniom. Jeżeli dane osobowe przetwarza ten sam lub inny administrator w celu wchodzącym w zakres stosowania niniejszej dyrektywy, ale innym niż cel, w którym dane zostały zebrane, przetwarzanie takie powinno być dopuszczalne, pod warunkiem że przetwarzanie jest dozwolone na mocy mających zastosowanie przepisów prawa oraz jest niezbędne i proporcjonalne do tego innego celu.

([1]) Wspólne stanowisko Rady 2005/69/WSiSW z dnia 24 stycznia 2005 r. w sprawie wymiany niektórych danych z Interpolem (Dz.U. L 27 z 29.1.2005, s. 61).

([2]) Decyzji Rady 2007/533/WSiSW z dnia 12 czerwca 2007 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II) (Dz.U. L 205 z 7.8.2007, s. 63).

(30) Zasadę prawidłowości danych należy stosować z uwzględnieniem charakteru i celu odnośnego przetwarzania. W szczególności w postępowaniu sądowym oświadczenia zawierające dane osobowe opierają się na subiektywnym osądzie osób fizycznych i nie zawsze są weryfikowalne. Dlatego wymóg prawidłowości danych nie powinien odnosić się do prawidłowości oświadczenia, lecz jedynie do faktu, że konkretne oświadczenie zostało złożone.

(31) Nieodłączną cechą przetwarzania danych osobowych w obszarze współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej jest to, że przetwarzane są dane osobowe dotyczące różnych kategorii osób, których dane dotyczą. W stosownych przypadkach należy zatem w jak największym stopniu wyraźnie rozróżniać dane osobowe różnych kategorii osób, których dane dotyczą, takich jak osoby podejrzane, osoby skazane za czyn zabroniony, ofiary i inne osoby, np. świadkowie, osoby posiadające istotne informacje lub kontakty oraz wspólnicy osób podejrzanych i skazanych przestępców. Nie powinno to uniemożliwiać stosowania – zgodnie z wykładnią przedstawioną odpowiednio w orzecznictwie Trybunału Sprawiedliwości i Europejskiego Trybunału Praw Człowieka – zasady domniemania niewinności zagwarantowanej w Karcie oraz w EKPC.

(32) Właściwe organy powinny zapewnić, by nieprawidłowe, niekompletne lub nieaktualne dane osobowe nie były przesyłane ani udostępniane. Aby zapewnić ochronę osób fizycznych, prawidłowość, kompletność i stopień aktualności danych oraz wiarygodność przesyłanych lub udostępnianych danych osobowych, właściwe organy powinny w miarę możliwości opatrywać wszelkie przesyłane dane osobowe niezbędnymi informacjami.

(33) Jeżeli w niniejszej dyrektywie jest mowa o prawie państwa członkowskiego, podstawie prawnej lub akcie prawnym, niekoniecznie wymaga to przyjęcia aktu prawnego przez parlament, z zastrzeżeniem wymogów wynikających z porządku konstytucyjnego danego państwa członkowskiego. Takie prawo państwa członkowskiego, podstawa prawna lub akt prawny powinny jednakże być jasne i precyzyjne, a ich zastosowanie przewidywalne dla osób im podlegających – jak wymaga tego orzecznictwo Trybunału Sprawiedliwości i Europejskiego Trybunału Praw Człowieka. Prawo państwa członkowskiego regulujące przetwarzanie danych osobowych w ramach zakresu zastosowania niniejszej dyrektywy powinno co najmniej określać cele ogólne, dane osobowe mające podlegać przetwarzaniu, cele przetwarzania oraz procedury pozwalające chronić integralność i poufność danych osobowych oraz procedury niszczenia tych danych, a tym samym powinno zapewniać dostateczną ochronę przed ryzykiem nadużyć i arbitralności.

(34) Przetwarzanie danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w tym do celów ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom powinno obejmować każdą operację lub każdy zestaw operacji, które wykonuje się do wspomnianych celów na danych osobowych lub na ich zestawach w sposób zautomatyzowany lub niezautomatyzowany, takie jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, dopasowywanie lub łączenie, ograniczanie przetwarzania, usuwanie lub niszczenie. W szczególności przepisy niniejszej dyrektywy powinny mieć zastosowanie do przesyłania danych osobowych, które służy celom określonym w niniejszej dyrektywie, odbiorcom niepodlegającym niniejszej dyrektywie. Odbiorca taki powinien oznaczać osobę fizyczną lub prawną, organ publiczny, jednostkę organizacyjną lub inny podmiot, któremu właściwy organ ujawnia te dane zgodnie z prawem. Jeżeli właściwy organ pierwotnie zebrał dane osobowe do jednego z celów określonych w niniejszej dyrektywie, to do przetwarzania tych danych do celów innych niż określone w niniejszej dyrektywie – jeżeli przetwarzanie to jest dozwolone przez prawo Unii lub prawo państwa członkowskiego – powinno mieć zastosowanie rozporządzenie (UE) 2016/… (*). W szczególności przepisy rozporządzenia (UE) 2016/… (*) powinny mieć zastosowanie do przesyłania danych osobowych do celów niewchodzących z zakres stosowania niniejszej dyrektywy. Do przetwarzania danych osobowych przez odbiorcę, który nie jest właściwym organem lub nie występuje w charakterze właściwego organu w rozumieniu niniejszej dyrektywy i któremu właściwy organ ujawnia dane osobowe zgodnie z prawem, zastosowanie powinno mieć rozporządzenie (UE) 2016/… (*). Przy wdrażaniu niniejszej dyrektywy państwa członkowskie powinny też mieć możliwość dalszego doprecyzowania zastosowania przepisów rozporządzenia (UE) 2016/… (*), na warunkach w nim określonych.

(35) Aby przetwarzanie danych osobowych w ramach niniejszej dyrektywy było zgodne z prawem, powinno ono być niezbędne do wykonania zadań realizowanych przez właściwy organ w interesie publicznym na podstawie prawa

(*) Rozporządzenie w st 5419/16.

Unii lub prawa państwa członkowskiego do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w tym do celów ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom. Działania takie powinny obejmować ochronę żywotnych interesów osoby, której dane dotyczą. Wykonywanie zadań polegających na zapobieganiu przestępczości, prowadzeniu postępowań przygotowawczych, wykrywaniu i ściganiu czynów zabronionych, instytucjonalnie powierzonych na mocy prawa właściwym organom, pozwala tym organom wymagać lub nakazywać, aby osoby fizyczne zastosowały się do stawianych żądań. W takim przypadku zgoda osoby, której dane dotyczą, określona w rozporządzeniu (UE) 2016/… (*), nie powinna stanowić podstawy prawnej przetwarzania danych osobowych przez właściwe organy. Jeżeli osoba, której dane dotyczą, musi wywiązać się z obowiązku prawnego, nie ma ona faktycznego, swobodnego wyboru, a tym samym nie można uznać, iż jej reakcja jest swobodnym wyrazem jej woli. Nie powinno to stanowić dla państw członkowskich przeszkody w ustanowieniu z mocy prawa, że osoba, której dane dotyczą, może wyrazić zgodę na przetwarzanie jej danych osobowych do celów określonych w niniejszej dyrektywie, takich jak badania DNA w postępowaniu przygotowawczym czy monitorowanie miejsca jej pobytu za pomocą aparatury elektronicznej na potrzeby wykonania kary.

(36) Państwa członkowskie powinny zapewnić, aby ilekroć prawo Unii lub prawo państwa członkowskiego mające zastosowanie do właściwego organu przesyłającego stawia w określonych sytuacjach szczególne wymogi co do przetwarzania danych osobowych, takie jak stosowanie kodeksów postępowania, właściwy organ przesyłający informował o takich wymogach i o obowiązku ich przestrzegania odbiorcę danych osobowych. Wymogi takie mogą przykładowo obejmować zakaz przesyłania danych osobowych innym odbiorcom lub wykorzystywania ich do innych celów niż cele, dla których przesłano je odbiorcy, lub udzielenia informacji osobie, której dane dotyczą, w przypadku ograniczenia prawa do informacji bez uprzedniej zgody właściwego organu przesyłającego. Obowiązki takie powinny także dotyczyć przekazywania danych przez właściwy organ przesyłający odbiorcom w państwach trzecich lub organizacjach międzynarodowych. Państwa członkowskie powinny zapewnić, by właściwy organ przesyłający nie stosował względem odbiorców w innych państwach członkowskich ani w organach i jednostkach organizacyjnych ustanowionych na mocy tytułu V rozdział 4 i 5 TFUE wymogów innych niż mające zastosowanie do podobnego przesyłania danych w obrębie państwa członkowskiego właściwego organu.

(37) Dane osobowe, które z racji swego charakteru są szczególnie wrażliwe w świetle podstawowych praw i wolności, wymagają szczególnej ochrony, gdyż kontekst ich przetwarzania może powodować poważne ryzyko naruszenia podstawowych praw i wolności. Do takich danych osobowych powinny zaliczać się dane osobowe ujawniające pochodzenie rasowe lub etniczne, przy czym użycie w niniejszej dyrektywie terminu „pochodzenie rasowe" nie oznacza, że Unia akceptuje teorie sugerujące istnienie osobnych ras ludzkich. Takich danych nie należy przetwarzać, chyba że przetwarzanie podlega odpowiednim, określonym prawem gwarancjom praw i wolności osoby, której dane dotyczą, i jest dozwolone w przypadkach dopuszczonych prawem, a jeżeli nie jest dotąd dopuszczone takim prawem – jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby, albo też dotyczy danych ewidentnie upublicznionych przez samą osobę, której dane dotyczą. Odpowiednie zabezpieczenia praw i wolności osoby, której dane dotyczą, mogą obejmować możliwość zbierania takich danych tylko w połączeniu z innymi danymi dotyczącymi danej osoby fizycznej, możliwość odpowiedniego zabezpieczenia takich danych, ściślejsze uregulowanie dostępu pracowników właściwego organu do danych lub zakaz przesyłania danych. Przetwarzanie takich danych powinno być także dozwolone prawem, gdy osoba, której dane dotyczą, udzieliła wyraźnej zgody na szczególnie dla niej inwazyjne przetwarzanie. Niemniej sama zgoda osoby, której dane dotyczą, nie powinna stanowić podstawy prawnej przetwarzania takich wrażliwych danych osobowych przez właściwe organy.

(38) Osoba, której dane dotyczą, powinna mieć prawo do tego, by nie stosowano względem niej decyzji analizującej jej cechy osobiste, opierającej się wyłącznie na przetwarzaniu automatycznym, która ma niekorzystne skutki prawne dla takiej osoby lub poważnie na nią wpływa. Przetwarzanie takie powinno zawsze podlegać odpowiednim zabezpieczeniom, wraz z konkretną informacją dla osoby, której dane dotyczą, i prawem do uzyskania interwencji ludzkiej, a zwłaszcza prawem do wyrażenia własnego stanowiska, uzyskania wyjaśnienia decyzji wydanej wskutek takiej analizy lub zaskarżenia tej decyzji. Profilowanie skutkujące dyskryminacją osób fizycznych na podstawie danych osobowych, które z racji swego charakteru są szczególnie wrażliwe w świetle podstawowych praw i wolności, jest zakazane na warunkach określonych w art. 21 i 52 Karty.

(39) Aby osoba, której dane dotyczą, mogła wykonywać swoje prawa, wszelkie kierowane do niej informacje powinny być łatwo dostępne, także na stronie internetowej administratora, i zrozumiałe, przy użyciu jasnego i prostego języka. Informacje takie powinny być dostosowane do potrzeb osób wymagających szczególnej opieki, np. dzieci.

(*) Rozporządzenie w st 5419/16.

(40) Należy wprowadzić ułatwienia pozwalające osobie, której dane dotyczą, na wykonywanie praw wynikających z przepisów przyjętych na podstawie niniejszej dyrektywy, w tym mechanizmy żądania – i w stosownych przypadkach bezpłatnego uzyskiwania – w szczególności dostępu do danych osobowych i ich sprostowania lub usunięcia oraz ograniczenia ich przetwarzania. Administrator powinien mieć obowiązek odpowiadania na żądania osoby, której dane dotyczą, bez zbędnej zwłoki, chyba że stosuje ograniczenia praw osoby, której dane dotyczą, zgodnie z niniejszą dyrektywą. Ponadto, jeżeli żądania są w sposób oczywisty nieuzasadnione lub nadmierne – tak jak wtedy, gdy osoba, której dane dotyczą, nieracjonalnie i ustawicznie żąda informacji lub gdy nadużywa przysługującego jej prawa do informacji, przykładowo podając fałszywe lub mylne dane przy występowaniu z żądaniem – administrator powinien mieć możliwość pobrania rozsądnej opłaty lub odmowy podjęcia działań w stosunku do tego żądania.

(41) W przypadku gdy administrator żąda dodatkowych informacji, aby potwierdzić tożsamość osoby, której dane dotyczą, informacje te powinny być przetwarzane wyłącznie w tym konkretnym celu i nie powinny być przechowywane dłużej niż to konieczne dla realizacji tego celu.

(42) Osobie, której dane dotyczą, należy udostępnić następujące informacje: tożsamość administratora, prowadzenie operacji przetwarzania, cele przetwarzania oraz prawo do wniesienia skargi, istnienie prawa do zażądania od administratora dostępu do danych, sprostowania lub usunięcia danych osobowych lub ograniczenia ich przetwarzania. Można to uczynić na stronie internetowej właściwego organu. Ponadto w konkretnych przypadkach i w celu zapewnienia osobie, której dane dotyczą, możliwości wykonywania jej praw, osoba ta powinna być informowana o podstawie prawnej przetwarzania oraz o okresie przechowywania danych, o ile udzielenie takich informacji jest konieczne z uwzględnieniem konkretnych okolicznościach przetwarzania danych, dla zagwarantowania rzetelnego przetwarzania danych tej osoby.

(43) Każda osoba fizyczna powinna mieć prawo dostępu do zebranych danych jej dotyczących oraz powinna mieć możliwość łatwego wykonywania tego prawa w rozsądnych odstępach czasu, by mieć świadomość przetwarzania danych i móc zweryfikować jego zgodność z prawem. Dlatego każda osoba, której dane dotyczą, powinna mieć prawo do poznania i uzyskania informacji na temat celów przetwarzania danych, okresu ich przetwarzania oraz odbiorców danych, także w państwach trzecich. Jeśli takie informacje obejmują informacje o pochodzeniu danych osobowych, nie powinny one ujawniać tożsamości osób fizycznych, w szczególności poufnych źródeł informacji. Dla realizacji tego prawa wystarczy przekazać osobie, której dane dotyczą, pełne podsumowanie tych danych w zrozumiałej formie, czyli w formie pozwalającej jej poznać te dane, sprawdzić ich prawidłowość oraz zweryfikować zgodność ich przetwarzania z niniejszą dyrektywą, tak by mogła ona wykonywać prawa przysługujące jej na mocy niniejszej dyrektywy. Takie podsumowanie może mieć formę kopii przetwarzanych danych osobowych.

(44) Państwa członkowskie powinny mieć możliwość przyjmowania aktów prawnych pozwalających opóźnić, ograniczyć lub pominąć informowanie osób, których dane dotyczą, lub ograniczyć, w całości lub w części, dostęp tych osób do ich własnych danych osobowych w takim zakresie i przez taki czas, w jakim odnośny środek jest działaniem niezbędnym i proporcjonalnym w społeczeństwie demokratycznym – przy należytym uwzględnieniu praw podstawowych i uzasadnionych interesów danej osoby fizycznej – tak aby uniemożliwić zakłócanie czynności postępowań urzędowych lub sądowych, postępowań przygotowawczych lub czynności procesowych, aby uniemożliwić zakłócanie zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, aby chronić bezpieczeństwo publiczne lub narodowe lub aby chronić prawa i wolności innych osób. Administrator powinien dokonywać oceny – badając konkretnie i indywidualnie każdy przypadek – czy prawo dostępu powinno zostać częściowo lub całkowicie ograniczone.

(45) Co do zasady o każdej odmowie lub każdym ograniczeniu dostępu należy powiadomić pisemnie osobę, której dane dotyczą, z podaniem faktycznych lub prawnych podstaw decyzji.

(46) Każde ograniczenie praw osoby, której dane dotyczą, musi być zgodne z Kartą i EKPC, w myśl wykładni zawartej, odpowiednio, w orzecznictwie Trybunału Sprawiedliwości i Europejskiego Trybunału Praw Człowieka, a zwłaszcza musi odbywać się z poszanowaniem istoty tych praw i wolności.

(47) Każda osoba fizyczna powinna mieć prawo do uzyskania sprostowania dotyczących jej nieprawidłowych danych osobowych, zwłaszcza danych dotyczących faktów, oraz prawo do usunięcia danych, jeżeli przetwarzanie takich danych narusza niniejszą dyrektywę. Niemniej prawo do sprostowania danych nie powinno dotyczyć, na przykład,

treści zeznania świadka. Każda osoba fizyczna powinna mieć również prawo do ograniczenia przetwarzania danych osobowych, gdy kwestionuje ona ich prawidłowość, której nie da się potwierdzić, lub gdy dane osobowe muszą zostać zachowane do celów dowodowych. W szczególności należy ograniczyć przetwarzanie danych osobowych zamiast ich usuwania, jeżeli w konkretnym przypadku uzasadnione przesłanki sugerują, że usunięcie mogłoby wpłynąć na uprawnione interesy osoby, której dane dotyczą. W takim przypadku ograniczone dane należy przetwarzać tylko w celu, który zapobiegł ich usunięciu. Metody ograniczonego przetwarzania danych osobowych obejmują między innymi przeniesienie wybranych danych do innego systemu przetwarzania – np. do celów archiwizacyjnych – lub uniemożliwienie użytkownikom dostępu do wybranych danych. W zautomatyzowanych zbiorach danych ograniczenie przetwarzania danych osobowych należy zasadniczo zapewnić środkami technicznymi. Fakt ograniczenia przetwarzania danych osobowych należy zaznaczyć w systemie w sposób jasno wskazujący, że przetwarzanie tych danych jest ograniczone. O takim sprostowaniu lub usunięciu danych osobowych lub ograniczeniu ich przetwarzania należy poinformować odbiorców, którym dane zostały ujawnione, oraz właściwe organy, od których pochodzą nieprawidłowe dane. Administratorzy powinni również powstrzymać się od dalszego rozpowszechniania tych danych.

(48) Jeżeli administrator odmawia osobie, której dane dotyczą, prawa do informacji, dostępu lub sprostowania lub usunięcia danych osobowych lub ograniczenia ich przetwarzania, osoba, której dane dotyczą, powinna mieć prawo wystąpienia do krajowego organu nadzorczego o weryfikację zgodności przetwarzania z prawem. O prawie tym należy poinformować osobę, której dane dotyczą. Jeżeli organ nadzorczy podejmie działanie w imieniu osoby, której dane dotyczą, spoczywa na nim obowiązek poinformowania tej osoby co najmniej o fakcie przeprowadzenia wszelkich niezbędnych przeglądów lub kontroli. Organ nadzorczy powinien także poinformować osobę, której dane dotyczą, o przysługującym jej prawie do środka prawnego przed sądem.

(49) Jeżeli dane osobowe przetwarza się w toku postępowania przygotowawczego i sądowego w sprawie karnej, państwa członkowskie powinny mieć możliwość zapewnienia wykonywania prawa do informacji, dostępu lub poprawienia, usunięcia i ograniczenia przetwarzania zgodnie z krajowymi przepisami o postępowaniu sądowym.

(50) Należy nałożyć na administratora obowiązki i ustanowić odpowiedzialność prawną administratora za przetwarzanie danych osobowych przez niego samego lub w jego imieniu. W szczególności administrator powinien mieć obowiązek wdrożenia odpowiednich i skutecznych środków oraz powinien być w stanie wykazać, że czynności przetwarzania są zgodne z niniejszą dyrektywą. Środki te powinny uwzględniać charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw i wolności osób fizycznych. Środki podejmowane przez administratora powinny obejmować opracowanie i wdrożenie szczególnych zabezpieczeń w odniesieniu do postępowania z danymi osobowymi osób fizycznych wymagających szczególnej opieki, takich jak dzieci.

(51) Z przetwarzania danych może wynikać ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, której dane dotyczą, to zaś może prowadzić do uszczerbku fizycznego oraz szkód majątkowych i niemajątkowych, w szczególności: jeżeli przetwarzanie może skutkować dyskryminacją, kradzieżą lub sfałszowaniem tożsamości, stratą finansową, naruszeniem dobrego imienia, naruszeniem poufności danych chronionych tajemnicą służbową, niedozwolonym odwróceniem pseudonimizacji lub wszelką inną znaczną szkodą gospodarczą lub społeczną; jeżeli osoby, których dane dotyczą, mogą zostać pozbawione przysługujących im praw i wolności lub możliwości sprawowania kontroli nad swoimi danymi osobowymi; jeżeli przetwarzane są dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe lub przynależność do związków zawodowych; jeżeli przetwarzane są dane genetyczne lub biometryczne w celu jednoznacznego zidentyfikowania osoby lub jeżeli przetwarzane są dane dotyczące zdrowia lub dane dotyczące seksualności i orientacji seksualnej lub dane o wyrokach skazujących i czynach zabronionych lub o odnośnych środkach zabezpieczających; jeżeli oceniane są cechy osobowe, w szczególności poprzez analizowanie i prognozowanie okoliczności dotyczących efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się, w celu tworzenia lub wykorzystywania profili osobistych; jeżeli przetwarzane są dane osobowe osób fizycznych wymagających szczególnej opieki, zwłaszcza dzieci; lub jeżeli przetwarzanie dotyczy dużej ilości danych osobowych i wpływa na dużą liczbę osób, których dane dotyczą.

(52) Prawdopodobieństwo i wagę ryzyka naruszenia należy określić poprzez uwzględnienie charakteru, zakresu, kontekstu i celów przetwarzania danych. Ryzyko naruszenia należy oszacować na podstawie obiektywnej oceny, w ramach której stwierdza się, czy operacje przetwarzania danych niosą poważne zagrożenie. Wysokie ryzyko jest szczególnym ryzykiem naruszenia praw i wolności osób, których dane dotyczą.

(53) Ochrona praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych wymaga wdrożenia odpowiednich środków technicznych i organizacyjnych, by zapewnić spełnienie wymogów niniejszej dyrektywy. Wdrożenie takich środków nie powinno zależeć wyłącznie od względów gospodarczych. Aby móc wykazać przestrzeganie przepisów niniejszej dyrektywy, administrator powinien przyjąć wewnętrzne polityki i wdrożyć środki, które są zgodne w szczególności z zasadą uwzględniania ochrony danych w fazie projektowania oraz z zasadą domyślnej ochrony danych. Jeśli administrator przeprowadził ocenę skutków dla ochrony danych zgodnie z niniejszą dyrektywą, jej wyniki uwzględnia się przy opracowywaniu wspomnianych środków i procedur. Środki takie mogą polegać między innymi na stosowaniu pseudonimizacji najszybciej, jak to możliwe. Stosowanie pseudonimizacji do celów niniejszej dyrektywy może być narzędziem ułatwiającym zwłaszcza swobodny przepływ danych osobowych w obszarze wolności, bezpieczeństwa i sprawiedliwości.

(54) Ochrona praw i wolności osób, których dane dotyczą, oraz obowiązki i odpowiedzialność prawna administratorów i podmiotów przetwarzających – także w odniesieniu do monitorowania ze strony organów nadzorczych i do środków przez nie stosowanych – wymagają dokonania jasnego podziału obowiązków przyjętych w niniejszej dyrektywie, w tym w sytuacji, gdy administrator określa cele i sposoby przetwarzania wspólnie z innymi administratorami lub gdy operacji przetwarzania dokonuje się w imieniu administratora.

(55) Przetwarzanie przez podmiot przetwarzający powinno być regulowane aktem prawnym, w tym umową wiążącą podmiot przetwarzający z administratorem i przewidującą w szczególności, że podmiot przetwarzający powinien działać wyłącznie zgodnie z poleceniami administratora. Podmiot przetwarzający powinien uwzględniać zasadę ochrony danych w fazie projektowania oraz zasadę domyślnej ochrony danych.

(56) Dla zachowania zgodności z niniejszą dyrektywą administrator lub podmiot przetwarzający powinni prowadzić wykazy wszystkich kategorii czynności przetwarzania danych osobowych, za które są odpowiedzialni. Każdy administrator i każdy podmiot przetwarzający powinien mieć obowiązek współpracy z organem nadzorczym i na jego żądanie udostępniać wskazane wykazy w celu monitorowania tych operacji przetwarzania. Administrator lub podmiot przetwarzający dane osobowe w niezautomatyzowanych systemach przetwarzania powinien dysponować skutecznymi metodami, które pozwolą mu wykazać zgodność przetwarzania danych z prawem, monitorować własną działalność i zapewnić integralność i bezpieczeństwo danych, takimi jak ewidencja lub inne formy zapisu.

(57) Należy ewidencjonować przynajmniej operacje dokonywane w zautomatyzowanych systemach przetwarzania, takie jak zbieranie, modyfikowanie, przeglądanie, ujawnianie wraz z przekazywaniem, łączenie lub usuwanie danych. Należy ewidencjonować tożsamość osoby, która przeglądała lub ujawniła dane osobowe, co powinno pozwolić na ustalenie uzasadnienia operacji przetwarzania. Ewidencja powinna być używana wyłącznie do weryfikacji zgodności przetwarzania danych z prawem, do monitorowania własnej działalności, zapewniania integralności i bezpieczeństwa danych oraz do celów postępowania karnego. Monitorowanie własnej działalności powinno także obejmować wewnętrzne postępowanie dyscyplinarne przeprowadzane przez właściwe organy.

(58) Ocena skutków dla ochrony danych powinna być przeprowadzana przez administratora, jeżeli operacje przetwarzania – z racji swego charakteru, zakresu lub celów – mogą stwarzać poważne zagrożenie dla praw i wolności osób, których dane dotyczą, i powinna obejmować w szczególności przewidywane środki, gwarancje i mechanizmy mające na celu zapewnienie ochrony danych osobowych oraz wykazanie zgodności z niniejszą dyrektywą. Oceny skutków powinny dotyczyć stosownych systemów i procesów związanych z czynnościami przetwarzaniem danych osobowych, lecz nie indywidualnych przypadków.

(59) Aby zapewnić skuteczną ochronę praw i wolności osób, których dane dotyczą, administrator lub podmiot przetwarzający powinni w określonych przypadkach konsultować się z organem nadzorczym przed przetwarzaniem.

(60) W celu zachowania bezpieczeństwa i zapobiegania przetwarzaniu z naruszeniem niniejszej dyrektywy administrator lub podmiot przetwarzający powinni oszacować ryzyko właściwe dla przetwarzania oraz powinni wdrożyć środki – takie jak szyfrowanie – minimalizujące takie ryzyko. Środki takie powinny zapewnić odpowiedni stopień bezpieczeństwa i poufności, oraz uwzględniać stan wiedzy technicznej oraz koszty ich wdrożenia w stosunku do ryzyka naruszenia i charakteru danych osobowych podlegających ochronie. Oceniając ryzyko naruszenia bezpieczeństwa danych, należy wziąć pod uwagę ryzyko cechujące przetwarzanie danych – takie jak przypadkowe lub niezgodne z prawem zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony

dostęp do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych – i mogące w szczególności prowadzić do uszczerbku fizycznego oraz szkód majątkowych i niemajątkowych. Administrator i podmiot przetwarzający powinni zapewnić, by przetwarzanie danych osobowych nie było prowadzone przez osoby nieuprawnione.

(61) Przy braku odpowiedniej i szybkiej reakcji naruszenie ochrony danych osobowych może skutkować powstaniem uszczerbku fizycznego oraz szkód majątkowych i niemajątkowych u osób fizycznych, takich jak utrata kontroli nad własnymi danymi osobowymi lub ograniczenie praw, dyskryminacja, kradzież lub sfałszowanie tożsamości, strata finansowa, nieuprawnione odwrócenie pseudonimizacji, naruszenie dobrego imienia, naruszenie poufności danych osobowych chronionych tajemnicą służbową lub wszelkie inne poważne szkody gospodarcze lub społeczne dla zainteresowanej osoby fizycznej. Dlatego natychmiast po stwierdzeniu naruszenia ochrony danych osobowych administrator powinien zgłosić je organowi nadzorczemu bez zbędnej zwłoki – jeżeli to wykonalne, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – chyba że administrator jest w stanie wykazać zgodnie z zasadą rozliczalności, że jest mało prawdopodobne, by to naruszenie danych osobowych mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych. Jeżeli nie można wnieść zgłoszenia w terminie 72 godzin, powinno mu towarzyszyć wyjaśnienie przyczyn opóźnienia, a informacje mogą być przekazywane stopniowo, bez dalszej zbędnej zwłoki.

(62) Jeżeli naruszenie ochrony danych może rodzić prawdopodobieństwo wystąpienia wysokiego ryzyka naruszenia praw i wolności osób fizycznych, osoby fizyczne należy poinformować bez zbędnej zwłoki, tak by mogły podjąć niezbędne środki ostrożności. Informacja taka powinna zawierać opis charakteru naruszenia ochrony danych osobowych oraz zalecenia dla danej osoby fizycznej co do minimalizacji potencjalnych niekorzystnych skutków. Informacje należy przekazywać osobom, których dane dotyczą, tak szybko, jak jest to rozsądnie możliwe, w ścisłej współpracy z organem nadzorczym oraz zgodnie z zaleceniami przekazanymi przez ten organ lub inne właściwe organy. Przykładowo potrzeba zminimalizowania bezpośredniego ryzyka wystąpienia szkody będzie wymagać niezwłocznego poinformowania osób, których dane dotyczą, natomiast wdrożenie odpowiednich środków przeciwko takim samym lub podobnym naruszeniom ochrony danych może uzasadniać późniejsze poinformowanie. Jeżeli unikania zakłócania czynności postępowań urzędowych lub sądowych, postępowań przygotowawczych lub procedur, unikania zakłócania zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, ochrony bezpieczeństwa publicznego lub narodowego lub ochrony praw i wolności innych osób, nie można osiągnąć poprzez opóźnienie lub ograniczenie przekazania danej osobie fizycznej informacji o naruszeniu jej danych osobowych, w wyjątkowych okolicznościach można nie przekazywać takich informacji.

(63) Administrator powinien wyznaczyć osobę, która będzie pomagać mu w monitorowaniu wewnętrznego przestrzegania przepisów przyjętych na podstawie niniejszej dyrektywy, z wyjątkiem sytuacji, w której państwo członkowskie podejmie decyzję o zwolnieniu z tego obowiązku sądów i innych niezależnych organów wymiaru sprawiedliwości w toku sprawowania przez nie wymiaru sprawiedliwości. Osoba ta może być członkiem dotychczasowego personelu administratora po odbyciu specjalnego szkolenia z prawa i praktyki ochrony danych w celu uzyskania wiedzy fachowej w tej dziedzinie. Niezbędny poziom wiedzy fachowej należy ustalić zwłaszcza w świetle prowadzonych operacji przetwarzania danych oraz ochrony, której wymagają dane osobowe przetwarzane przez administratora. Swoje zadania osoba ta może wykonywać w niepełnym lub w pełnym wymiarze czasu pracy. Kilku administratorów może, uwzględniając swoją strukturę organizacyjną i wielkość, wspólnie wyznaczyć jednego inspektora ochrony danych, na przykład w przypadku dzielonych zasobów w jednostkach centralnych. Osoba ta może być również mianowana na różne stanowiska w ramach struktury poszczególnych administratorów. Osoba ta powinna pomagać administratorowi i pracownikom przetwarzającym dane osobowe, dostarczając im informacji i porad na temat przestrzegania spoczywających na nich obowiązków w zakresie ochrony danych. Inspektorzy ochrony danych powinni być w stanie wykonywać swoje obowiązki i zadania w sposób niezależny, zgodnie z prawem państwa członkowskiego.

(64) Państwa członkowskie powinny zapewnić, by dane były przekazywane do państwa trzeciego lub organizacji międzynarodowej tylko wtedy, jeżeli jest to konieczne dla zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w tym dla ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom, oraz gdy administrator w państwie trzecim lub w organizacji międzynarodowej jest organem właściwym w rozumieniu niniejszej dyrektywy. Wyłącznie organy właściwe pełniące funkcję administratora powinny dokonywać przekazania, z wyjątkiem sytuacji gdy podmiotom przetwarzającym jednoznacznie polecono dokonać przekazania w imieniu administratorów. Przekazanie takie może nastąpić w przypadkach, w których Komisja zdecydowała, że dane państwo trzecie lub organizacja międzynarodowa zapewniają odpowiedni stopień ochrony, gdy wprowadzono odpowiednie zabezpieczenia lub gdy mają zastosowanie wyjątki w konkretnych sytuacjach. Przekazując dane osobowe z Unii administratorom, podmiotom przetwarzającym lub innym odbiorcom w państwach trzecich lub organizacjom międzynarodowym, nie należy jednak obniżać stopnia ochrony osób fizycznych przewidzianego w Unii na mocy niniejszej dyrektywy, także w przypadkach dalszego przekazywania danych osobowych z państwa trzeciego lub organizacji międzynarodowej administratorom lub podmiotom przetwarzającym w tym samym lub w innym państwie trzecim lub tej samej lub innej organizacji międzynarodowej.

(65) Przekazywanie danych osobowych z któregokolwiek państwa członkowskiego do państw trzecich lub organizacji międzynarodowych powinno zasadniczo odbywać się wyłącznie za zgodą państwa członkowskiego, od którego te dane uzyskano. Jeżeli zagrożenie dla bezpieczeństwa publicznego państwa członkowskiego lub państwa trzeciego lub dla ważnych interesów państwa członkowskiego jest tak nagłe, że nie da się na czas uzyskać uprzedniej zgody, wtedy z uwagi na efektywność współpracy w zakresie ścigania właściwy organ powinien móc przekazać odnośne dane osobowe do danego państwa trzeciego lub danej organizacji międzynarodowej bez takiej uprzedniej zgody. Państwa członkowskie powinny przyjąć, że należy informować państwa trzecie lub organizacje międzynarodowe o wszelkich specjalnych wymogach dotyczących przekazania. Dalsze przekazanie danych osobowych powinno podlegać uprzedniej zgodzie właściwego organu, który dokonał pierwotnego przekazania. Podejmując decyzję w sprawie wniosku o zgodę na dalsze przekazanie danych, właściwy organ, który dokonał pierwotnego przekazania, powinien odpowiednio uwzględnić wszelkie istotne czynniki, w tym wagę czynu zabronionego, szczególne warunki pierwotnego przekazania danych oraz cel tego przekazania, rodzaj i warunki wykonania kary oraz stopień ochrony danych osobowych w państwie trzecim lub organizacji międzynarodowej, którym dane osobowe są dalej przekazywane. Właściwy organ, który dokonał pierwotnego przekazania, powinien także mieć możliwość uzależnienia dalszego przekazania od spełnienia szczególnych warunków. Warunki te mogą zostać opisane na przykład w kodeksach postępowania.

(66) Komisja powinna mieć możliwość stwierdzenia ze skutkiem dla całej Unii, że niektóre państwa trzecie, lub terytorium lub co najmniej jeden określony sektor w państwie trzecim, lub organizacja międzynarodowa, zapewniają odpowiedni stopień ochrony danych, gwarantując tym samym pewność i jednolitość prawną w całej Unii w odniesieniu do państw trzecich lub organizacji międzynarodowych, które zostały uznane za zapewniające taki stopień ochrony. W takich przypadkach powinna istnieć możliwość przekazania danych osobowych do tych państw bez konieczności uzyskania specjalnego zezwolenia, z wyjątkiem sytuacji, gdy inne państwo członkowskie, od którego uzyskano dane, musi wydać zgodę na ich przekazanie.

(67) Zgodnie z podstawowymi wartościami, na których opiera się Unia, w szczególności z ochroną praw człowieka, w swojej ocenie państwa trzeciego lub terytorium lub określonego sektora w państwie trzecim Komisja powinna wziąć pod uwagę sposób, w jaki dane państwo trzecie przestrzega praworządności, dostępu do wymiaru sprawiedliwości oraz międzynarodowych norm i standardów ochrony praw człowieka, jego prawo ogólne i sektorowe, w tym ustawodawstwo dotyczące bezpieczeństwa publicznego, obrony, bezpieczeństwa narodowego i porządku publicznego, a także w dziedzinie prawa karnego. Przy przyjmowaniu decyzji stwierdzających odpowiedni stopień ochrony w odniesieniu do terytorium lub w określonym sektorze w państwie trzecim jest odpowiedni, należy wziąć pod uwagę jasne i obiektywne kryteria, takie jak konkretne czynności przetwarzania, zakres mających zastosowanie standardów prawnych i ustawodawstwo obowiązujące w danym państwie trzecim. Państwo trzecie powinno dawać gwarancje zapewniające odpowiedni stopień ochrony, zasadniczo odpowiadający stopniowi przewidzianemu w Unii, w szczególności gdy dane są przetwarzane w jednym konkretnym sektorze lub większej ich liczbie. Państwo trzecie powinno w szczególności zapewnić skuteczny niezależny nadzór nad ochroną danych oraz powinno przewidzieć mechanizmy współpracy z organami ochrony danych państw członkowskich, a osoby, których dane dotyczą, powinny uzyskać skuteczne, egzekwowalne prawa oraz skuteczne administracyjne i sądowe środki zaskarżenia.

(68) Poza międzynarodowymi zobowiązaniami, które przyjęły państwo trzecie lub organizacja międzynarodowa, Komisja powinna brać pod uwagę także obowiązki wynikające z udziału państwa trzeciego lub organizacji międzynarodowej w systemach wielostronnych lub regionalnych, zwłaszcza w odniesieniu do ochrony danych osobowych, a także realizację takich obowiązków. W szczególności powinna wziąć pod uwagę przystąpienie państwa trzeciego do Konwencji Rady Europy z dnia 28 stycznia 1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych oraz do Protokołu dodatkowego do tej Konwencji. Oceniając stopień ochrony w państwach trzecich lub organizacjach międzynarodowych Komisja powinna konsultować się z Europejską Radą Ochrony Danych ustanowioną rozporządzeniem (UE) 2016/… (*). Komisja powinna także brać pod uwagę wszelkie swoje decyzje stwierdzające odpowiedni stopień ochrony przyjęte na mocy art. 45 rozporządzenia (UE) 2016/… (*).

(69) Komisja powinna monitorować obowiązywanie decyzji o stopniu ochrony w państwie trzecim, na terytorium lub na określonym sektorze w państwie trzecim, lub w organizacji międzynarodowej. W swoich decyzjach stwierdzających odpowiedni stopień ochrony Komisja powinna przewidzieć mechanizm okresowego przeglądu ich funkcjonowania. Takiego okresowego przeglądu Komisja powinna dokonywać w porozumieniu z danym państwem trzecim lub daną organizacją międzynarodową i powinna w nim uwzględniać wszelkie istotne zmiany w państwie trzecim lub organizacji międzynarodowej.

(70) Komisja powinna mieć również możliwość uznania, że państwo trzecie, terytorium lub określony sektor w państwie trzecim, lub organizacja międzynarodowa przestały zapewniać odpowiedni stopień ochrony danych. W związku z tym przekazywanie danych osobowych do tego państwa trzeciego lub tej organizacji międzynarodowej powinno zostać zakazane, chyba że spełnione są wymogi niniejszej dyrektywy dotyczące przesyłania z zastrzeżeniem

(*) Rozporządzenie w st 5419/16.

odpowiednich zabezpieczeń i wyjątków w konkretnych sytuacjach. Należy przewidzieć procedury konsultacji między Komisją a takimi państwami trzecimi lub organizacjami międzynarodowymi. Komisja powinna niezwłocznie poinformować to państwo trzecie lub tę organizację międzynarodową o powodach oraz podjąć z nimi konsultacje w celu rozwiązania sytuacji.

(71) Przekazania nieprzeprowadzone na podstawie decyzji stwierdzającej odpowiedni stopień ochrony powinny być dopuszczalne jedynie wtedy, gdy w prawnie wiążącym akcie przewidziano odpowiednie zabezpieczenia zapewniające ochronę danych osobowych, lub gdy administrator ocenił wszystkie okoliczności towarzyszące przekazaniu danych **i** na podstawie tej oceny stwierdza, że istnieją odpowiednie zabezpieczenia w odniesieniu do ochrony danych osobowych. Takim prawnie wiążącym aktem może być przykładowo prawnie wiążąca umowa dwustronna, która została zawarta przez państwo członkowskie i wprowadzona przez nie do jego porządku prawnego, i która może być egzekwowana przez osoby, których dane dotyczą, i która zapewnia przestrzeganie wymogów ochrony danych oraz praw osób, której dane dotyczą, w tym prawa do skutecznych administracyjnych lub sądowych środków zaskarżenia. Oceniając wszystkie okoliczności towarzyszące przekazaniu danych, administrator powinien mieć możliwość uwzględnienia umów o współpracy zawartych przez Europol lub Eurojust z państwami trzecimi, pozwalających na wymianę danych osobowych. Administrator powinien też mieć możliwość uwzględnienia tego, czy przekazanie danych osobowych będzie podlegać obowiązkom zachowania poufności i zasadzie ograniczonego celu, tak aby dane nie były przetwarzane do celów innych niż cele, w których zostały przekazane. Ponadto administrator powinien wziąć pod uwagę to, czy dane osobowe nie posłużą do zażądania, orzeczenia lub wykonania kary śmierci ani do innego rodzaju okrutnego lub nieludzkiego traktowania. Jakkolwiek kryteria te można uznać za odpowiednie zabezpieczenia umożliwiające przekazanie danych, administrator powinien mieć możliwość zażądania dodatkowych zabezpieczeń.

(72) Jeżeli nie wydano decyzji stwierdzającej odpowiedni stopień ochrony lub nie ma odpowiednich zabezpieczeń, przekazanie lub określona kategoria przekazań może nastąpić tylko w szczególnych sytuacjach, gdy jest to konieczne, dla ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby, lub dla zabezpieczenia uzasadnionych prawnie interesów osoby, której dane dotyczą, zgodnie z wymogami prawa państwa członkowskiego przekazującego dane osobowe; dla zapobieżenia bezpośredniemu, poważnemu zagrożeniu dla bezpieczeństwa publicznego państwa członkowskiego lub państwa trzeciego; w indywidualnym przypadku dla celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kary, w tym dla ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegać takim zagrożeniom; w indywidualnym przypadku dla celów ustalenia roszczenia, jego dochodzenia lub obrony. Wyjątki te należy interpretować wąsko i nie powinny one umożliwiać częstego, masowego i zorganizowanego przekazywania danych osobowych ani przekazywania danych na dużą skalę; powinny też być ograniczone do danych ściśle niezbędnych. Takie operacje przekazywania powinny być udokumentowane, a dokumentacja ta powinna być udostępniana na żądanie organowi nadzorczemu w celu kontroli zgodności przekazania z prawem.

(73) Właściwe organy państw członkowskich stosują obowiązujące dwustronne lub wielostronne umowy międzynarodowe zawarte z państwami trzecimi w dziedzinie współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej, by wymieniać istotne informacje do wykonywania prawnie ciążących na nich obowiązków. Odbywa się to zasadniczo dzięki współpracy właściwych organów państw trzecich prowadzonej na potrzeby niniejszej dyrektywy, lub przynajmniej we współpracy z tymi organami, czasami nawet przy braku odpowiedniej dwustronnej lub wielostronnej umowy międzynarodowej. Niemniej w konkretnych indywidualnych przypadkach rutynowy tryb postępowania wymagający skontaktowania się z takim organem w państwie trzecim może okazać się nieskuteczny lub niewłaściwy, w szczególności ze względu na to, że przekazanie mogłoby ulec opóźnieniu, lub dlatego, że organ w państwie trzecim nie przestrzega praworządności lub międzynarodowych norm i standardów ochrony praw człowieka – w takiej sytuacji właściwe organy państw członkowskich mogą podjąć decyzję, że dane osobowe przekazane zostaną bezpośrednio odbiorcom znajdującym się w takich państwach trzecich. Może się tak zdarzyć wówczas, gdy zachodzi pilna potrzeba przekazania danych osobowych w celu ratowania życia osobie zagrożonej czynem zabronionym, lub gdy jest to konieczne do zapobieżenia spodziewanemu popełnieniu czynu zabronionego, w tym czynu terrorystycznego. Nawet jeżeli takie przekazanie między organami a odbiorcami mającymi siedzibę w państwach trzecich miałoby się odbywać tylko w konkretnych indywidualnych przypadkach, niniejsza dyrektywa powinna wskazać zasady służące uregulowaniu takich przypadków. Takich przepisów nie należy uznawać za wyjątki od obowiązujących dwustronnych lub wielostronnych umów międzynarodowych w dziedzinie współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej. Zasady te powinny obowiązywać obok pozostałych przepisów dyrektywy, zwłaszcza przepisów o zgodności przetwarzania z prawem i przepisów rozdziału V.

(74) Transgraniczne przekazywanie danych osobowych może spowodować wzrost ryzyka, że osoby fizyczne nie będą mogły wykonywać praw do ochrony danych osobowych w celu ochrony przed niezgodnym z prawem wykorzystaniem lub ujawnieniem tych danych. Jednocześnie organy nadzorcze mogą uznać, że nie są w stanie rozpatrzyć skargi lub prowadzić postępowania w sprawie działań, która mają miejsce poza granicami ich państwa. Ich starania na rzecz współpracy w kontekście transgranicznym mogą także zostać zakłócone przez niewystarczające uprawnienia prewencyjne lub zaradcze oraz niespójne systemy prawne. Należy więc upowszechniać ściślejszą współpracę między organami nadzorującymi ochronę danych w celu wspierania wymiany informacji z ich zagranicznymi odpowiednikami.

(75) Zasadniczym elementem ochrony osób fizycznych w związku z przetwarzaniem danych osobowych jest utworzenie w państwach członkowskich organów nadzorczych, które mają możliwość wykonywania swych funkcji w sposób całkowicie niezależny. Organy nadzorcze powinny monitorować stosowanie niniejszej dyrektywy oraz powinny przyczyniać się do ich spójnego stosowania w całej Unii, po to by chronić osoby fizyczne w związku z przetwarzaniem jej danych osobowych. W tym celu organy nadzorcze powinny współpracować ze sobą oraz z Komisją.

(76) Odpowiedzialność za zadania, które mają być realizowane przez krajowe organy nadzorcze ustanowione na podstawie niniejszej dyrektywy, państwa członkowskie mogą powierzyć organom nadzorczym już ustanowionym na mocy rozporządzenia (UE) 2016/… (*).

(77) Aby odzwierciedlić swoją strukturę konstytucyjną, organizacyjną i administracyjną, państwa członkowskie powinny mieć możliwość utworzenia więcej niż jednego organu nadzorczego. Każdy organ nadzorczy powinien zostać wyposażony w zasoby finansowe i kadrowe, pomieszczenia i infrastrukturę niezbędne do skutecznego wykonywania zadań, w tym zadań związanych z wzajemną pomocą i współpracą z innymi organami nadzorczymi z całej Unii. Każdy organ nadzorczy powinien dysponować odrębnym, publicznym budżetem rocznym, który może być częścią ogólnego budżetu państwowego lub krajowego.

(78) Organy nadzorcze powinny pod względem swoich wydatków finansowych podlegać niezależnym mechanizmom kontroli lub monitorowania, pod warunkiem że taka kontrola finansowa nie wpływa na ich niezależność.

(79) Ogólne warunki członkostwa w organie nadzorczym powinny zostać określone w prawie państwa członkowskiego i powinny w szczególności zapewniać, by członków tego organu powoływał przy zastosowaniu procedury zapewniającej przejrzystość parlament, rząd lub szef danego państwa członkowskiego – na wniosek rządu, członka rządu, parlamentu lub izby parlamentu – lub niezależny organ, któremu zadanie to powierzono w prawie państwa członkowskiego. Aby zapewnić niezależność organu nadzorczego, jego członek lub członkowie powinni działać uczciwie, powstrzymać się od wszelkich czynności niezgodnych ze swoimi obowiązkami i nie powinni podczas swojej kadencji podejmować żadnego zajęcia zarobkowego ani niezarobkowego niezgodnego z tymi obowiązkami. Aby zapewnić niezależność organu nadzorczego, organ sam powinien dobierać swój personel, co może też oznaczać wybór personelu przez niezależny organ utworzony na mocy prawa państwa członkowskiego.

(80) Niniejsza dyrektywa ma zastosowanie także do działalności sądów krajowych i innych organów wymiaru sprawiedliwości, niemniej właściwość organów nadzorczych nie powinna obejmować przetwarzania danych osobowych przez sądy w ramach sprawowania wymiaru sprawiedliwości, tak by chronić niezawisłość sędziów w wykonywaniu ich zadań sądowych. Wyjątek ten należy ograniczyć do czynności sądowych w sprawach sądowych i nie powinien on mieć zastosowania do innych czynności, w których sędziowie mogą brać udział zgodnie z prawem państwa członkowskiego. Państwa członkowskie powinny mieć również możliwość przyjęcia, że właściwość organu nadzorczego nie obejmuje przetwarzania danych osobowych przez inne niezależne organy wymiaru sprawiedliwości w toku sprawowania przez nie wymiaru sprawiedliwości, przykładowo przez prokuraturę. Niemniej przestrzeganie przepisów niniejszej dyrektywy przez sądy i inne niezależne organy wymiaru sprawiedliwości zawsze podlegają niezależnej kontroli zgodnie z art. 8 ust. 3 Karty.

(81) Każdy organ nadzorczy powinien rozpatrywać skargi wnoszone przez osoby, których dane dotyczą, oraz powinien zbadać taką sprawę lub przekazać ją do rozpatrzenia właściwemu organowi nadzorczemu. Postępowanie wyjaśniające na podstawie skargi powinno być prowadzone – z zastrzeżeniem kontroli sądowej – w zakresie odpowiadającym konkretnej sprawy. Organ nadzorczy powinien w rozsądnym terminie poinformować osobę, której dane dotyczą, o postępach i wynikach rozpatrywania skargi. Jeżeli dana sprawa wymaga przeprowadzenia dalszego postępowania lub koordynacji działań z innym organem nadzorczym, osoba, której dane dotyczą, powinna zostać o tym uprzednio poinformowana.

(82) Aby zapewnić skuteczne, rzetelne i spójnie przestrzeganie i wykonywanie niniejszej dyrektywy w całej Unii zgodnie z TFUE w interpretacji Trybunału Sprawiedliwości, organy nadzorcze powinny mieć w każdym państwie członkowskim te same zadania i faktyczne uprawnienia, w tym uprawnienia w zakresie prowadzenia postępowań, uprawnienia naprawcze i doradcze, które umożliwiają wykonywanie powierzonych im zadań. Ich uprawnienia nie powinny jednak kolidować ze szczegółowymi przepisami postępowania karnego, w tym o prowadzeniu postępowań przygotowawczych i ściganiu czynów zabronionych, ani z niezawisłością sądów. Z zastrzeżeniem uprawnień organów prokuratorskich na mocy prawa państwa członkowskiego organy nadzorcze powinny również mieć uprawnienie do wnoszenia naruszeń niniejszej dyrektywy przed organy sądowe lub do udziału w postępowaniu sądowym. Ze swoich uprawnień organ nadzorczy powinien korzystać zgodnie z odpowiednimi gwarancjami

(*) Rozporządzenie w st 5419/16.

proceduralnymi przewidzianymi w prawie Unii i w prawie państwa członkowskiego, bezstronnie, sprawiedliwie i w rozsądnym terminie. W szczególności każdy środek powinien być odpowiedni, niezbędny i proporcjonalny do zapewnienia przestrzegania niniejszej dyrektywy, z uwzględnieniem okoliczności danej sprawy, poszanowania prawa wysłuchania danej osoby przed zastosowaniem indywidualnego środka, który miałby niekorzystnie na nią wpłynąć, i bez nadmiernych kosztów i niedogodności dla danej osoby. Z uprawnień w zakresie prowadzenia postępowań wyjaśniających, jeżeli chodzi o dostęp do pomieszczeń, należy korzystać zgodnie ze szczegółowymi wymogami prawa państwa członkowskiego, takimi jak wymóg uzyskania wcześniejszej zgody sądu. Wydanie prawnie wiążącej decyzji powinno podlegać kontroli sądowej w państwie członkowskim organu nadzorczego, który ją wydał.

(83) Organy nadzorcze powinny wspierać się wzajemnie w wykonywaniu swoich zadań oraz świadczyć sobie wzajemną pomoc, by zapewnić spójne stosowanie i wykonanie niniejszej dyrektywy.

(84) Europejska Rada Ochrony Danych powinna przyczyniać się do spójnego stosowania niniejszej dyrektywy w całej Unii, m.in. poprzez doradzanie Komisji i propagowanie współpracy organów nadzorczych w całej Unii.

(85) Każda osoba, której dane dotyczą, powinna mieć prawo wniesienia skargi do jednego organu nadzorczego oraz prawo do skutecznego środka prawnego przed sądem zgodnie z art. 47 Karty praw podstawowych, jeżeli uzna, że jej prawa wynikające z przepisów przyjętych na podstawie niniejszej dyrektywy są naruszane, lub jeżeli organ nadzorczy nie reaguje na skargę, w części lub w całości ją odrzuca lub oddala lub nie podejmuje działania, choć jest ono niezbędne do ochrony praw osoby, której dane dotyczą. Postępowanie wyjaśniające w sprawie skargi powinno być prowadzone – z zastrzeżeniem kontroli sądowej – w zakresie odpowiednim do konkretnej sprawy. Właściwy organ nadzorczy powinien w rozsądnym terminie poinformować osobę, której dane dotyczą, o postępach i wynikach rozpatrywania skargi. Jeżeli dana sprawa wymaga przeprowadzenia dalszego postępowania wyjaśniającego lub koordynacji działań z innym organem nadzorczym, osoba, której dane dotyczą, powinna zostać o tym uprzednio poinformowana. Aby ułatwić wnoszenie skarg, każdy organ nadzorczy powinien przedsięwziąć takie środki, jak udostępnienie formularza skargi, który można wypełnić także elektronicznie, przy czym nie należy wykluczać innych sposobów komunikacji.

(86) Każda osoba fizyczna lub prawna powinna mieć prawo do skutecznego środka prawnego przed właściwym sądem krajowym od decyzji organu nadzorczego wywołującej skutki prawne wobec tej osoby. Taka decyzja może dotyczyć zwłaszcza wykonywania przez organ nadzorczy uprawnień do prowadzenia postępowań wyjaśniających, uprawnień naprawczych i do wydawania zezwoleń lub oddalania lub odrzucania skarg. Prawo to nie dotyczy jednak innych niewiążących prawnie środków organów nadzorczych, takich jak wydawane przez organ opinie czy zalecenia. Postępowanie przeciwko organowi nadzorczemu należy wszcząć przed sądem państwa członkowskiego, w którym organ nadzorczy ma siedzibę, a postępowanie powinno się toczyć zgodnie z prawem tego państwa członkowskiego. Sądy te powinny wykonywać pełną jurysdykcję w sprawie, w tym w zakresie ustalenia okoliczności faktycznych i prawnych istotnych dla rozstrzygnięcia sprawy.

(87) Jeżeli osoba, której dane dotyczą, uzna, że naruszane są jej prawa wynikające z niniejszej dyrektywy, powinna mieć prawo do umocowania podmiotu – którego celem jest ochrona praw i interesów osób w odniesieniu do ochrony ich danych osobowych oraz który został ustanowiony zgodnie z prawem państwa członkowskiego – do wniesienia skargi w swoim imieniu do organu nadzorczego oraz do wykonania prawa do środka prawnego przed sądem. Prawo osoby, której dane dotyczą, do reprezentacji nie powinno uchybiać prawu procesowemu państwa członkowskiego, które może wymagać, by osoba, której dane dotyczą, była przed sądami krajowymi obowiązkowo reprezentowana przez prawnika w rozumieniu dyrektywy Rady 77/249/EWG ([1]).

(88) Za wszelką szkodę, którą dana osoba mogła ponieść wskutek przetwarzania z naruszeniem przepisów przyjętych na podstawie niniejszej dyrektywy, powinno przysługiwać odszkodowanie od administratora lub innego organu właściwego w świetle prawa państwa członkowskiego. Pojęcie szkody należy interpretować szeroko, w świetle orzecznictwa Trybunału Sprawiedliwości, w sposób w pełni odzwierciedlający cele niniejszej dyrektywy. Nie ma to wpływu na jakiekolwiek roszczenia z tytułu szkód wynikających z naruszenia innych przepisów prawa Unii lub prawa państwa członkowskiego. W przypadku odwołania do przetwarzania niezgodnego z prawem lub z naruszeniem przepisów przyjętych na podstawie niniejszej dyrektywy, odwołanie obejmuje także przetwarzanie, które narusza akty wykonawcze przyjęte na podstawie niniejszej dyrektywy. Osoby, których dane dotyczą, powinny uzyskać pełne i skuteczne odszkodowanie za poniesioną szkodę.

([1]) Dyrektywa Rady 77/249/EWG z dnia 22 marca 1977 r. mająca na celu ułatwienie skutecznego korzystania przez prawników ze swobody świadczenia usług (Dz.U. L 78 z 26.3.1977, s. 17).

(89) Każda osoba fizyczna lub prawna, niezależnie od tego czy działa na podstawie prawa prywatnego czy publicznego, która narusza niniejszą dyrektywę, powinna podlegać sankcjom. Państwa członkowskie powinny zapewnić, by sankcje były skuteczne, proporcjonalne i odstraszające, oraz powinny podjąć wszelkie środki służące wykonaniu sankcji.

(90) Aby zapewnić jednolite warunki wdrażania niniejszej dyrektywy, należy powierzyć Komisji uprawnienia wykonawcze w odniesieniu do: stwierdzania odpowiedniego stopnia ochrony zapewnianego przez państwo trzecie, terytorium lub określony sektor w państwie trzecim, lub organizację międzynarodową; określania formuły i trybu wzajemnej pomocy oraz ustalania zasad wymiany informacji drogą elektroniczną między organami nadzorczymi oraz między organami nadzorczymi a Europejską Radą Ochrony Danych. Uprawnienia te powinny być wykonywane zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 182/2011 ([1]).

(91) Należy stosować procedurę sprawdzającą dla przyjmowania aktów wykonawczych w sprawie stwierdzenia odpowiedniego stopnia ochrony zapewnianego przez państwo trzecie, terytorium lub określony sektor w państwie trzecim, lub organizację międzynarodową oraz w sprawie formuły i trybu wzajemnej pomocy i ustalania zasad wymiany informacji drogą elektroniczną między organami nadzorczymi oraz między organami nadzorczymi a Europejską Radą Ochrony Danych, zważywszy że akty te mają zasięg ogólny.

(92) Komisja powinna przyjmować akty wykonawcze o natychmiastowym zastosowaniu, jeżeli jest to szczególnie pilne w należycie uzasadnionych przypadkach, dotyczących państwa trzeciego, terytorium lub określonego sektora w państwie trzecim, lub organizacji międzynarodowej, które nie zapewniają dłużej odpowiedniego stopnia ochrony.

(93) Ponieważ cele niniejszej dyrektywy – którymi są ochrona podstawowych praw i wolności osób fizycznych, w szczególności ich prawo do ochrony danych osobowych, oraz zapewnienie swobodnego przepływu danych osobowych między właściwymi organami w ramach całej Unii – nie mogą w wystarczającym stopniu zostać osiągnięte przez państwa członkowskie, natomiast z uwagi na zakres i skutki działania możliwe jest lepsze ich osiągnięcie na szczeblu unijnym, Unia może przyjąć środki zgodnie z zasadą pomocniczości, o której mowa w art. 5 TUE. Zgodnie z zasadą proporcjonalności określoną w tym samym artykule niniejsza dyrektywa nie wykracza poza zakres niezbędny do osiągnięcia tych celów.

(94) Dyrektywa nie powinna wpływać na szczegółowe przepisy aktów unijnych przyjętych w dziedzinie współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej, które zostały przyjęte przed datą przyjęcia niniejszej dyrektywy i regulują przetwarzanie danych osobowych między państwami członkowskimi lub dostęp wyznaczonych organów państw członkowskich do systemów informacyjnych ustanowionych na mocy traktatów – przepisy takie, jak np. szczegółowe przepisy o ochronie danych osobowych stosowane na mocy decyzji Rady 2008/615/WSiSW ([2]) czy art. 23 Konwencji o pomocy prawnej w sprawach karnych pomiędzy państwami członkowskimi Unii Europejskiej ([3]). Jako że zgodnie z art. 8 Karty i art. 16 TFUE prawo podstawowe do ochrony danych osobowych powinno być spójnie stosowane w całej Unii, Komisja powinna ocenić sytuację pod kątem stosunku niniejszej dyrektywy do aktów, które zostały przyjęte przed datą przyjęcia niniejszej dyrektywy i regulują przetwarzanie danych osobowych między państwami członkowskimi lub dostęp wyznaczonych organów państw członkowskich do systemów informacyjnych ustanowionych na mocy traktatów, oraz ustalić, czy należy te szczegółowe przepisy dostosować do niniejszej dyrektywy. W razie potrzeby Komisja powinna przedstawić wnioski celem zapewnienia spójności przepisów dotyczących przetwarzania danych osobowych.

(95) Aby ochrona danych osobowych w Unii była kompleksowa i spójna, międzynarodowe porozumienia, które zostały zawarte przez państwa członkowskie przed wejściem niniejszej dyrektywy w życie i które są zgodne z odnośnym prawem Unii mającym zastosowanie przed tą datą, powinny pozostać w mocy do czasu ich zmiany, zastąpienia lub uchylenia.

([1]) Rozporządzenie 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 (Dz.U. L 55 z 28.2.2011, s. 13).

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

([3]) Akt Rady z dnia 29 maja 2000 r. ustanawiający zgodnie z art. 34 Traktatu o Unii Europejskiej Konwencję o pomocy prawnej w sprawach karnych pomiędzy państwami członkowskimi Unii Europejskiej (Dz.U. C 197 z 12.7.2000, s. 1).

(96) Na transponowanie niniejszej dyrektywy państwom członkowskim należy przyznać nie więcej niż dwa lata od dnia jej wejścia w życie. Przetwarzanie, które w tym dniu jest w toku, powinno w terminie dwóch lat od dnia wejścia w życie niniejszej dyrektywy zostać dostosowane do jej przepisów. Jeżeli jednak takie przetwarzanie jest zgodne z prawem Unii mającym zastosowanie przed dniem wejścia niniejszej dyrektywy w życie, wymogi niniejszej dyrektywy dotyczące uprzednich konsultacji z organem nadzorczym nie powinny mieć zastosowania do operacji przetwarzania, które już ma miejsce, gdyż z uwagi na ich charakter wymogi te powinny zostać spełnione przed przetwarzaniem. Jeżeli państwa członkowskie stosują dłuższy termin wdrożenia, upływający siedem lat po dniu wejścia niniejszej dyrektywy w życie, dla wypełnienia zobowiązań dotyczących ewidencjonowania w zautomatyzowanych systemach przetwarzania ustanowionych przed tą datą, administrator lub podmiot przetwarzający powinni dysponować skutecznymi metodami, które pozwolą im na wykazanie zgodności przetwarzania danych z prawem, monitorowanie własnej działalności i zapewnienie integralności i bezpieczeństwa danych, takimi jak ewidencja lub inne formy zapisu.

(97) Niniejsza dyrektywa nie wpływa na przepisy o zwalczaniu niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz o zwalczaniu pornografii dziecięcej ustanowione w dyrektywie 2011/93/UE Parlamentu Europejskiego i Rady. ([1])

(98) Należy zatem uchylić decyzję ramową 2008/977/WSiSW.

(99) Zgodnie z art. 6a Protokołu nr 21 w sprawie stanowiska Zjednoczonego Królestwa i Irlandii w odniesieniu do przestrzeni wolności, bezpieczeństwa i sprawiedliwości, który jest załączony do TUE i TFUE, Zjednoczone Królestwo i Irlandia nie są związane przepisami ustanowionymi w niniejszej dyrektywie, dotyczącymi przetwarzania danych osobowych przez państwa członkowskie w ramach wykonywania działań wchodzących w zakres zastosowania części trzeciej tytuł V rozdział 4 lub rozdział 5 TFUE, jeżeli państwa te nie są związane zasadami regulującymi formy współpracy wymiarów sprawiedliwości w sprawach karnych lub współpracy policyjnej, w ramach której należy przestrzegać przepisów ustanowionych na podstawie art. 16 TFUE.

(100) Zgodnie z art. 2 i 2a Protokołu nr 22 w sprawie stanowiska Danii, który jest załączony do TUE i TFUE, Dania nie jest związana przepisami ustanowionymi w niniejszej dyrektywie ani im nie podlega, o ile przepisy te dotyczą przetwarzania danych osobowych przez państwa członkowskie w ramach wykonywania działań wchodzących w zakres zastosowania części trzeciej tytuł V rozdział 4 lub rozdział 5 TFUE. Ponieważ niniejsza dyrektywa stanowi rozwinięcie przepisów dorobku Schengen w rozumieniu części trzeciej tytuł V TFUE, Dania zgodnie z art. 4 tego protokołu podejmie w terminie sześciu miesięcy od daty przyjęcia niniejszej dyrektywy decyzję, czy dokona jej transpozycji do swojego prawa krajowego.

(101) W odniesieniu do Islandii i Norwegii 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 ([2]).

(102) W odniesieniu do Szwajcarii niniejsza dyrektywa stanowi rozwinięcie przepisów dorobku Schengen w rozumieniu Umowy zawartej między Unią Europejską, Wspólnotą Europejską a Konfederacją Szwajcarską w sprawie włączenia Konfederacji Szwajcarskiej we wprowadzanie w życie, stosowanie i rozwój dorobku Schengen ([3]).

(103) W odniesieniu do Liechtensteinu 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 ([4]).

([1]) Dyrektywa Parlamentu Europejskiego i Rady 2011/93/UE z dnia 13 grudnia 2011 r. w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej, zastępująca decyzję ramową Rady 2004/68/WSiSW (Dz.U. L 335 z 17.12.2011, s. 1).
([2]) Dz.U. L 176 z 10.7.1999, s. 36.
([3]) Dz.U. L 53 z 27.2.2008, s. 52.
([4]) Dz.U. L 160 z 18.6.2011, s. 21.

(104) Niniejsza dyrektywa nie narusza praw podstawowych i jest zgodna z zasadami uznanymi w Karcie umocowanej TFUE, w szczególności z prawem do poszanowania życia prywatnego i rodzinnego, prawem do ochrony danych osobowych oraz prawem do skutecznego środka prawnego i do rzetelnego procesu. Ograniczenia tych praw są zgodne z art. 52 ust. 1 karty, ponieważ są niezbędne do realizacji celów leżących w interesie ogólnym i uznanych przez Unię lub do ochrony praw i wolności innych osób.

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

(106) Zgodnie z art. 28 ust. 2 rozporządzenia (WE) nr 45/2001 przeprowadzono konsultację z Europejskim Inspektorem Ochrony Danych, który wydał opinię w dniu 7 marca 2012 r. ([1]).

(107) Niniejsza dyrektywa nie powinna uniemożliwiać państwom członkowskim wdrożenia praw osób, których dane dotyczą, do informacji, dostępu i do sprostowania lub usunięcia danych osobowych oraz ograniczenia przetwarzania w toku postępowania karnego, oraz ewentualnych ograniczeń tych praw, w krajowych przepisach procedury karnej,

PRZYJMUJE NINIEJSZĄ DYREKTYWĘ:

ROZDZIAŁ I

Przepisy ogólne

Artykuł 1

Przedmiot i cele

1. Niniejsza dyrektywa ustanawia przepisy o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom.

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, jeżeli wynika z prawa Unii lub prawa krajowego, nie była ograniczana ani zakazywana z powodów dotyczących ochrony osób fizycznych w związku z przetwarzaniem danych osobowych.

3. Niniejsza dyrektywa nie wyklucza ustanowienia przez państwa członkowskie zabezpieczeń wyższych niż zabezpieczenia przewidziane w niniejszej dyrektywie dla ochrony praw i wolności osoby, której dane dotyczą, w związku z przetwarzaniem danych osobowych przez właściwe organy.

Artykuł 2

Zakres zastosowania

1. Niniejsza dyrektywa ma zastosowanie 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 całkowicie lub częściowo zautomatyzowany, oraz do przetwarzania w sposób inny niż zautomatyzowany danych osobowych stanowiących część zbioru danych lub mających stanowić część zbioru danych.

([1]) Dz.U. C 192 z 30.6.2012, s. 7.

3. Niniejsza dyrektywa nie ma zastosowania do przetwarzania danych osobowych:

a) w ramach działalności nieobjętej zakresem prawa Unii;

b) przez instytucje, organy i jednostki organizacyjne Unii.

Artykuł 3

Definicje

Do celów niniejszej dyrektywy:

1) „dane osobowe" oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy bądź jeden lub kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

2) „przetwarzanie" oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

3) „ograniczenie przetwarzania" oznacza oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;

4) „profilowanie" oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;

5) „pseudonimizacja" oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;

6) „zbiór danych" oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;

7) „właściwy organ" oznacza:

   a) organ publiczny właściwy do zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom; lub

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

8) „administrator" oznacza właściwy organ, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby przetwarzania są określone prawem Unii lub prawem państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania;

9) „podmiot przetwarzający” oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę organizacyjną lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;

10) „odbiorca” oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę organizacyjną lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania;

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

12) „dane genetyczne” oznaczają dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej;

13) „dane biometryczne” oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby fizycznej, takie jak wizerunek twarzy lub dane daktyloskopijne;

14) „dane dotyczące zdrowia” oznaczają dane osobowe dotyczące zdrowia fizycznego lub psychicznego osoby fizycznej, w tym o korzystaniu z usług opieki zdrowotnej, ujawniające informacje o stanie jej zdrowia;

15) „organ nadzorczy” oznacza niezależny organ publiczny ustanowiony przez państwo członkowskie na mocy art. 41;

16) „organizacja międzynarodowa” oznacza organizację i organy jej podlegające działające na podstawie prawa międzynarodowego publicznego lub inny organ powołany w drodze umowy między co najmniej dwoma państwami lub na podstawie takiej umowy.

ROZDZIAŁ II

Zasady

Artykuł 4

Zasady dotyczące przetwarzania danych osobowych

1. Państwa członkowskie zapewniają, by dane osobowe były:

a) przetwarzane zgodnie z prawem i rzetelnie;

b) zbierane w konkretnych, wyraźnych i uzasadnionych celach i nieprzetwarzane w sposób niezgodny z tymi celami;

c) adekwatne, stosowne i nienadmierne do celów, dla których są przetwarzane;

d) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe, w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane;

e) przechowywane w formie umożliwiającej identyfikację osób, których dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów ich przetwarzania;

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

2. Przetwarzanie przez tego samego lub innego administratora w jednym z celów określonych w art. 1 ust. 1 innym niż cel, w którym dane osobowe zostały zebrane, jest dozwolone, o ile:

a) administratorowi wolno przetwarzać takie dane osobowe w takim celu na mocy prawa Unii lub prawa państwa członkowskiego; oraz

b) przetwarzanie jest niezbędne i proporcjonalne w tym innym celu na mocy prawa Unii lub prawa państwa członkowskiego.

3. Przetwarzanie przez tego samego lub innego administratora może obejmować archiwizację w interesie publicznym, wykorzystanie do celów naukowych, statystycznych lub historycznych, o których mowa w art. 1 ust. 1, o ile podlega ono odpowiednim zabezpieczeniom praw i wolności osób, których dane dotyczą.

4. Za przestrzeganie przepisów ust. 1, 2 i 3 odpowiada administrator, który musi być w stanie wykazać fakt ich przestrzegania.

Artykuł 5

Terminy przechowywania i przeglądu

Państwa członkowskie zapewniają, by przyjęto odpowiednie terminy usuwania danych osobowych lub okresowego przeglądu konieczności przechowywania danych osobowych. Przestrzeganiu tych terminów służą odpowiednie środki proceduralne.

Artykuł 6

Rozróżnianie poszczególnych kategorii osób, których dane dotyczą

1. Państwa członkowskie zapewniają, by administrator – w stosownym przypadku i w miarę możliwości – wyraźnie rozróżniał dane osobowe poszczególnych kategorii osób, których dane dotyczą, takich jak:

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

b) osoby skazane za czyn zabroniony;

c) pokrzywdzeni czynem zabronionym lub osoby, w przypadku których określone fakty wskazują, że mogą stać się ofiarą czynu zabronionego; oraz

d) osoby inne w stosunku do czynu zabronionego, takie jak osoby, które mogą zostać wezwane do złożenia zeznań w ramach postępowania przygotowawczego w sprawie czynu zabronionego lub dalszych etapów postępowania karnego, osoby, które mogą dostarczyć informacji o czynach zabronionych, lub osoby, które mają kontakty lub powiązania z jedną z osób, o których mowa w lit. a) i b).

Artykuł 7

Rozróżnianie pomiędzy danymi osobowymi i weryfikacja jakości danych osobowych

1. Państwa członkowskie zapewniają, by dane osobowe oparte na faktach były rozróżniane, tak dalece, jak to możliwe, z danymi osobowych opartymi na indywidualnych ocenach.

2. Państwa członkowskie zapewniają, by właściwe organy podejmowały wszelkie rozsądne działania dla zagwarantowania, by nieprawidłowe, niekompletne lub nieaktualne dane osobowe nie były przesyłane lub udostępniane. W tym celu każdy właściwy organ weryfikuje tak dalece, jak to zasadne, jakość danych osobowych przed ich przesłaniem lub udostępnieniem. W miarę możliwości, we wszystkich przypadkach przesyłania danych osobowych, należy dodać niezbędne dodatkowe informacje pozwalające właściwemu organowi odbierającemu ocenić stopień prawidłowości, kompletności wiarygodności danych osobowych oraz stopień ich aktualności.

3. Jeżeli okaże się, że przesłano dane nieprawidłowe, lub że dane osobowe przesłano niezgodnie z prawem, należy o tym bezzwłocznie powiadomić odbiorcę. W takim przypadku dane osobowe należy sprostować, usunąć lub ograniczyć ich przetwarzanie zgodnie z art. 16.

Artykuł 8

Zgodność przetwarzania z prawem

1. Państwa członkowskie zapewniają, by przetwarzanie było zgodne z prawem wyłącznie wówczas i w zakresie, w jakim jest ono niezbędne do wykonania zadania realizowanego przez właściwy organ w celach określonych w art. 1 ust. 1 oraz ma podstawę w prawie Unii lub prawie państwa członkowskiego.

2. Prawo państwa członkowskiego regulujące przetwarzanie w zakresie stosowania niniejszej dyrektywy określa co najmniej powody przetwarzania, dane osobowe mające podlegać przetwarzaniu oraz cele przetwarzania.

Artykuł 9

Szczególne warunki przetwarzania

1. Danych osobowych zebranych przez właściwe organy do celów określonych w art. 1 ust. 1 nie przetwarza się do celów innych niż określone w art. 1 ust. 1, chyba że takie przetwarzanie jest dozwolone prawem Unii lub prawem państwa członkowskiego. Jeżeli przetwarzanie danych osobowych odbywa się w takich innych celach, zastosowanie ma rozporządzenie (UE) 2016/… (*), chyba że przetwarzanie odbywa się w toku działalności nieobjętej prawem Unii.

2. Jeżeli prawo państwa członkowskiego powierza właściwym organom wykonywanie zadań innych niż zadania wykonywane w celach określonych w art. 1 ust. 1, to do przetwarzania w takich celach, w tym na potrzeby archiwizacji w interesie publicznym, wykorzystania do celów naukowych, statystycznych lub historycznych, ma zastosowanie rozporządzenie (UE) 2016/… (*), chyba że przetwarzanie odbywa się w toku działalności nieobjętej prawem Unii.

3. Państwa członkowskie zapewniają, by wówczas, gdy prawo Unii lub państwa członkowskiego mające zastosowanie do właściwego organu przesyłającego przewiduje szczególne warunki przetwarzania, właściwy organ przesyłający informował odbiorcę takich danych osobowych o tych warunkach i o obowiązku ich przestrzegania.

4. Państwa członkowskie zapewniają, by właściwy organ przesyłający nie stosował warunków wskazanych w ust. 3 do odbiorców w innych państwach członkowskich ani w organach i jednostkach organizacyjnych ustanowionych na mocy tytułu V rozdział 4 i 5 TFUE, innych niż mające zastosowanie do podobnego przesyłania danych w obrębie państwa członkowskiego właściwego organu przesyłającego.

Artykuł 10

Przetwarzanie szczególnych kategorii danych osobowych

Przetwarzanie danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe lub przynależność do związków zawodowych oraz przetwarzanie danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej, danych dotyczących zdrowia lub danych dotyczących seksualności i orientacji seksualnej osoby fizycznej jest dozwolone wyłącznie wtedy, jeżeli jest bezwzględnie niezbędne, podlega odpowiednim zabezpieczeniom dla praw i wolności osoby, której dane dotyczą, oraz:

a) jest dopuszczone prawem Unii lub prawem państwa członkowskiego;

b) jest niezbędne dla ochrony żywotnych interesów osoby fizycznej, której dane dotyczą, lub innej osoby; lub

c) takie przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą.

Artykuł 11

Zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach

1. Państwa członkowskie zapewniają, by decyzje, które opierają się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i mają niekorzystne skutki prawne dla osoby, której dane dotyczą, lub poważnie na nią wpływają, były zakazane, chyba że dopuszcza je prawo Unii lub prawo państwa członkowskiego, któremu podlega administrator i które przewiduje odpowiednie zabezpieczenia praw i wolności osoby, której dane dotyczą, a przynajmniej prawo do uzyskania interwencji ludzkiej ze strony administratora.

(*) Rozporządzenie w st 5419/16.

2. Decyzje, o których mowa w ust. 1 niniejszego artykułu, nie mogą opierać się na danych osobowych szczególnych kategorii, o których mowa w art. 10, chyba że istnieją właściwe środki ochrony praw, wolności i uzasadnionych interesów osoby, której dane dotyczą.

3. Profilowanie skutkujące dyskryminacją osób fizycznych na podstawie danych osobowych szczególnych kategorii, o których mowa w art. 10, jest zabronione zgodnie z prawem Unii.

ROZDZIAŁ III

Prawa osoby, której dane dotyczą

Artykuł 12

Komunikacja oraz ułatwienia w wykonywaniu praw osób, których dane dotyczą

1. Państwa członkowskie zapewniają, by administrator podejmował wszelkie rozsądne działania, aby udzielić osobie, której dane dotyczą, wszelkich informacji, o których mowa w art. 13, oraz aby prowadził z nią wszelką komunikację wskazaną w art. 11, 14–18 i 31 w sprawie przetwarzania w zwięzłej, zrozumiałej i łatwo dostępnej formie, przy użyciu jasnego i prostego języka. Informacji udziela się wszelkimi stosownymi sposobami, w tym elektronicznie. Co do zasady administrator udziela informacji w takiej samej formie, w jakiej wniesiono żądanie.

2. Państwa członkowskie zapewniają, by administrator ułatwiał osobie, której dane dotyczą, wykonywanie praw przysługujących jej na mocy art. 11 i 14–18.

3. Państwa członkowskie zapewniają, by administrator bez zbędnej zwłoki informował pisemnie osobę, której dane dotyczą, o działaniach podjętych w związku z jej żądaniem.

4. Państwa członkowskie zapewniają, by informacje przekazywane na mocy art. 13 oraz wszelka komunikacja i wszelkie działania podjęte na mocy art. 11, 14–18 i 31 były wolne od opłat. Jeżeli żądania osoby, której dane dotyczą, są w sposób oczywisty nieuzasadnione lub nadmierne, zwłaszcza ze względu na ich powtarzalność, administrator może:

a) pobrać rozsądną opłatę, uwzględniając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań; lub

b) odmówić podjęcia działań w związku z żądaniem.

Obowiązek wykazania, że żądanie jest w sposób oczywisty nieuzasadnione lub nadmierne, spoczywa na administratorze.

5. Jeżeli administrator ma uzasadnione wątpliwości co do tożsamości osoby fizycznej składającej żądanie, o którym mowa w art. 14 i 16, może zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby, której dane dotyczą.

Artykuł 13

Informacje udostępniane lub przekazywane osobie, której dane dotyczą

1. Państwa członkowskie zapewniają, by administrator udostępniał osobie, której dane dotyczą, przynajmniej następujące informacje:

a) tożsamość i dane kontaktowe administratora;

b) dane kontaktowe inspektora ochrony danych, w razie potrzeby;

c) cele przetwarzania, do których mają posłużyć dane osobowe;

d) informacje o prawie do wniesienia skargi do organu nadzorczego oraz dane kontaktowe organu nadzorczego;

e) informacje o prawie żądania od administratora dostępu do danych osobowych, sprostowania lub usunięcia danych osobowych lub ograniczenia przetwarzania danych osobowych odnoszącego się do osoby, której dane dotyczą.

2. Państwa członkowskie zapewniają, by oprócz informacji, o których mowa w ust. 1, w konkretnych przypadkach administrator przekazywał osobie, której dane dotyczą, następujące dalsze informacje umożliwiające wykonywanie przysługujących jej praw:

a) podstawa prawna przetwarzania;

b) okres przechowywania danych osobowych lub, gdy nie jest to możliwe, kryteria służące określeniu tego okresu;

c) w stosownym przypadku kategorie odbiorców danych osobowych, w tym odbiorców w państwach trzecich lub organizacjach międzynarodowych;

d) w razie potrzeby dalsze informacje, zwłaszcza gdy dane osobowe są zbierane bez wiedzy osoby, której dotyczą.

3. Państwa członkowskie mogą przyjąć akty prawne pozwalające opóźnić, ograniczyć lub pominąć informowanie osoby, której dane dotyczą, przewidziane w ust. 2 w takim zakresie i przez taki czas, w jakim odnośny środek jest działaniem koniecznym i proporcjonalnym w społeczeństwie demokratycznym, z należytym uwzględnieniem praw podstawowych i uzasadnionych interesów danej osoby fizycznej, aby:

a) uniemożliwić utrudnianie czynności postępowań urzędowych lub sądowych, postępowań przygotowawczych lub procedur;

b) uniemożliwić zakłócanie zapobieganiu przestępczości, prowadzeniu postępowań przygotowawczych, wykrywaniu i ściganiu czynów zabronionych i wykonywaniu kar;

c) chronić bezpieczeństwo publiczne;

d) chronić bezpieczeństwo narodowe;

e) chronić prawa i wolności innych osób.

4. Państwa członkowskie mogą przyjąć akty prawne dla określenia kategorii przetwarzania, które w całości lub części wchodzą w zakres stosowania środków wskazanych w ust. 3 lit. a)–e).

Artykuł 14

Prawo dostępu przysługujące osobie, której dane dotyczą

Z zastrzeżeniem art. 15 państwa członkowskie zapewniają osobie, której dane dotyczą, prawo do uzyskania od administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli takie dane są przetwarzane, prawo dostępu do danych osobowych i do następujących informacji:

a) cele i podstawa prawna przetwarzania;

b) kategorie odnośnych danych osobowych;

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

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

e) informacje o prawie do żądania od administratora sprostowania lub usunięcia danych osobowych lub ograniczenia przetwarzania danych osobowych dotyczących tej osoby;

f) informacje o prawie wniesienia skargi do organu nadzorczego oraz dane kontaktowe organu nadzorczego;

g) wskazanie, jakie dane osobowe są przetwarzane, oraz wszelkie dostępne informacje o ich pochodzeniu.

Artykuł 15

Ograniczenia prawa dostępu

1. Państwa członkowskie mogą przyjąć akty prawne pozwalające ograniczyć w całości lub w części prawo dostępu osoby, której dane dotyczą, w takim stopniu i przez taki okres, w jakim takie częściowe lub całkowite ograniczenie jest działaniem niezbędnym i proporcjonalnym w społeczeństwie demokratycznym, z należytym uwzględnieniem praw podstawowych i uzasadnionych interesów danej osoby fizycznej, aby:

a) uniemożliwić utrudnianie czynności postępowań urzędowych lub sądowych, postępowań przygotowawczych lub procedur;

b) uniemożliwić zakłócanie zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar;

c) chronić bezpieczeństwo publiczne;

d) chronić bezpieczeństwo narodowe;

e) chronić prawa i wolności innych osób.

2. Państwa członkowskie mogą przyjąć akty prawne, aby ustalić kategorie przetwarzania, które w całości lub części wchodzą w zakres stosowania ust. 1 lit. a)–e).

3. W przypadkach, o których mowa w ust. 1 i 2, państwa członkowskie zapewniają, by administrator bez zbędnej zwłoki informował pisemnie osobę, której dane dotyczą, o każdej odmowie lub o każdym ograniczeniu dostępu i o przyczynach tej odmowy lub tego ograniczenia. Informacje takie można pominąć, jeżeli ich udzielenie godziłoby w którykolwiek z celów, o których mowa w ust. 1. Państwa członkowskie zapewniają, by administrator informował osobę, której dane dotyczą, o możliwości wniesienia skargi do organu nadzorczego lub środka prawnego do sądu.

4. Państwa członkowskie zapewniają, by administrator dokumentował faktyczne lub prawne powody, na jakich opiera się decyzja. Informacje te udostępnia się organom nadzorczym.

Artykuł 16

Prawo do sprostowania lub usunięcia danych osobowych oraz ograniczenia ich przetwarzania

1. Państwa członkowskie zapewniają, by osoba, której dane dotyczą, miała prawo uzyskania od administratora sprostowania bez zbędnej zwłoki jej danych osobowych, jeżeli są nieprawidłowe. Mając na względzie cel przetwarzania, państwa członkowskie zapewniają, by osoba, której dane dotyczą, miała prawo uzyskania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.

2. Państwa członkowskie nakładają na administratora wymóg usunięcia bez zbędnej zwłoki danych osobowych i zapewniają, by osoba, której dane dotyczą, miała prawo uzyskać od administratora usunięcie bez zbędnej zwłoki jej danych osobowych, jeżeli przetwarzanie narusza przepisy przyjęte na podstawie art. 4, 8 i 10, lub jeżeli dane osobowe muszą zostać usunięte w celu wypełnienia obowiązku prawnego ciążącego na administratorze.

3. Zamiast usunięcia, administrator ogranicza przetwarzanie, jeżeli:

a) osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych, a ich prawidłowości lub nieprawidłowości nie można stwierdzić; lub

b) dane osobowe muszą zostać zachowane do celów dowodowych.

Jeżeli przetwarzanie jest ograniczone na mocy akapitu pierwszego lit. a), przed zniesieniem tego ograniczenia administrator informuje o tym osobę, której dane dotyczą.

4. Państwa członkowskie zapewniają, by administrator informował pisemnie osobę, której dane dotyczą, o każdej odmowie sprostowania lub usunięcia danych osobowych lub ograniczenia przetwarzania danych oraz o przyczynach tej odmowy. Państwa członkowskie mogą przyjąć akty prawne, które w całości lub w części ograniczają obowiązek udzielania takich informacji, jeżeli takie ograniczenie przetwarzania jest działaniem niezbędnym i proporcjonalnym w społeczeństwie demokratycznym, z należytym uwzględnieniem praw podstawowych i uzasadnionych interesów danej osoby fizycznej, aby:

a) uniemożliwić utrudnianie czynności postępowań urzędowych lub sądowych, postępowań przygotowawczych lub procedur;

b) uniemożliwić zakłócanie zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar;

c) chronić bezpieczeństwo publiczne;

d) chronić bezpieczeństwo narodowe;

e) chronić prawa i wolności innych osób.

Państwa członkowskie zapewniają, by administrator informował osobę, której dane dotyczą, o możliwości wniesienia skargi do organu nadzorczego lub środka prawnego do sądu.

5. Państwa członkowskie zapewniają, by administrator informował o sprostowaniu nieprawidłowych danych osobowych właściwy organ, od którego nieprawidłowe dane pochodzą.

6. Państwa członkowskie zapewniają, by w przypadkach sprostowania lub usunięcia danych osobowych lub ograniczenia ich przetwarzania, na podstawie ust. 1, 2 i 3, administrator miał obowiązek powiadomienia o tym odbiorców, a odbiorcy mieli obowiązek sprostowania lub usunięcia danych osobowych lub ograniczenia przetwarzania danych osobowych.

Artykuł 17

Wykonywanie praw osoby, której dane dotyczą, oraz weryfikacja dokonywana przez organ nadzorczy

1. W odniesieniu do przypadków, o których mowa w art. 13 ust. 3, art. 15 ust. 3 i art. 16 ust. 4, państwa członkowskie przyjmują środki przewidujące, że osoba, której dane dotyczą, może wykonywać swoje prawa także za pośrednictwem właściwego organu nadzorczego.

2. Państwa członkowskie zapewniają, by administrator informował osobę, której dane dotyczą, o możliwości wykonywania przysługujących jej praw za pośrednictwem organu nadzorczego na mocy ust. 1.

3. W razie wykonywania prawa, o którym mowa w ust. 1, organ nadzorczy informuje osobę, której dane dotyczą, przynajmniej o fakcie przeprowadzenia wszelkich niezbędnych weryfikacji lub przeglądów. Organ nadzorczy informuje osobę, której dane dotyczą, także o przysługującym jej prawie do wniesienia środka prawnego do sądu.

Artykuł 18

Prawa osoby, której dane dotyczą, w postępowaniu przygotowawczym i sądowym w sprawie karnej

Państwa członkowskie mogą zapewnić, by wykonywanie praw określonych w art. 13, 14 i 16 odbywało się zgodnie z prawem państwa członkowskiego, jeżeli dane osobowe znajdują się w orzeczeniu sądu, protokole lub aktach sprawy przetwarzanych w toku postępowania przygotowawczego lub sądowego w sprawie karnej.

ROZDZIAŁ IV

Administrator I podmiot przetwarzający

Sekcja 1

Obowiązki ogólne

Artykuł 19

Obowiązki administratora

1. Państwa członkowskie zapewniają, by administrator wdrażał – uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia – odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszą dyrektywą i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane.

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

Artykuł 20

Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych

1. Państwa członkowskie zapewniają, by – uwzględniając stan wiedzy technicznej i koszt wdrożenia oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia wynikające z przetwarzania – administrator zarówno w czasie określania sposobów przetwarzania, jak i w czasie samego przetwarzania, miał obowiązek wdrożenia odpowiednich środków technicznych i organizacyjnych, takie jak pseudonimizacja, które zostały zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacji danych, oraz w nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi niniejszej dyrektywy oraz chronić prawa osób, których dane dotyczą.

2. Państwa członkowskie zapewniają, by administrator wdrażał odpowiednie środki techniczne i organizacyjne w celu zapewnienia, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne w stosunku do każdego konkretnego celu przetwarzania. Obowiązek ten ma zastosowanie do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. W szczególności środki te zapewniają, że domyślnie dane osobowe nie są udostępniane bez interwencji osoby fizycznej nieokreślonej liczbie osób fizycznych.

Artykuł 21

Współadministratorzy

1. Państwa członkowskie zapewniają, by w przypadku gdy co najmniej dwaj administratorzy wspólnie ustalają cele i sposoby przetwarzania, byli oni współadministratorami. W drodze wspólnych uzgodnień współadministratorzy w przejrzysty sposób określają podział swych obowiązków w zakresie wypełnienia niniejszej dyrektywy, w szczególności w odniesieniu do wykonywania przez osobę, której dane dotyczą, przysługujących jej praw, oraz podział obowiązków w zakresie udzielania informacji, o których mowa w art. 13, chyba że przypadające im obowiązki i ich zakres określa prawo Unii lub prawo państwa członkowskiego, któremu administratorzy ci podlegają. W uzgodnieniach wskazuje się punkt kontaktowy dla osób, których dane dotyczą. Państwa członkowskie mogą wskazać, który ze współadministratorów może pełnić funkcję pojedynczego punktu kontaktowego wobec osób, których dane dotyczą, w celu wykonywania ich praw.

2. Niezależnie od uzgodnień, o których mowa w ust. 1, państwa członkowskie mogą ustanowić, że osoba, której dane dotyczą, może wykonywać prawa przysługujące jej na mocy przepisów przyjętych na podstawie niniejszej dyrektywy w odniesieniu do każdego z administratorów i przeciwko każdemu z nich.

Artykuł 22

Podmiot przetwarzający

1. Państwa członkowskie zapewniają, by – jeżeli przetwarzanie ma być dokonywane w imieniu administratora – administrator miał obowiązek korzystania z usług wyłącznie takich podmiotów przetwarzających, które dają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, oraz zapewniał, by przetwarzanie odpowiadało wymogom niniejszej dyrektywy i chroniło prawa osoby, której dane dotyczą.

2. Państwa członkowskie zapewniają, by podmiot przetwarzający nie korzystał z usług innego podmiotu przetwarzającego bez wcześniejszej szczegółowej lub ogólnej pisemnej zgody administratora. W przypadku ogólnej pisemnej zgody podmiot przetwarzający informuje administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających, dając tym samym administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian.

3. Państwa członkowskie zapewniają, by przetwarzanie przez podmiot przetwarzający było regulowane umową lub innym instrumentem prawnym prawa Unii lub prawa państwa członkowskiego, które wiąże podmiot przetwarzający z administratorem oraz określa przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych i kategorie osób, których dane dotyczą oraz prawa i obowiązki administratora. Taka umowa lub inny instrument prawny stanowią w szczególności, że podmiot przetwarzający:

a) działa wyłącznie zgodnie z poleceniami administratora;

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

c) wszelkimi odpowiednimi sposobami pomaga administratorowi w przestrzeganiu przepisów o prawach osoby, której dane dotyczą;

d) po zakończeniu świadczenia usługi przetwarzania danych, w zależności od decyzji administratora, usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego wymaga przechowywanie danych osobowych;

e) udostępnia administratorowi wszelkie informacje niezbędne do wykazania zgodności z niniejszym artykułem;

f) przestrzega warunków zaangażowania innego podmiotu przetwarzającego, o których mowa w ust. 2 i 3.

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

5. Jeżeli podmiot przetwarzający określi, z naruszeniem niniejszej dyrektywy, cele i sposoby przetwarzania, uznaje się go za administratora w odniesieniu do tego przetwarzania.

Artykuł 23

Przetwarzanie z upoważnienia administratora lub podmiotu przetwarzającego

Państwa członkowskie zapewniają, by podmiot przetwarzający oraz każda osoba działająca z upoważnienia administratora lub podmiotu przetwarzającego i mająca dostęp do danych osobowych przetwarzała je wyłącznie zgodnie z poleceniami administratora, chyba że wymaga tego prawo Unii lub prawo państwa członkowskiego.

Artykuł 24

Wykazy czynności przetwarzania

1. Państwa członkowskie zapewniają, by administratorzy prowadzili wykaz wszystkich kategorii czynności przetwarzania, za które odpowiadają. W wykazie tym zamieszcza się wszystkie następujące informacje:

a) imię i nazwisko lub nazwa oraz dane kontaktowe administratora i, w razie potrzeby współadministratora oraz inspektora ochrony danych;

b) cele przetwarzania;

c) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub organizacjach międzynarodowych;

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

e) w stosownym przypadku informacje o stosowaniu profilowania;

f) w stosownym przypadku kategorie przekazań danych osobowych do państwa trzeciego lub organizacji międzynarodowej;

g) wskazanie podstawy prawnej operacji przetwarzania, w tym przekazań, do których dane osobowe są przeznaczone;

h) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;

i) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 29 ust. 1.

2. Państwa członkowskie zapewniają, by podmioty przetwarzające prowadziły wykaz wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora, w którym znajdują się:

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

b) kategorie przetwarzań dokonywanych w imieniu każdego z administratorów;

c) w stosownym przypadku przypadki przekazania danych osobowych do państw trzecich lub organizacji międzynarodowej, w razie jednoznacznego polecenia administratora, łącznie z nazwą tego państwa trzeciego lub organizacji międzynarodowej;

d) w miarę możliwości ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 29 ust. 1.

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

Administrator i podmiot przetwarzający udostępniają wskazane wykazy organowi nadzorczemu na jego żądanie.

Artykuł 25

Ewidencja czynności

1. Państwa członkowskie zapewniają, by ewidencjonowano przynajmniej następujące operacje przetwarzania prowadzone w zautomatyzowanych systemach przetwarzania: zbieranie, modyfikowanie, przeglądanie, ujawnianie wraz z przekazywaniem, łączenie i usuwanie. Ewidencja przeglądania i ujawniania pozwala ustalić zasadność, datę i godzinę takich operacji oraz w miarę możliwości tożsamość osoby, która przeglądała lub ujawniła dane osobowe, oraz tożsamość odbiorców takich danych osobowych.

2. Ewidencja jest używana wyłącznie do weryfikacji zgodności przetwarzania z prawem, do monitorowania własnej działalności, zapewnienia integralności i bezpieczeństwa danych osobowych oraz na potrzeby postępowania karnego.

3. Administrator i podmiot przetwarzający na żądanie udostępniają ewidencję organowi nadzorczemu.

Artykuł 26

Współpraca z organem nadzorczym

Państwa członkowskie zapewniają, by administrator i podmiot przetwarzający współpracowali z organem nadzorczym, na jego żądanie, w ramach wykonywania jego zadań.

Artykuł 27

Ocena skutków dla ochrony danych

1. Jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele może skutkować powstaniem wysokiego ryzyka naruszenia praw i wolności osób fizycznych, państwa członkowskie zapewniają, by administrator przed przetworzeniem dokonał oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych.

2. Ocena, o której mowa w ust. 1, zawiera co najmniej ogólny opis planowanych operacji przetwarzania, ocenę ryzyka naruszenia praw i wolności osób, których dane dotyczą, środki planowane w celu rozwiązania takiego ryzyka, zabezpieczenia, środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazanie zgodności z niniejszą dyrektywą, z uwzględnieniem praw i uzasadnionych interesów osób, których dane dotyczą, i innych zainteresowanych osób.

Artykuł 28

Uprzednie konsultacje z organem nadzorczym

1. Państwa członkowskie zapewniają, by administrator lub podmiot przetwarzający przed przetwarzaniem danych osobowych, które będzie częścią mającego powstać nowego zbioru danych, skonsultowali się z organem nadzorczym, jeżeli:

a) ocena skutków dla ochrony danych, o której mowa w art. 27, wykaże, że przetwarzanie powodowałoby wysokie ryzyko naruszenia w razie niepodjęcia przez administratora środków w celu zminimalizowania tego ryzyka; lub

b) odnośny rodzaj przetwarzania – zwłaszcza z użyciem nowych technologii, mechanizmów lub procedur – stwarza poważne ryzyko naruszenia praw i wolności osób, których dane dotyczą.

2. Państwa członkowskie zapewniają przeprowadzenie konsultacji z organem nadzorczym w toku przygotowywania projektu aktu prawnego przyjmowanego przez parlament narodowy lub aktu wykonawczego opartego na takim akcie prawnym, jeżeli projekt dotyczy przetwarzania.

3. Państwa członkowskie zapewniają, by organ nadzorczy mógł sporządzać wykaz operacji przetwarzania, które wymagają uprzednich konsultacji zgodnie z ust. 1.

4. Państwa członkowskie zapewniają, by administrator przedstawiał organowi nadzorczemu ocenę wpływu na ochronę danych, o której mowa w art. 27, oraz na żądanie wszelkie inne informacje umożliwiające organowi nadzorczemu ocenę zgodności przetwarzania z przepisami, a w szczególności ocenę ryzyka w sferze ochrony danych osobowych osoby, której dane dotyczą, oraz powiązanych zabezpieczeń.

5. Państwa członkowskie zapewniają, by – jeżeli organ nadzorczy jest zdania, że zamierzone przetwarzanie, o którym mowa w ust. 1 niniejszego artykułu, stanowiłoby naruszenie przepisów przyjętych na podstawie niniejszej dyrektywy, w szczególności jeżeli administrator niedostatecznie zidentyfikował lub zminimalizował ryzyko – organ nadzorczy, w terminie do sześciu tygodni po otrzymaniu wniosku o konsultacje, przedstawił administratorowi, a w stosownym przypadku podmiotowi przetwarzającemu, pisemne zalecenia i mógł skorzystać z uprawnień, o których mowa w art. 47. Termin ten można przedłużyć o kolejny miesiąc ze względu na złożony charakter zamierzonego przetwarzania. Organ nadzorczy informuje administratora oraz, w stosownym przypadku, podmiot przetwarzający o takim przedłużeniu w terminie jednego miesiąca od otrzymania wniosku w sprawie konsultacji, z podaniem przyczyn tego opóźnienia.

Sekcja 2

Bezpieczeństwo danych osobowych

Artykuł 29

Bezpieczeństwo przetwarzania

1. Państwa członkowskie zapewniają, by – uwzględniając stan wiedzy technicznej i koszt wdrożenia oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia – administrator i podmiot przetwarzający mieli obowiązek wdrożenia odpowiednich środków technicznych i organizacyjnych dla zagwarantowania poziomu bezpieczeństwa odpowiadającego zagrożeniu, zwłaszcza jeżeli chodzi o przetwarzanie szczególnych kategorii danych osobowych, o których mowa w art. 10.

2. W odniesieniu do zautomatyzowanego przetwarzania każde państwo członkowskie zapewnia, by po ocenie ryzyka administrator lub podmiot przetwarzający wdrożyli środki, które:

a) uniemożliwią osobom nieuprawnionym dostęp do sprzętu używanego do przetwarzania (kontrola dostępu do sprzętu);

b) zapobiegną nieuprawnionemu odczytywaniu, kopiowaniu, zmienianiu lub usuwaniu nośników danych (kontrola nośników danych);

c) zapobiegną nieuprawnionemu wprowadzaniu danych osobowych oraz nieuprawnionemu oglądaniu, zmienianiu lub usuwaniu przechowywanych danych osobowych (kontrola przechowywania);

d) zapobiegną korzystaniu z systemów zautomatyzowanego przetwarzania przez osoby nieuprawnione, używające sprzętu do przesyłu danych (kontrola użytkowników);

e) zapewniają, że osoby uprawnione do korzystania z systemu zautomatyzowanego przetwarzania będą mieć dostęp wyłącznie do danych osobowych objętych posiadanym przez siebie uprawnieniem (kontrola dostępu do danych);

f) pozwolą zweryfikować i ustalić podmioty, którym dane osobowe zostały lub mogą zostać przesłane lub udostępnione za pomocą sprzętu do przesyłu danych (kontrola przesyłu danych);

g) pozwolą następczo zweryfikować i stwierdzić, które dane osobowe zostały wprowadzone do systemów zautomatyzowanego przetwarzania, kiedy i przez kogo (kontrola wprowadzania danych);

h) zapobiegną nieuprawnionemu odczytywaniu, kopiowaniu, zmienianiu lub usuwaniu danych osobowych podczas ich przekazywania lub podczas przenoszenia nośników danych (kontrola transportu);

i) zapewniają, że w razie awarii można będzie przywrócić zainstalowane systemy (odzyskiwanie);

j) zapewniają działanie funkcji systemu, zgłaszanie występujących w nich błędów (niezawodność) oraz odporność przechowywanych danych na uszkodzenia powodowane błędnym działaniem systemu (integralność).

Artykuł 30

Zgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu

1. Państwa członkowskie zapewniają, by w przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki, w miarę możliwości nie później niż 72 godzin po stwierdzeniu naruszenia, zgłosił naruszenie organowi nadzorczemu, chyba że jest mało prawdopodobne, by naruszenie to stwarzało ryzyko naruszenia praw i wolności osób fizycznych. W przypadku gdy zgłoszenie naruszenia organowi nadzorczemu nie następuje w terminie 72 godzin, towarzyszy mu uzasadnienie opóźnienia.

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

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

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

b) zawierać imię i nazwisko lub nazwę oraz dane kontaktowe inspektora ochrony danych lub innego punktu kontaktowego, od którego można uzyskać więcej informacji;

c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;

d) opisywać środki zastosowane lub proponowane przez administratora w celu naprawy naruszenia ochrony danych osobowych, w tym w stosownym przypadku zminimalizowania jego ewentualnych negatywnych skutków.

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

5. Państwa członkowskie zapewniają, by administrator dokumentował wszelkie naruszenia ochrony danych osobowych, o których mowa w ust. 1, wraz z okolicznościami naruszenia danych osobowych, jego skutkami oraz podjętymi działaniami naprawczymi. Dokumentacja ta pozwala organowi nadzorczemu na weryfikację przestrzegania niniejszego artykułu.

6. Państwa członkowskie zapewniają, by w przypadku gdy naruszenie ochrony danych osobowych dotyczy danych osobowych przesłanych przez lub do administratora innego państwa członkowskiego, informacje, o których mowa w ust. 3, zostały dostarczone bez zbędnej zwłoki administratorowi tego państwa członkowskiego.

Artykuł 31

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

1. Państwa członkowskie zapewniają, by w przypadku gdy naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadomił osobę, której dane dotyczą, o naruszeniu ochrony danych osobowych.

2. Skierowane do osoby, której dane dotyczą, zawiadomienie wskazane w ust. 1 niniejszego artykułu, opisuje jasnym i prostym językiem charakter naruszenia ochrony danych osobowych i zawiera co najmniej informacje i zalecenia, o których mowa w art. 30 ust. 3 lit. b), c) i d).

3. Skierowane do osoby, której dane dotyczą, zawiadomienie wskazane w ust. 1 niniejszego artykułu, nie jest wymagane, jeżeli spełniony został którykolwiek z następujących warunków:

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

b) administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osób, których dane dotyczą, wskazanych w ust. 1; lub

c) wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

4. Jeżeli administrator nie zawiadomił jeszcze osoby, której dane dotyczą, o naruszeniu ochrony danych, organ nadzorczy – biorąc pod uwagę prawdopodobieństwo, że naruszenie ochrony danych osobowych spowoduje wysokie ryzyko – może zażądać wystosowania przez administratora zawiadomienia, lub może stwierdzić, że spełniony został jeden z warunków, o których mowa w ust. 3.

5. Skierowane do osoby, której dane dotyczą, zawiadomienie wskazane w ust. 1 niniejszego artykułu, można opóźnić, ograniczyć lub pominąć, z zastrzeżeniem warunków i z powodów wskazanych w art. 13 ust. 3.

Sekcja 3

Inspektor ochrony danych

Artykuł 32

Wyznaczenie inspektora ochrony danych

1. Państwa członkowskie zapewniają, by administrator wyznaczył inspektora ochrony danych. Państwa członkowskie mogą zwolnić z tego obowiązku sądy i inne niezawisłe organy sądowe w ramach sprawowania przez te organy wymiaru sprawiedliwości.

2. Inspektor ochrony danych jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyki w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, o których mowa w art. 34.

3. Można wyznaczyć jednego inspektora ochrony danych dla kilku właściwych organów, uwzględniając ich strukturę organizacyjną i wielkość.

4. Państwa członkowskie zapewniają, by administrator opublikował dane kontaktowe inspektora ochrony danych i zawiadomił o nich organ nadzorczy.

Artykuł 33

Status inspektora ochrony danych

1. Państwa członkowskie zapewniają, by administrator gwarantował odpowiednie i niezwłoczne włączenie inspektora ochrony danych we wszystkie sprawach dotyczących ochrony danych osobowych.

2. Administrator wspiera inspektora ochrony danych w wypełnianiu zadań, o których mowa w art. 34, zapewniając zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania oraz zasoby niezbędne do podtrzymania jego wiedzy fachowej.

Artykuł 34

Zadania inspektora ochrony danych

Państwa członkowskie zapewniają, by administrator powierzył inspektorowi ochrony danych co najmniej następujące zadania:

a) informowanie administratora oraz pracowników zajmujących się przetwarzaniem o obowiązkach spoczywających na nich na mocy niniejszej dyrektywy oraz innych przepisów prawa Unii lub państwa członkowskiego dotyczących ochrony danych;

b) monitorowanie przestrzegania niniejszej dyrektywy, innych przepisów prawa Unii lub państwa członkowskiego dotyczących ochrony danych oraz realizowanie polityk administratora w dziedzinie ochrony danych osobowych, w tym przydział obowiązków, działania podnoszące świadomość i szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;

c) przedstawianie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie ich wykonania na mocy art. 27;

d) współpraca z organem nadzorczym;

e) pełnienie funkcji punktu kontaktowego wobec organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 28, oraz w stosownym przypadku prowadzenie konsultacji we wszelkich innych sprawach.

ROZDZIAŁ V

Przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych

Artykuł 35

Ogólne zasady przekazywania danych osobowych

1. Państwa członkowskie zapewniają, by przekazanie przez właściwe organy danych osobowych, które są przetwarzane lub mają być przetwarzane po przekazaniu do państwa trzeciego lub organizacji międzynarodowej, w tym dalsze przekazane do innego państwa trzeciego lub innej organizacji międzynarodowej, mogło nastąpić pod warunkiem zgodności z przepisami krajowymi przyjętymi na podstawie innych przepisów niniejszej dyrektywy, jedynie jeżeli spełnione zostały warunki ustanowione w niniejszym rozdziale, a mianowicie:

a) przekazanie jest niezbędne do celów, o których mowa w art. 1 ust. 1;

b) dane osobowe są przekazywane administratorowi w państwie trzecim lub organizacji międzynarodowej, który jest organem właściwym do realizacji celów, o których mowa w art. 1 ust. 1;

c) w przypadku przesyłania lub udostępniana danych od innego państwa członkowskiego to inne państwo członkowskie wyraziło na przekazanie uprzednią zgodę zgodnie ze swoim prawem krajowym;

d) Komisja wydała decyzję w przedmiocie zgodności na podstawie art. 36, lub w razie braku takiej decyzji zapewnione zostały lub istnieją odpowiednie zabezpieczenia zgodnie z art. 37, lub w razie braku decyzji w przedmiocie zgodności wydanej na podstawie art. 36 lub zabezpieczeń zgodnie z art. 37, zastosowanie mają wyjątki w szczególnych sytuacjach zgodnie z art. 38; oraz

e) w przypadku dalszego przekazania do innego państwa trzeciego lub organizacji międzynarodowej właściwy organ, który dokonał pierwotnego przekazania, lub inny właściwy organ tego samego państwa członkowskiego zezwala na dalsze przekazanie po należytym uwzględnieniu wszystkich istotnych czynników, w tym powagi czynu zabronionego, celu, w którym dane osobowe zostały pierwotnie przekazane, oraz stopnia ochrony danych osobowych w państwie trzecim lub organizacji międzynarodowej, do których dane osobowe są dalej przekazywane.

2. Państwa członkowskie zapewniają, by przekazanie danych osobowych bez uprzedniej zgody innego państwa członkowskiego, o której mowa w ust. 1 lit. c), było dozwolone wyłącznie wtedy, gdy odnośne przekazanie jest niezbędne do zapobieżenia bezpośredniemu, poważnemu zagrożeniu dla bezpieczeństwa publicznego w państwie członkowskim lub państwie trzecim bądź dla ważnych interesów państwa członkowskiego, a uprzedniej zgody nie da się uzyskać w odpowiednim terminie. Organ odpowiadający za wydanie uprzedniej zgody zostaje powiadomiony bez zbędnej zwłoki.

3. Wszystkie przepisy niniejszego rozdziału stosuje się w celu zapewnienia, by stopień ochrony osób fizycznych zapewniony niniejszą dyrektywą nie został obniżony.

Artykuł 36

Przekazywanie na podstawie decyzji stwierdzającej odpowiedni stopień ochrony

1. Państwa członkowskie zapewniają, by przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej mogło nastąpić wtedy, gdy Komisja stwierdzi, że to państwo trzecie, terytorium lub przynajmniej jeden sektor w tym państwie trzecim, lub dana organizacja międzynarodowa zapewniają odpowiedni stopień ochrony. Takie przekazanie nie wymaga specjalnego zezwolenia.

2. Oceniając, czy stopień ochrony jest odpowiedni, Komisja uwzględnia w szczególności następujące elementy:

a) praworządność, poszanowanie praw człowieka i podstawowych wolności, odpowiednie prawodawstwo – zarówno ogólne, jak i sektorowe – w tym w dziedzinie bezpieczeństwa publicznego, obrony, bezpieczeństwa narodowego i prawa karnego oraz dostępu organów publicznych do danych osobowych, a także wdrażanie takiego prawodawstwa, zasady ochrony danych osobowych, zasady dotyczące wykonywania zawodu, środki bezpieczeństwa, w tym zasady dalszego przekazywania danych osobowych do kolejnego państwa trzeciego lub innej organizacji międzynarodowej, których przestrzega się w tym państwie trzecim lub w organizacji międzynarodowej, orzecznictwo, a także skuteczne i wykonalne prawa osób, których dane dotyczą, oraz prawa osób, których dane osobowe są przekazywane, do skutecznych administracyjnych i sądowych środków zaskarżenia;

b) istnienie i skuteczne funkcjonowanie co najmniej jednego niezależnego organu nadzorczego w państwie trzecim lub organu nadzorującego organizację międzynarodową, mającego obowiązek zapewniać i egzekwować przestrzeganie przepisów o ochronie danych – w tym posiadające odpowiednie uprawnienia do egzekwowania przestrzegania przepisów – pomagać i doradzać osobom, których dane dotyczą, w toku wykonywania przysługujących im praw, a także współpracować z organami nadzorczymi państw członkowskich; oraz

c) międzynarodowe zobowiązania państwa trzeciego lub organizacji międzynarodowej lub inne obowiązki wynikające z prawnie wiążących konwencji lub aktów prawnych oraz z udziału w systemach wielostronnych lub regionalnych, w szczególności w dziedzinie ochrony danych osobowych.

3. Po dokonaniu oceny, czy stopień ochrony jest odpowiedni, w drodze aktu wykonawczego Komisja może zdecydować, że państwo trzecie, terytorium lub przynajmniej jeden określony sektor w państwie trzecim, lub organizacja międzynarodowa zapewniają odpowiedni stopień ochrony w rozumieniu ust. 2 niniejszego artykułu. W akcie wykonawczym przewiduje się mechanizm okresowego przeglądu – przynajmniej raz na cztery lata – podczas którego uwzględnia się wszelkie mające znaczenie zmiany w państwie trzecim lub organizacji międzynarodowej. W akcie wykonawczym zostaje określony terytorialny i sektorowy zakres jego zastosowania, a w stosownym przypadku wskazany zostaje organ nadzorczy lub organy nadzorcze, o których mowa w ust. 2 lit. b) niniejszego artykułu. Akt wykonawczy zostaje przyjęty zgodnie z procedurą sprawdzającą, o której mowa w art. 58 ust. 2.

4. Komisja na bieżąco monitoruje zmiany w państwach trzecich i organizacjach międzynarodowych mogące wpłynąć na obowiązywanie decyzji przyjętych na mocy ust. 3.

5. Jeżeli dostępne informacje tak wskazują, zwłaszcza po przeglądzie, o którym mowa w ust. 3 niniejszego artykułu, Komisja przyjmuje decyzję stwierdzającą, że państwo trzecie, terytorium lub przynajmniej jeden określony sektor w państwie trzecim, lub organizacja międzynarodowa przestały zapewniać odpowiedni stopień ochrony w rozumieniu ust. 2 niniejszego artykułu, i w niezbędnym zakresie uchyla, zmienia lub zawiesza decyzję, o której mowa w ust. 3 niniejszego artykułu, w drodze aktów wykonawczych bez mocy wstecznej. Takie akty wykonawcze są przyjmowane zgodnie z procedurą sprawdzającą, o której mowa w art. 58 ust. 2, lub w przypadkach wyjątkowo pilnych zgodnie z procedurą, o której mowa w art. 58 ust. 2.

W należycie uzasadnionych, szczególnie pilnych przypadkach Komisja przyjmuje zgodnie z procedurą, o której mowa w art. 58 ust. 3 akty wykonawcze mające natychmiastowe zastosowanie.

6. Komisja podejmuje konsultacje z państwem trzecim lub organizacją międzynarodową w celu naprawy sytuacji będącej przyczyną decyzji przyjętej na mocy ust. 5.

7. Państwa członkowskie zapewniają, by decyzja wydana na mocy ust. 5 nie wpływała na przekazywanie danych osobowych do danego państwa trzeciego, terytorium lub jednego lub więcej określonych sektorów w tym państwie trzecim, lub do danej organizacji międzynarodowej na mocy art. 37 i 38.

8. Komisja publikuje w *Dzienniku Urzędowym Unii Europejskiej* i na swojej stronie internetowej wykaz tych państw trzecich, terytoriów i określonych sektorów w państwie trzecim, oraz organizacji międzynarodowych, co do których przyjęła decyzję stwierdzającą odpowiedni stopień ochrony lub jego brak.

Artykuł 37

Przekazywanie z zastrzeżeniem odpowiednich zabezpieczeń

1. W razie braku decyzji na mocy art. 36 ust. 3 państwa członkowskie zapewniają, by dane osobowe mogły być przekazane do państwa trzeciego lub organizacji międzynarodowej, jeżeli:

a) w prawnie wiążącym akcie wprowadzono odpowiednie zabezpieczenia ochrony danych osobowych; lub

b) administrator ocenił wszystkie okoliczności związane z przekazaniem danych osobowych i stwierdził, że istnieją odpowiednie zabezpieczenia ochrony danych osobowych.

2. Administrator informuje organ nadzorczy o kategoriach przekazań, o których mowa w ust. 1 lit. b).

3. Jeżeli przekazanie odbywa się na podstawie ust. 1 lit. b), musi być udokumentowane, a dokumentacja, w tym data i godzina przekazania, informacje o właściwym organie odbierającym, uzasadnienie przekazania oraz przekazane dane osobowe, musi zostać udostępniona na żądanie organowi nadzorczemu.

Artykuł 38

Wyjątki w szczególnych sytuacjach

1. W razie braku decyzji stwierdzającej odpowiedni stopień ochrony na mocy art. 36 lub braku odpowiednich zabezpieczeń określonych w art. 37 państwa członkowskie zapewniają, by przekazanie lub określona kategoria przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej mogły nastąpić wyłącznie pod warunkiem, że przekazanie jest niezbędne:

a) w celu ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby;

b) w celu zabezpieczenia uzasadnionych interesów osoby, której dane dotyczą, jeżeli prawo państwa członkowskiego przekazującego dane osobowe tak stanowi;

c) dla zapobieżenia bezpośredniemu, poważnemu ryzyku naruszenia bezpieczeństwa publicznego państwa członkowskiego lub państwa trzeciego;

d) w indywidualnym przypadku do celów, o których mowa w art. 1 ust. 1; lub

e) w indywidualnym przypadku, dla ustalenia, dochodzenia lub obrony roszczeń w związku z celami określonymi w art. 1 ust. 1.

2. Danych osobowych nie przekazuje się, jeżeli właściwy organ przekazujący stwierdzi, że podstawowe prawa i wolności konkretnej osoby, której dane dotyczą, są nadrzędne wobec interesu publicznego przemawiającego za przekazaniem, o którym mowa w ust. 1 lit. d) i e).

3. Jeżeli przekazanie odbywa się na podstawie ust. 1, musi być udokumentowane, a dokumentacja, w tym data i godzina przekazania, informacje o właściwym organie odbierającym, uzasadnienie przekazania oraz przekazane dane osobowe, musi zostać udostępniona na żądanie organowi nadzorczemu.

Artykuł 39

Przekazywanie danych osobowych odbiorcom mającym siedzibę w państwach trzecich

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

a) przekazanie jest ściśle niezbędne do wykonania zadania właściwego organu przekazującego zgodnie z prawem Unii lub prawem państwa członkowskiego do celów, o których mowa w art. 1 ust. 1;

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

c) właściwy organ przekazujący uznaje, że przekazanie organowi właściwemu do celów, o których mowa w art. 1 ust. 1, w państwie trzecim byłoby nieskuteczne lub niewłaściwe, w szczególności dlatego, że przekazanie nie może nastąpić w odpowiednim terminie;

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

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

2. Umowa międzynarodowa, o której mowa w ust. 1, oznacza jakąkolwiek dwustronną lub wielostronną umowę międzynarodową obowiązującą między państwami członkowskimi a państwami trzecimi dotyczącą współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej.

3. Właściwy organ przekazujący informuje organ nadzorczy o przekazaniach na mocy niniejszego artykułu.

4. Jeżeli przekazanie odbywa się na podstawie ust. 1, musi być udokumentowane.

Artykuł 40

Międzynarodowa współpraca na rzecz ochrony danych osobowych

Komisja i państwa członkowskie podejmują wobec państw trzecich i organizacji międzynarodowych odpowiednie działania na rzecz:

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

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

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

d) upowszechnienia wymiany i dokumentowania przepisów i praktyk w dziedzinie ochrony danych osobowych, w tym dotyczących kolizji jurysdykcyjnych z państwami trzecimi.

ROZDZIAŁ VI

Niezależne organy nadzorcze

Sekcja 1

Niezależny status

Artykuł 41

Organ nadzorczy

1. Państwo członkowskie zapewnia, by za monitorowanie stosowania niniejszej dyrektywy odpowiadał co najmniej jeden niezależny organ publiczny, dla ochrony podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem oraz ułatwiania swobodnego przepływu danych osobowych w Unii.

2. Każdy organ nadzorczy przyczynia się do spójnego stosowania niniejszej dyrektywy w całej Unii. W tym celu organy nadzorcze współpracują ze sobą i z Komisją zgodnie z rozdziałem VII.

3. Państwa członkowskie mogą zapewnić, by organem nadzorczym, o którym mowa w niniejszej dyrektywie i na którym spoczywa obowiązek realizacji zadań organu nadzorczego mającego powstać na mocy ust. 1, mógł zostać organ nadzorczy ustanowiony na mocy rozporządzenia (UE) 2016/… (*).

4. Jeżeli w państwie członkowskim ustanowiono więcej niż jeden organ nadzorczy, państwo to wyznacza organ nadzorczy, który ma reprezentować te organy w Europejskiej Radzie Ochrony Danych, o której mowa w art. 51.

Artykuł 42

Niezależność

1. Państwa członkowskie zapewniają, by każdy organ nadzorczy podczas wypełniania swoich zadań i wykonywania swoich uprawnień zgodnie z niniejszą dyrektywą działał w sposób w pełni niezależny.

2. Państwa członkowskie zapewniają, by członek lub członkowie ich organów nadzorczych podczas wypełniania swoich zadań i wykonywania swoich uprawnień zgodnie z niniejszą dyrektywą pozostawali wolni od bezpośrednich i pośrednich wpływów zewnętrznych, nie zwracali się do nikogo o instrukcje ani ich od nikogo nie przyjmowali.

3. Członkowie organów nadzorczych państw członkowskich powstrzymują się od wszelkich czynności sprzecznych ze swoimi obowiązkami i podczas swojej kadencji nie podejmują żadnego zajęcia zarobkowego ani niezarobkowego sprzecznego z tymi obowiązkami.

4. Państwa członkowskie zapewniają, by każdy organ nadzorczy dysponował zasobami kadrowymi, technicznymi i finansowymi, pomieszczeniami i infrastrukturą niezbędną do skutecznego wypełniania swoich zadań i wykonywania swoich uprawnień, w tym w kontekście wzajemnej pomocy, współpracy i uczestnictwa w pracach Europejskiej Rady Ochrony Danych.

5. Państwa członkowskie zapewniają, by każdy organ nadzorczy wybierał i posiadał własny personel, działający pod wyłącznym kierownictwem członka lub członków danego organu nadzorczego.

6. Państwa członkowskie zapewniają, by ich organy nadzorcze podlegały kontroli finansowej w sposób nienaruszający ich niezależności, oraz by dysponowały odrębnym, publicznym budżetem rocznym, który może być częścią ogólnego budżetu państwowego lub krajowego.

Artykuł 43

Ogólne warunki dotyczące członków organu nadzorczego

1. Państwa członkowskie zapewniają, by każdy członek organu nadzorczego był powołany na drodze przejrzystej procedurze przez

— parlament,

— rząd,

— głowę państwa, lub

— niezależny organ uprawniony do powoływania członków organu nadzorczego na podstawie prawa państwa członkowskiego.

(*) Rozporządzenie w st 5419/16.

2. Każdy członek musi posiadać kwalifikacje, doświadczenie i umiejętności, w szczególności w dziedzinie ochrony danych osobowych, potrzebne do wypełniania swoich obowiązków i wykonywania swoich uprawnień.

3. W razie upływu kadencji, rezygnacji lub przymusowego pozbawienia funkcji członek organu przestaje pełnić swoje obowiązki zgodnie z prawem danego państwa członkowskiego.

4. Członek zostaje odwołany ze stanowiska tylko w przypadku, gdy dopuścił się poważnego uchybienia lub przestał spełniać warunki potrzebne do wypełniania obowiązków.

Artykuł 44

Zasady ustanawiania organu nadzorczego

1. Każde państwo członkowskie określa w swoich przepisach prawnych wszystkie poniższe kwestie:

a) ustanowienie każdego z organów nadzorczych;

b) kwalifikacje i warunki wyboru wymagane do powołania na stanowisko członka swych organów nadzorczych;

c) zasady i procedury powołania członka lub członków każdego z organów nadzorczych;

d) długość kadencji członka lub członków każdego z organów nadzorczych, nie krótszy niż cztery lata, z wyjątkiem pierwszej kadencji po … *[Dz.U proszę wstawić datę wejścia w życie niniejszej dyrektywy]*, która to kadencja może częściowo trwać krócej, jeżeli jest to niezbędne dla ochrony niezależności organu nadzorczego w drodze procedury stopniowej wymiany członków;

e) możliwość ponownego powołania członka lub członków każdego z organów nadzorczych, oraz liczbę kadencji;

f) zasady regulujące obowiązki członka lub członków oraz personelu każdego z organów nadzorczych, zakaz podejmowania sprzecznych z nimi działań, zajęć i czerpania korzyści, w trakcie kadencji oraz po jej zakończeniu, a także przepisy regulujące ustanie stosunku pracy.

2. Członek lub członkowie oraz personel każdego z organów nadzorczych podlegają zgodnie z prawem Unii lub prawem państwa członkowskiego obowiązkowi dochowania tajemnicy służbowej – w trakcie kadencji oraz po jej zakończeniu – w odniesieniu do wszelkich poufnych informacji, które uzyskali w toku wypełniania zadań lub wykonywania swoich uprawnień. Obowiązek dochowania tajemnicy służbowej w trakcie kadencji dotyczy zwłaszcza sytuacji, w których osoby fizyczne zgłaszają naruszenia niniejszej dyrektywy.

Sekcja 2

Właściwość, zadania I uprawnienia

Artykuł 45

Właściwość

1. Państwa członkowskie zapewniają, by każdy organ nadzorczy był właściwy do wypełniania przeznaczonych mu zadań i wykonywania uprawnień powierzonych mu zgodnie z niniejszą dyrektywą na terytorium swego państwa członkowskiego.

2. Państwa członkowskie zapewniają, by żaden organ nadzorczy nie był właściwy do nadzorowania operacji przetwarzania dokonywanych przez sądy w toku sprawowania przez nie wymiaru sprawiedliwości. Państwa członkowskie mogą postanowić, że organ nadzorczy nie jest właściwy do nadzorowania operacji przetwarzania dokonywanych przez inne niezależne organy wymiaru sprawiedliwości w ramach sprawowania przez nie wymiaru sprawiedliwości.

Artykuł 46

Zadania

1. Państwa członkowskie zapewniają, by na ich terytorium każdy organ nadzorczy:

a) monitorował i egzekwował stosowanie przepisów przyjętych na podstawie niniejszej dyrektywy oraz jej aktów wykonawczych;

b) upowszechniał w społeczeństwie wiedzę o ryzyku, przepisach, zabezpieczeniach i prawach związanych z przetwarzaniem oraz rozumienie tych zjawisk;

c) doradzał, zgodnie z prawem państwa członkowskiego, parlamentowi narodowemu, rządowi oraz innym instytucjom i organom w sprawie ustawowych i administracyjnych środków ochrony praw i wolności osób fizycznych w związku z przetwarzaniem;

d) upowszechniał wśród administratorów i podmiotów przetwarzających wiedzę o obowiązkach spoczywających na nich na mocy niniejszej dyrektywy;

e) udzielał osobie, której dane dotyczą, na jej żądanie informacji o wykonywaniu praw przysługujących jej na mocy niniejszej dyrektywy, a w stosownym przypadku współpracował w tym celu z organami nadzorczymi innych państw członkowskich;

f) rozpatrywał skargi wniesione przez osobę, której dane dotyczą, lub przez podmiot, organizację lub zrzeszenia zgodnie z art. 55, w odpowiednim zakresie prowadził postępowanie w przedmiocie tych skarg i w rozsądnym terminie informował skarżącego o postępach i wynikach takiego postępowania, w szczególności jeżeli niezbędne jest dalsze prowadzenie postępowania lub koordynacja działań z innym organem nadzorczym;

g) sprawdzał zgodność przetwarzania z prawem na mocy art. 17 oraz informował osobę, której dane dotyczą, w rozsądnym terminie o wynikach tej kontroli zgodnie z art. 17 ust. 3 lub o powodach jej nieprzeprowadzenia;

h) współpracował z innymi organami nadzorczymi, w tym dzielił się informacjami oraz świadczył wzajemną pomoc w celu zapewnienia spójnego stosowania i egzekwowania niniejszej dyrektywy;

i) prowadził postępowania w sprawie stosowania niniejszej dyrektywy, w tym na podstawie informacji otrzymanych od innego organu nadzorczego lub innego organu publicznego;

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

k) pełnił funkcje konsultacyjne, o których mowa w art. 28, co do operacji przetwarzania; oraz

l) brał udział w pracach Europejskiej Rady Ochrony Danych.

2. Każdy organ nadzorczy ułatwia wnoszenie skarg, o których mowa w ust. 1 lit. f), za pomocą takich środków jak gotowy formularz skargi, który można wypełnić elektronicznie, co nie wyklucza innych sposobów komunikacji.

3. Każdy organ nadzorczy wypełnia zadania na rzecz osoby, której dane dotyczą, i inspektora ochrony danych bezpłatnie.

4. Jeżeli żądanie jest w sposób oczywisty nieuzasadnione lub nadmierne, zwłaszcza ze względu na swą powtarzalność, organ nadzorczy może pobrać rozsądną opłatę wynikającą z kosztów administracyjnych lub może odmówić podjęcia działań w związku z żądaniem. Obowiązek wykazania, że żądanie jest w sposób oczywisty nieuzasadnione lub nadmierne, spoczywa na organie nadzorczym.

Artykuł 47

Uprawnienia

1. Państwa członkowskie zapewniają, by każdy organ nadzorczy posiadał skuteczne uprawnienia w zakresie prowadzenia postępowań. Uprawnienia te obejmują co najmniej uprawnienie do uzyskania od administratora i podmiotu przetwarzającego dostępu do wszelkich przetwarzanych danych osobowych i wszelkich informacji niezbędnych mu do wypełnienia zadań.

2. Państwa członkowskie zapewniają, by każdy organ nadzorczy posiadał skuteczne uprawnienia naprawcze, przykładowo takie jak:

a) wydawanie ostrzeżeń administratorowi lub podmiotowi przetwarzającemu, zgodnie z którymi planowane operacje przetwarzania mogą skutkować naruszeniem przepisów przyjętych na podstawie niniejszej dyrektywy;

b) nakazanie administratorowi lub podmiotowi przetwarzającemu dostosowania operacji do przepisów przyjętych na podstawie niniejszej dyrektywy, w razie potrzeby w konkretny sposób i w konkretnym terminie, zwłaszcza poprzez nakazanie sprostowania lub usunięcia danych osobowych lub ograniczenia ich przetwarzania zgodnie z art. 16;

c) wprowadzenie czasowych lub stałych ograniczeń przetwarzania, w tym zakazu przetwarzania.

3. Państwa członkowskie zapewniają, by każdy organ nadzorczy posiadał skuteczne uprawnienia doradcze pozwalające przedstawić administratorowi zalecenia zgodnie z procedurą uprzednich konsultacji, o której mowa w art. 28, oraz by z własnej inicjatywy lub na wniosek mógł wydawać opinie skierowane do parlamentu narodowego, rządu lub, zgodnie z jego prawem krajowym, innych instytucji i organów oraz do społeczeństwa we wszelkich sprawach związanych z ochroną danych osobowych.

4. Wykonywanie uprawnień powierzonych organowi nadzorczemu na mocy niniejszego artykułu podlega odpowiednim gwarancjom, w tym prawu do skutecznego środka prawnego przed sądem i rzetelnego procesu, określonym w prawie Unii i prawie państwa członkowskiego zgodnie z Kartą.

5. Państwa członkowskie zapewniają, by każdy organ nadzorczy miał uprawnienie do wniesienia do organów sądowych sprawy dotyczącej naruszenia przepisów przyjętych na podstawie niniejszej dyrektywy oraz, w stosownym przypadku, do wszczęcia lub udziału w inny sposób w postępowaniu sądowym mającym na celu egzekwowanie przepisów przyjętych na podstawie niniejszej dyrektywy.

Artykuł 48

Zgłaszanie naruszeń

Państwa członkowskie zapewniają, by właściwe organy wprowadziły skuteczne mechanizmy zachęcania do poufnego zgłaszania naruszeń niniejszej dyrektywy.

Artykuł 49

Sprawozdania z działalności

Każdy organ nadzorczy sporządza roczne sprawozdanie ze swojej działalności, w którym może wyszczególnić rodzaje zgłoszonych mu naruszeń i rodzaje nałożonych kar. Sprawozdania są przekazywane parlamentowi narodowemu, rządowi i innym organom wskazanym prawem krajowym. Są one udostępniane opinii publicznej, Komisji oraz Europejskiej Radzie Ochrony Danych.

ROZDZIAŁ VII

Współpraca

Artykuł 50

Wzajemna pomoc

1. Państwa członkowskie zapewniają, by ich organy nadzorcze przekazywały sobie stosowne informacje i świadczyły sobie wzajemną pomoc w celu spójnego wdrażania i stosowania niniejszej dyrektywy oraz wprowadziły środki na rzecz skutecznej wzajemnej współpracy. Wzajemna pomoc obejmuje w szczególności wnioski o udzielenie informacji oraz środki nadzorcze, takie jak wnioski o przeprowadzenie konsultacji, kontroli i postępowań.

2. Państwa członkowskie zapewniają, by każdy organ nadzorczy podjął wszelkie odpowiednie środki, by odpowiedzi na wniosek innego organu nadzorczego udzielić bez zbędnej zwłoki, nie później niż w terminie jednego miesiąca po otrzymaniu wniosku. Środki takie mogą obejmować w szczególności przekazanie odpowiednich informacji o przebiegu postępowania.

3. Wnioski o pomoc zawierają wszelkie niezbędne informacje, w tym cel i uzasadnienie wniosku. Uzyskane informacje są wykorzystywane wyłącznie do celu, w którym o nie wystąpiono.

4. Organ nadzorczy, do którego skierowano wniosek o pomoc, nie może odmówić jego wykonania, chyba że:

a) nie jest organem właściwym w zakresie przedmiotu wniosku lub środków, o których wykonanie wystąpiono; lub

b) wykonanie wniosku naruszyłoby niniejszą dyrektywę lub prawo Unii lub prawo państwa członkowskiego, któremu podlega organ nadzorczy, który otrzymał wniosek.

5. Organ nadzorczy, do którego skierowano wniosek, informuje organ nadzorczy, od którego wniosek pochodzi, o wynikach lub, w razie potrzeby, o postępach lub środkach podjętych w celu udzielenia odpowiedzi na ten wniosek. Organ nadzorczy, do którego skierowano wniosek o pomoc, przedstawia powody odmowy nieuwzględnienia wniosku zgodnie z ust. 4.

6. Informacje, o które zwróciły się inne organy nadzorcze, organ nadzorczy, do którego skierowano wniosek o pomoc, co do zasady przekazuje drogą elektroniczną w standardowym formacie.

7. Organy nadzorcze, do których skierowano wniosek o pomoc, nie pobierają opłaty za działania podejmowane w związku z wnioskiem o wzajemną pomoc. Organy nadzorcze mogą uzgodnić zasady wzajemnej rekompensaty wydatków poniesionych w wyniku świadczenia wzajemnej pomocy w wyjątkowych okolicznościach.

8. Komisja może określić w drodze aktów wykonawczych formułę i procedury wzajemnej pomocy, o których mowa w niniejszym artykule, oraz zasady wymiany informacji drogą elektroniczną między organami nadzorczymi oraz między organami nadzorczymi a Europejską Radą Ochrony Danych. Akty wykonawcze są przyjmowane zgodnie z procedurą sprawdzającą, o której mowa w art. 58 ust. 2.

Artykuł 51

Zadania Europejskiej Rady Ochrony Danych

1. Europejska Rada Ochrony Danych ustanowiona rozporządzeniem (UE) 2016/… (*) wypełnia następujące zadania w odniesieniu do przetwarzania wchodzącego w zakres zastosowania niniejszej dyrektywy:

a) doradza Komisji w każdej sprawie związanej z ochroną danych osobowych w Unii, w tym w sprawie wszelkich proponowanych zmian do niniejszej dyrektywy;

b) z własnej inicjatywy, na wniosek jednego ze swoich członków lub na wniosek Komisji bada wszelkie kwestie dotyczące stosowania niniejszej dyrektywy i opracowuje wytyczne, zalecenia i najlepsze praktyki w celu wspierania spójnego stosowania niniejszej dyrektywy;

c) opracowuje wytyczne dla organów nadzorczych w sprawie stosowania środków, o których mowa w art. 47 ust. 1 i 3;

d) opracowuje wytyczne, zalecenia i najlepsze praktyki, o których mowa w lit. b) niniejszego ustępu, określające naruszenia ochrony danych osobowych i zbędną zwłokę w rozumieniu art. 30 ust. 1 i 2 oraz poszczególne okoliczności, w jakich administrator lub podmiot przetwarzający mają obowiązek zgłosić naruszenie ochrony danych osobowych;

e) opracowuje wytyczne, zalecenia i najlepsze praktyki zgodnie z lit. b) niniejszego ustępu, określające okoliczności, w jakich naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych, o których mowa w art. 31 ust. 1;

f) dokonuje przeglądu praktycznego stosowania wytycznych, zaleceń i najlepszych praktyk, o których mowa w lit. b) i c);

g) przedstawia Komisji opinię na potrzeby oceny, czy stopień ochrony w państwie trzecim, na terytorium lub jednym lub więcej określonym sektorze państwa trzeciego lub w organizacji międzynarodowej jest odpowiedni, w tym na potrzeby oceny, czy takie państwo trzecie, terytorium, określony sektor lub organizacja międzynarodowa nie przestały zapewniać odpowiedniego stopnia ochrony.

(*) Rozporządzenie w st 5419/16.

h) wspiera współpracę oraz skuteczną dwustronną i wielostronną wymianę informacji i najlepszych praktyk między organami nadzorczymi;

i) wspiera wspólne programy szkoleń oraz ułatwia wymianę personelu między organami nadzorczymi, a w stosownym przypadku z organami nadzorczymi państw trzecich lub organizacji międzynarodowych;

j) wspiera wymianę wiedzy i dokumentów na temat prawa i praktyki w dziedzinie ochrony danych z organami nadzorczymi odpowiedzialnymi za ochronę danych na świecie.

W odniesieniu do akapitu pierwszego lit. g) Komisja udostępnia Europejskiej Radzie Ochrony Danych wszelką niezbędną dokumentację, w tym korespondencję z rządem państwa trzeciego, terytorium lub określonym sektorem w tym państwie trzecim lub organizacją międzynarodową.

2. Jeżeli Komisja zwraca się do Europejskiej Rady Ochrony Danych z wnioskiem o opinię, może wskazać termin udzielenia odpowiedzi uwzględniając pilność sprawy.

3. Europejska Rada Ochrony Danych przekazuje swoje opinie, wytyczne, zalecenia i najlepsze praktyki Komisji i komitetowi, o którym mowa w art. 58 ust. 1, oraz podaje je do wiadomości publicznej.

4. Komisja informuje Europejską Radę Ochrony Danych o swoich działaniach w odniesieniu do opinii, wytycznych, zaleceń i najlepszych praktyk opracowanych przez Europejską Radę Ochrony Danych.

ROZDZIAŁ VIII

Środki ochrony prawnej, odpowiedzialność prawna I sankcje

Artykuł 52

Prawo do wniesienia skargi do organu nadzorczego

1. Z zastrzeżeniem innych środków administracyjnych lub środków prawnych przed sądem, państwa członkowskie zapewniają, by każda osoba, której dane dotyczą, miała prawo wnieść skargę do jednego organu nadzorczego, jeżeli sądzi, że dotyczące jej przetwarzanie danych osobowych narusza przepisy przyjęte na podstawie niniejszej dyrektywy.

2. Państwa członkowskie zapewniają, by – jeżeli skarga nie zostaje wniesiona do organu nadzorczego właściwego zgodnie z art. 45 ust. 1 – organ nadzorczy, do którego wniesiono skargę, miał obowiązek przekazania jej bez zbędnej zwłoki właściwemu organowi nadzorczemu. O przekazaniu skargi poinformowana zostaje osoba, której dane dotyczą.

3. Państwa członkowskie zapewniają, by organ nadzorczy, do którego wniesiono skargę, udzielił osobie, której dane dotyczą, dalszej pomocy na jej wniosek.

4. Właściwy organ nadzorczy informuje osobę, której dane dotyczą, o postępach i wyniku skargi, w tym o możliwości wniesienia sądowego środka ochrony prawnej na mocy art. 53.

Artykuł 53

Prawo do skutecznego środka prawnego przed sądem od decyzji organu nadzorczego

1. Z zastrzeżeniem innych środków administracyjnych lub pozasądowych środków ochrony prawnej państwa członkowskie stanowią prawem, że każda osoba fizyczna lub prawna ma prawo do skutecznego środka prawnego przed sądem od prawnie wiążącej decyzji organu nadzorczego, która jej dotyczy.

2. Z zastrzeżeniem innych środków administracyjnych lub pozasądowych środków ochrony prawnej każda osoba, której dane dotyczą, ma prawo do skutecznego środka prawnego przed sądem, jeżeli organ nadzorczy właściwy zgodnie z art. 45 ust. 1 nie rozpatrzył skargi lub nie poinformował osoby, której dane dotyczą, w terminie trzech miesięcy o postępach lub wyniku rozpatrzenia skargi wniesionej na mocy art. 52.

3. Państwa członkowskie zapewniają, by postępowanie przeciwko organowi nadzorczemu zostało wszczęte przed sądem państwa członkowskiego, w którym organ nadzorczy ma siedzibę.

Artykuł 54

Prawo do skutecznego środka prawnego przed sądem przeciwko administratorowi lub podmiotowi przetwarzającemu

Z zastrzeżeniem dostępnych środków administracyjnych lub pozasądowych środków ochrony prawnej, w tym prawa do wniesienia skargi do organu nadzorczego na mocy art. 52, państwa członkowskie zapewniają osobie, której dane dotyczą, prawo do skutecznego środka prawnego przed sądem, jeżeli osoba ta uważa, iż jej prawa ustanowione w przepisach przyjętych na podstawie niniejszej dyrektywy zostały naruszone w skutek przetwarzania jej danych osobowych w sposób niezgodny z tymi przepisami.

Artykuł 55

Reprezentowanie osób, których dane dotyczą

Państwa członkowskie, zgodnie z prawem procesowym państwa członkowskiego, zapewniają osobie, której dane dotyczą, prawo do umocowania organu, organizacji lub zrzeszenia o charakterze niezarobkowym, które zostały należycie ustanowione zgodnie z prawem państwa członkowskiego, mają statutowo na celu interes publiczny i działają w dziedzinie ochrony praw i wolności osób, których dane dotyczą, w związku z ochroną ich danych osobowych, do wniesienia w jej imieniu skargi oraz wykonywanie w jej imieniu praw, o których mowa w art. 52, 53 i 54.

Artykuł 56

Prawo do odszkodowania

Państwa członkowskie zapewniają każdej osobie, która poniosła szkodę majątkową lub niemajątkową w wyniku operacji przetwarzania niezgodnej z prawem lub w wyniku czynności naruszającej przepisy przyjęte na podstawie niniejszej dyrektywy, prawo otrzymania od administratora lub innego organu właściwego w świetle prawa państwa członkowskiego odszkodowania za poniesioną szkodę.

Artykuł 57

Sankcje

Państwa członkowskie przyjmują przepisy określające sankcje za naruszenie przepisów przyjętych na podstawie niniejszej dyrektywy i podejmują wszelkie środki niezbędne do ich wykonania. Sankcje te muszą być skuteczne, proporcjonalne i odstraszające.

ROZDZIAŁ IX

Akty wykonawcze

Artykuł 58

Procedura komitetowa

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

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

3. W przypadku odesłania do niniejszego ustępu zastosowanie ma art. 8 rozporządzenia (UE) nr 182/2011 w związku z jego art. 5.

ROZDZIAŁ X

Przepisy końcowe

Artykuł 59

Uchylenie decyzji ramowej 2008/977/WSiSW

1. Uchyla się decyzję ramową Rady 2008/977/WSiSW ze skutkiem od dnia … *[dwa lata od dnia wejścia w życie].*

2. Odesłania do uchylonej decyzji, o której mowa w ust. 1, należy interpretować jako odesłania do niniejszej dyrektywy.

(*) Rozporządzenie w st 5419/16.

Artykuł 60

Uprzednio przyjęte akty prawne Unii

Dyrektywa nie wpływa na szczegółowe przepisy o ochronie danych osobowych w aktach prawnych Unii, które weszły w życie do dnia … *[data wejścia w życie niniejszej dyrektywy]* w dziedzinie współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej, które regulują przetwarzanie między państwami członkowskimi oraz dostęp wyznaczonych organów państw członkowskich do systemów informacyjnych ustanowionych na mocy traktatów w ramach zakresu zastosowania niniejszej dyrektywy.

Artykuł 61

Stosunek do uprzednio zawartych umów międzynarodowych o współpracy wymiarów sprawiedliwości w sprawach karnych oraz o współpracy policyjnej

Umowy międzynarodowe, które przewidują przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych i które zostały zawarte przez państwa członkowskie przed … *[data wejścia niniejszej dyrektywy w życie]* i które są zgodne z prawem Unii mającym zastosowanie przed dniem … *[data wejścia niniejszej dyrektywy w życie]*, pozostają w mocy do czasu ich zmiany, zastąpienia lub uchylenia.

Artykuł 62

Sprawozdanie Komisji

1. Do dnia … *[6 lat po wejściu w życie niniejszej dyrektywy]*, a następnie co cztery lata Komisja przedkłada Parlamentowi Europejskiemu i Radzie sprawozdanie z oceny i przeglądu niniejszej dyrektywy. Sprawozdania te są publikowane.

2. W ramach tych ocen i przeglądów, o których mowa w ust. 1, Komisja analizuje w szczególności stosowanie i funkcjonowanie rozdziału V w sprawie przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych, ze szczególnym uwzględnieniem decyzji przyjętych na mocy art. 36 ust. 3 i art. 39.

3. Na potrzeby ust. 1 i 2, Komisja może wystąpić do państw członkowskich i organów nadzorczych o udzielenie informacji.

4. Dokonując ocen i przeglądów, o których mowa w ust. 1 i 2, Komisja uwzględnia stanowiska i ustalenia Parlamentu Europejskiego, Rady oraz do innych właściwych podmiotów lub źródeł.

5. Komisja może przedkładać, w razie konieczności, odpowiednie wnioski w celu zmiany niniejszej dyrektywy, w szczególności z uwzględnieniem rozwoju wiedzy informatycznej oraz rozwoju społeczeństwa informacyjnego.

6. Do dnia … *[trzy lata po wejściu niniejszej dyrektywy w życie]* Komisja dokonuje przeglądu innych przyjętych przez Unię aktów regulujących przetwarzanie przez właściwe organy do celów określonych w art. 1 ust. 1, w tym aktów, o których mowa w art. 60, w celu oceny konieczności dostosowania ich do niniejszej dyrektywy, i w razie potrzeby przedstawia niezbędne propozycje zmiany takich aktów dla zapewnienia spójnego podejścia do ochrony danych osobowych wchodzących w zakres zastosowania niniejszej dyrektywy.

Artykuł 63

Transpozycja

1. Państwa członkowskie przyjmują i publikują do dnia … *[data/dwa lata po dniu wejścia w życie niniejszej dyrektywy]* przepisy ustawowe, wykonawcze i administracyjne niezbędne do wykonania niniejszej dyrektywy. Tekst tych przepisów niezwłocznie przekazują Komisji. Państwa członkowskie stosują te przepisy od dnia … *[data/dwa lata po dniu wejścia w życie niniejszej dyrektywy]*.

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. W drodze wyjątku od ust. 1 państwo członkowskie może postanowić, że wyjątkowo, jeżeli wymaga to niewspółmiernie dużego wysiłku, zautomatyzowane systemy przetwarzania utworzone przed … *[dzień wejścia w życie niniejszej dyrektywy]* zostają dostosowane do art. 25 ust. 1 do dnia … *[7 lat od dnia jej wejścia w życie niniejszej dyrektywy]*.

3. W drodze wyjątku od ust. 1 i 2 niniejszego artykułu, w wyjątkowych okolicznościach państwo członkowskie może dostosować do art. 25 ust. 1 dany zautomatyzowany system przetwarzania, o którym mowa w ust. 2 niniejszego artykułu, w konkretnym terminie dłuższym niż termin, o którym mowa w ust. 2 niniejszego artykułu, jeżeli inaczej nastąpiłyby poważne problemy w funkcjonowaniu tego systemu. Dane państwo członkowskie informuje Komisję o przyczynach tych poważnych problemów i uzasadnia konkretny termin, w którym ma dostosować dany zautomatyzowany system przetwarzania do art. 25 ust. 1. Ten konkretny termin w żadnym wypadku nie upływa później niż …*[10 lat po dniu wejścia w życie niniejszej dyrektywy]*.

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

Artykuł 64

Wejście w życie

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

Artykuł 65

Adresaci

Niniejsza dyrektywa jest skierowana do państw członkowskich.

Sporządzono w …

W imieniu Parlamentu Europejskiego	*W imieniu Rady*
[…] […]	[…] […]
Przewodniczący	*Przewodniczący*

Uzasadnienie Rady: Stanowisko Rady (UE) nr 5/2016 w pierwszym czytaniu w sprawie przyjęcia dyrektywy Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylającej decyzję ramową Rady 2008/977/WSiSW

(2016/C 158/02)

I. WPROWADZENIE

W dniu 25 stycznia 2012 r. Komisja zaproponowała całościowy pakiet poświęcony ochronie danych. Na pakiet składają się:

— wniosek w sprawie ogólnego rozporządzenia o ochronie danych (dalej „proponowane rozporządzenie"), które to rozporządzenie ma zastąpić dyrektywę z roku 1995 o ochronie danych (poprzednio filar pierwszy);

— dyrektywa w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych (dalej „proponowana dyrektywa") ([1]), która to dyrektywa ma zastąpić decyzję ramową z roku 2008 o ochronie danych (poprzednio filar trzeci).

W marcu 2014 r. Parlament Europejski zaopiniował proponowaną dyrektywę ([2]).

W dniu 9 października 2015 r. Rada uzgodniła podejście ogólne ([3]), dając tym samym prezydencji mandat do rozpoczęcia rozmów trójstronnych z Parlamentem Europejskim.

W dniu 17 grudnia 2015 r. Parlament Europejski (na szczeblu Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych), a dzień później Rada (na szczeblu Komitetu Stałych Przedstawicieli) potwierdziły porozumienie co do kompromisowego tekstu powstałego podczas negocjacji trójstronnych.

W dniu 12 lutego Rada wypracowała porozumienie polityczne w sprawie proponowanej dyrektywy ([4]). W dniu 8 kwietnia 2016 r. przyjęła stanowisko w pierwszym czytaniu (dalej „stanowisko Rady"). Stanowisko to w pełni odpowiada kompromisowemu tekstowi dyrektywy uzgodnionemu w nieformalnych negocjacjach między Radą a Parlamentem Europejskim.

Komitet Regionów wydał opinię w sprawie proponowanej dyrektywy (Dz.U. 391 z 18.12.2012, s. 127).

Przeprowadzono też konsultacje z Europejskim Inspektorem Ochrony Danych, który pierwszą opinię przedstawił w roku 2012 (Dz.U. C 192 z 30.6.2012, s.7), a w roku 2015 – kolejną (Dz.U. C 301 z 12.9.2015, s. 1–8).

W dniu 1 października 2012 r. swoją opinię przedstawiła Agencja Praw Podstawowych.

II. CEL WNIOSKU

Proponowana dyrektywa ma zapewnić skuteczną współpracę wymiarów sprawiedliwości w sprawach karnych i współpracę policyjną oraz ułatwić wymianę danych osobowych między właściwymi organami państw członkowskich. Równocześnie ma zagwarantować osobom fizycznym spójną, wysoką ochronę ich danych osobowych. W odróżnieniu od ramowej decyzji Rady 2008/977/WSiSW, którą proponowana dyrektywa ma zastąpić, obecny projekt obejmuje też wewnątrzkrajowe przetwarzanie danych osobowych.

Artykuł 16 ust. 2 Traktatu o funkcjonowaniu Unii Europejskiej daje nową, szczegółową podstawę prawną do przyjmowania zasad ochrony danych osobowych. Podstawa ta znajduje zastosowanie m.in. właśnie w przetwarzaniu danych osobowych w ramach współpracy wymiarów sprawiedliwości w sprawach karnych oraz współpracy policyjnej.

([1]) Dok. 5833/12.
([2]) Dok. 7428/14.
([3]) Dok. 12555/15.
([4]) Dok. 5463/16.

III. ANALIZA STANOWISKA RADY Z PIERWSZEGO CZYTANIA

A. Uwagi ogólne

Proponowana dyrektywa jest częścią pakietu poświęconego ochronie danych. Drugim elementem pakietu jest wspomniane już ogólne rozporządzenie o ochronie danych.

Opierając się na projekcie dyrektywy przedstawionym przez Komisję, Parlament Europejski i Rada przeprowadziły nieformalne negocjacje, by wypracować porozumienie na etapie przyjmowania przez Radę stanowiska w pierwszym czytaniu. Tekst tego stanowiska jest pełnym odzwierciedleniem kompromisu osiągniętego przez obie instytucje ustawodawcze (przy udziale Komisji Europejskiej) co do dyrektywy. Wszelkie odniesienia do stanowiska Rady należy zatem w niniejszym dokumencie traktować jako odniesienia do kompromisu osiągniętego w rozmowach trójstronnych.

Ochrona osób fizycznych w związku z przetwarzaniem danych osobowych jest prawem podstawowym. O tym, że każda osoba ma prawo do ochrony danych osobowych jej dotyczących, mówi art. 8 ust. 1 Karty praw podstawowych Unii Europejskiej oraz art. 16 ust. 1 Traktatu o funkcjonowaniu Unii Europejskiej. Na tej podstawie stanowisko Rady określa zasady i przepisy dotyczące ochrony osób fizycznych, gdy przetwarzane są ich dane osobowe. Zasady te i przepisy muszą być zgodne z podstawowymi prawami i wolnościami osoby fizycznej – bez względu na jej obywatelstwo czy miejsce zamieszkania – a zwłaszcza z jej prawem do ochrony danych osobowych.

W swoim stanowisku Rada utrzymuje cele decyzji ramowej [1] oraz projektu Komisji, np. zasadę niezbędnej minimalnej harmonizacji pochodzącą z decyzji ramowej. Proponowana dyrektywa zawiera jaśniejsze, bardziej szczegółowe wersje większości przepisów decyzji ramowej – rozwinięte i rozbudowane zostały zwłaszcza przepisy o przekazywaniu danych do państw trzecich czy organizacji międzynarodowych.

W czerwcu 2015 r. Rada ustaliła podejście ogólne do proponowanego rozporządzenia, a w październiku 2015 r. – do proponowanej dyrektywy.

Nowa podstawa prawna z Traktatu o funkcjonowaniu Unii Europejskiej dotycząca ochrony danych osobowych ma zastosowanie do wszystkich dziedzin polityki (bez uszczerbku dla szczególnych uregulowań do ustalenia w dziedzinie wspólnej polityki zagranicznej i bezpieczeństwa). Niemniej deklaracja 21 załączona do traktatu lizbońskiego stwierdza, że konieczne mogą okazać się szczególne uregulowania w dziedzinie współpracy wymiarów sprawiedliwości w sprawach karnych i w dziedzinie współpracy policyjnej. Z tych względów oraz z uwagi na to, że proponowana dyrektywa jest elementem pakietu poświęconego ochronie danych, Rada starała się w wielu przepisach uzgodnić jej tekst z tekstem proponowanego rozporządzenia. Dotyczy to szczególnie definicji, zasad, rozdziału o administratorze i podmiocie przetwarzającym, decyzji stwierdzających odpowiedni stopień ochrony oraz rozdziału o niezależnych organach nadzorczych. Dlatego zostanie im poświęcone mniej uwagi w niniejszym dokumencie.

B. Podstawowe aspekty merytoryczne

1. *Zakres zastosowania (materialny i osobowy)*

Stanowisko Rady wyznacza w artykule 1 ust. 1 zakres materialny proponowanej dyrektywy. Zakres ten obejmuje przetwarzanie danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w tym do ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom. Oznacza to, że proponowana dyrektywa ma zastosowanie (w przeciwieństwie do decyzji ramowej 2008/977/WSiSW) także do wewnątrzkrajowego przetwarzania danych osobowych.

Drugi akt pakietu – proponowane rozporządzenie – wyłącza ze swojego zakresu zakres objęty dyrektywą, przez co oba zakresy stają się wzajemnie rozłączne. Proponowane rozporządzenie zawiera przepisy ogólne, natomiast proponowana dyrektywa ma zastosowanie do konkretnego sektora: współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej.

[1] 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).

Praca policji i innych organów ścigania może polegać m.in. na sprawowaniu władzy poprzez stosowanie środków przymusu, takich jak czynności policji podczas demonstracji, dużych imprez sportowych czy zamieszek. W swoim stanowisku Rada chce umożliwić takim organom (głównie policji) przetwarzanie danych na mocy pojedynczego aktu – prawa państwa członkowskiego stanowiącego transpozycję proponowanej dyrektywy. Jeżeli jednak policja przetwarza dane osobowe do celów spoza zakresu proponowanej dyrektywy, zastosowanie miałoby proponowane rozporządzenie, jak to określono w pkt 7. Dlatego w swoim stanowisku Rada doprecyzowała zakres proponowanej dyrektywy przez dodanie słów „ochrona przed zagrożeniami dla bezpieczeństwa publicznego i zapobieganie takim zagrożeniom".

Jeżeli chodzi o zakres osobowy, Rada w swoim stanowisku wychodzi poza organy publiczne właściwe do zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar i rozszerza go na takie organy lub podmioty, którym prawo państwa członkowskiego powierza sprawowanie władzy publicznej i wykonywanie uprawnień publicznych do wspomnianych celów. Przy czym tylko organy publiczne mogą przekazywać dane osobowe odbiorcom innym niż organ właściwy do celów proponowanej dyrektywy, mającym siedzibę w państwach trzecich

2. ***Zasady dotyczące danych osobowych***

a) **Przejrzystość**

W przeciwieństwie do stanowiska z pierwszego czytania proponowanego rozporządzenia Rada w swoim stanowisku z pierwszego czytania proponowanej dyrektywy nie wymienia „przejrzystości" wśród zasad przetwarzania danych osobowych, gdyż w zakresie ścigania przejrzystość mogłaby przynieść szkodę toczącym się postępowaniom przygotowawczym. Niemniej „przejrzystość" wspomniano w motywie dotyczącym tych zasad, przy czym zaznaczono, że zezwala się na prowadzenie czynności takich, jak nadzór niejawny czy monitoring wizyjny.

b) **Bezpieczeństwo przetwarzania danych**

W swoim stanowisku Rada dodaje, że dane osobowe należy przetwarzać w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem. Dodaje też, że w tym celu należy zastosować odpowiednie środki techniczne lub organizacyjne. Odpowiada to brzmieniu proponowanego rozporządzenia.

3. ***Dalsze przetwarzanie danych***

a) **Zgodność celu**

Kwestia dalszego przetwarzania (i to, czy może go dokonywać tylko ten sam administrator, czy także inny) oraz kwestia zgodnych celów okazały się problematyczne w dyskusjach nad proponowanym rozporządzeniem. Ostatecznie w swoim stanowisku z pierwszego czytania proponowanej dyrektywy Rada uznała, że za dozwolone należy uznać każde przetwarzanie prowadzone w którymkolwiek z celów, o których mowa w art. 1 ust. 1, pod warunkiem że w świetle prawa Unii lub prawa państwa członkowskiego administrator jest uprawniony do przetwarzania odnośnych danych osobowych w takim celu, a odnośne przetwarzanie jest niezbędne i proporcjonalne wobec takiego celu w świetle prawa Unii lub prawa państwa członkowskiego.

b) **Przetwarzanie do innych celów w ramach zakresu zastosowania proponowanej dyrektywy**

Stanowisko Rady przewiduje, że ten sam lub inny administrator mogą przetwarzać dane w którymkolwiek z celów określonych w art. 1 ust. 1, ale będących innymi niż cele, do których dane zostały zebrane, tylko wtedy, gdy taki administrator jest w świetle prawa Unii lub prawa państwa członkowskiego uprawniony do przetwarzania takich danych osobowych w takim celu i gdy w świetle prawa Unii lub prawa państwa członkowskiego odnośne przetwarzanie jest niezbędne i proporcjonalne względem tego innego celu. Dzięki temu prokurator np. będzie mógł w celu ścigania przestępstwa przetwarzać te same dane osobowe, które policja przetwarzała do wykrycia przestępstwa, o ile oba przykładowe cele są objęte artykułem 1 ust. 1.

4. ***Terminy przechowywania i przeglądu danych***

Stanowisko Rady przewiduje, że należy ustalić odpowiednie terminy usuwania danych osobowych lub okresowego przeglądu przechowywanych danych osobowych, by zweryfikować konieczność ich dalszego przechowywania. Już decyzja ramowa zawierała przepis o terminach, i Rada w swoim stanowisku uznała dodanie takiego przepisu za użyteczne.

Wzmacnia on zasadę określoną w art. 4, mianowicie że dane należy przechowywać nie dłużej, niż jest to niezbędne do celów, w których są przetwarzane.

5. ***Różne kategorie osób, których dane dotyczą***

Stanowisko Rady przewiduje, że państwa członkowskie muszą dopilnować, by administrator „w stosownym przypadku i w miarę możliwości" wyraźnie rozróżniał dane osobowe poszczególnych kategorii osób, których dane dotyczą. Niemniej stanowisko to przewiduje też, że zaliczanie osób, których dane dotyczą, do różnych kategorii nie może uniemożliwiać stosowania prawa do domniemania niewinności gwarantowanego w Karcie praw podstawowych, zwłaszcza jeżeli chodzi o kategorię osób, co do których istnieją poważne podstawy, by przypuszczać, że popełniły lub zamierzają popełnić czyn zabroniony.

6. ***Zgodność przetwarzania z prawem***

Stanowisko Rady przewiduje, że przetwarzanie danych osobowych jest zgodne z prawem wyłącznie wtedy, gdy – i w tylko w takim zakresie, w jakim – jest ono niezbędne do wykonania zadania realizowanego przez właściwy organ w celach zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w tym do ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom, oraz ma podstawę w prawie Unii lub prawie państwa członkowskiego. W motywach Rada stwierdza wyraźnie, że działania te obejmują ochronę żywotnych interesów osoby, której dane dotyczą.

Stanowisko Rady precyzuje też, jakie elementy muszą się znaleźć w przepisach państw członkowskich o ochronie danych – m. in. cele ogólne oraz cele przetwarzania.

7. ***Szczególne warunki przetwarzania***

Podstawową zasadą jest to, że dane osobowe pierwotnie zebrane przez właściwy organ do celów określonych w art. 1 ust. 1 proponowanej dyrektywy wolno przetwarzać wyłącznie w celach wskazanych w tej dyrektywie. Niemniej dane osobowe pierwotnie zebrane przez taki organ do celów wskazanych w proponowanej dyrektywie wolno także przetwarzać na podstawie proponowanego rozporządzenia (jeżeli na takie przetwarzanie zezwala prawo Unii lub prawo państwa członkowskiego), chyba że przetwarzanie odbywa się w toku działalności nieobjętej prawem Unii. Stanowisko Rady doprecyzowuje też, w jakich dwóch przypadkach zastosowanie ma proponowane rozporządzenie. Po pierwsze: gdy prawo państwa członkowskiego powierza właściwym organom wykonywanie zadań innych niż określone w art. 1 ust. 1. Po drugie: gdy przetwarzanie służy potrzebom archiwizacji w interesie publicznym lub wykorzystaniu do celów naukowych, statystycznych lub historycznych, chyba że przetwarzanie odbywa się w toku działalności nieobjętej prawem Unii.

8. ***Szczególne kategorie danych osobowych***

Dane osobowe, które z racji swego charakteru są szczególnie wrażliwe w świetle podstawowych praw i wolności, wymagają szczególnej ochrony, gdyż kontekst ich przetwarzania może powodować poważne ryzyko naruszenia podstawowych praw i wolności. Stanowisko Rady zezwala na przetwarzanie takich danych, ale wyłącznie wtedy, gdy jest bezwzględnie niezbędne i podlega odpowiednim zabezpieczeniom dla praw i wolności osoby, której dane dotyczą. Przy czym takie przetwarzanie jest dozwolone tylko pod warunkiem że jest dopuszczone prawem Unii lub prawem państwa członkowskiego do ochrony żywotnych interesów osoby, której dane dotyczą, lub dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą.

Ponieważ proponowana dyrektywa i proponowane rozporządzenie stanowią pakiet, stanowisko Rady powtarza w proponowanej dyrektywie te same kategorie co w proponowanym rozporządzeniu (w tym „dane biometryczne" i „orientację seksualną").

9. ***Zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach (w tym profilowanie)***

Kolejna zasada określona w proponowanej dyrektywie głosi, że decyzja, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu (w tym profilowaniu) i ma niekorzystne skutki prawne dla osoby, której dane dotyczą, lub poważnie na nią wpływa, jest zakazana, chyba że prawo Unii lub państwa członkowskiego ją dopuszcza i przewiduje odpowiednie zabezpieczenia praw i wolności osoby, której dane dotyczą. Odnośne zabezpieczenie musi polegać przynajmniej na tym, że osoba, której dane dotyczą, ma prawo uzyskać interwencję ludzką ze strony administratora. Stanowisko Rady jasno stwierdza, że podstawą decyzji opartej wyłącznie na zautomatyzowanym przetwarzaniu nie mogą być dane szczególnych kategorii wymienionych w art. 10, chyba że istnieją właściwe środki ochrony praw, wolności i uzasadnionych interesów osoby, której dane dotyczą. Jasno też stwierdza się, że zabronione jest profilowanie opierające się na danych szczególnych kategorii z art. 10 i skutkujące dyskryminacją.

10. ***Prawa osoby, której dane dotyczą***

a) **Komunikacja z osobą, której dane dotyczą**

Stanowisko Rady zawiera przepisy o prawach osoby, której dane dotyczą. Aby osoba ta mogła wykonywać swoje prawa, musi zostać poinformowana o tym, że jej dane osobowe są przetwarzane. Informacje te należy podawać w zrozumiałej, zwięzłej, czytelnej i łatwo dostępnej formie, przy użyciu jasnego i prostego języka. Inaczej niż w proponowanym rozporządzeniu stanowisko Rady z pierwszego czytania dyrektywy nie wymaga, aby informacje te podawać w sposób przejrzysty. Na przykład jeżeli w dziedzinie objętej dyrektywą poda się osobie, której dane dotyczą, na wczesnym etapie postępowania przygotowawczego informacje o konkretnym środku dochodzeniowym, cel postępowania przygotowawczego może zostać narażony na szwank.

b) **Informacje dla osoby, której dane dotyczą**

Stanowisko Rady określa, jakie informacje należy zawsze udostępniać osobie, której dane dotyczą: m.in. tożsamość i dane kontaktowe administratora oraz cel przetwarzania. Można to uczynić na stronie internetowej właściwego organu. Stanowisko określa też, jakie dodatkowe informacje należy podać w konkretnych przypadkach. Są to m.in. podstawa prawna przetwarzania, okres przechowywania danych osobowych oraz kategorie odbiorców. W pewnych okolicznościach podanie tych dodatkowych informacji można opóźnić, ograniczyć lub pominąć – np. gdy taki środek jest działaniem koniecznym i proporcjonalnym w społeczeństwie demokratycznym, przy uwzględnieniu praw podstawowych i uzasadnionych interesów danej osoby fizycznej. Ponadto, jeżeli chodzi o wspomniane dodatkowe informacje, państwa członkowskie mogą przewidzieć w swoim prawie, że niektóre kategorie przetwarzania danych osobowych wolno zwolnić z obowiązków informacyjnych.

c) **Prawo dostępu do danych**

W swoim stanowisku Rada ustanawia zarówno prawo dostępu do danych osobowych, jak i jego ograniczenia. Państwa członkowskie mogą prawo dostępu ograniczyć pod takimi samymi warunkami, pod jakimi można opóźnić, ograniczyć lub pominąć podanie dodatkowych informacji. Jeżeli prawo dostępu zostało ograniczone, państwa członkowskie muszą nakazać prawem, aby administrator poinformował osobę, której dane dotyczą, o przyczynach odmowy dostępu, chyba że np. cel takiego ograniczenia (np. postępowanie przygotowawcze) zostałby narażony na szwank, gdyby osoba ta została o tych przyczynach poinformowana.

d) **Szczególne przypadki ograniczenia przetwarzania danych osobowych**

Państwa członkowskie muszą zapewnić, by osoba, której dane dotyczą, miała prawo spowodować sprostowanie swoich danych, ich usunięcie lub ograniczenie ich przetwarzania. Stanowisko Rady dodaje możliwość, aby w dwóch konkretnych sytuacjach osoba, której dane dotyczą, spowodowała zamiast usunięcia danych ograniczenie ich przetwarzania. Po pierwsze, gdy osoba ta kwestionuje prawidłowość danych, a ich prawidłowości lub nieprawidłowości nie można stwierdzić. Po drugie, gdy dane osobowe zostają zachowane do celów dowodowych. Dla zilustrowania tego drugiego przypadku odnośny motyw mówi o sytuacjach, w których uzasadnione przesłanki sugerują, że usunięcie mogłoby wpłynąć na uprawnione interesy osoby, której dane dotyczą. W takich sytuacjach odnośne dane wolno przetwarzać tylko w celach, które zapobiegły ich usunięciu.

11. ***Wykonywanie praw osoby, której dane dotyczą, oraz weryfikacja***

Odnośnie do sytuacji, gdy osobie, której dane dotyczą, zostało ograniczone prawo do informacji, do dostępu, do sprostowania, do usunięcia lub do ograniczenia przetwarzania, państwa członkowskie muszą przyjąć środki przewidujące, że osoba, której dane dotyczą, powinna móc swoje prawa wykonywać za pośrednictwem właściwego organu nadzorczego.

12. ***Administrator i podmiot przetwarzający***

Proponowana dyrektywa będzie stosowana przez właściwe organy wewnętrzkrajowo lub przy przesyłaniu danych osobowych do innych państw członkowskich, lub też przy ich przekazywaniu do państw trzecich czy organizacji międzynarodowych. „Właściwe organy" są zdefiniowane jako organy publiczne lub jako każdy inny organ lub podmiot, któremu prawo państwa członkowskiego powierza sprawowanie władzy publicznej i wykonywanie uprawnień publicznych. Przepisy proponowanej dyrektywy będą stosowane przez organy publiczne, a w pewnych okolicznościach przez podmioty prywatne. Przetwarzając dane osobowe do celów innych niż określone w proponowanej dyrektywie, zdefiniowane w niej właściwe organy muszą zastosować proponowane rozporządzenie. Dlatego, jak zaznaczono już na wstępie, stanowisko Rady zestraja do pewnego stopnia przepisy proponowanej dyrektywy z przepisami proponowanego rozporządzenia.

Podobnie zatem jak w proponowanym rozporządzeniu stanowisko Rady przewiduje, że administrator musi wdrożyć odpowiednie środki techniczne i organizacyjne, by zapewnić i móc wykazać zgodność swojego przetwarzania z dyrektywą. Stanowisko Rady jednoznacznie wymienia też obowiązki podmiotu przetwarzającego, który musi np.:

— działać wyłącznie zgodnie z poleceniami administratora;

— zapewnić, by osoby upoważnione do przetwarzania danych osobowych przestrzegały poufności;

— udostępniać administratorowi wszelkie informacje na dowód tego, że wywiązuje się ze swoich obowiązków.

13. ***Wykazy czynności przetwarzania***

Jeżeli chodzi o wykazy czynności przetwarzania, stanowisko Rady nakłada mniej obowiązków na podmiot przetwarzający, dlatego obowiązki administratora i podmiotu przetwarzającego wymienia w odrębnych ustępach. Określa, że w wykazach żaden z nich nie musi zamieszczać każdej czynności przetwarzania, ale tylko ich kategorie. W pozostałych częściach ustępu przewiduje, że administrator musi odnotowywać odpowiednio dużo informacji, by zrealizować cel wykazów. Administrator ma np. obowiązek odnotowywać informacje o kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, informacje o kategoriach przekazań danych osobowych do państwa trzeciego lub organizacji międzynarodowej, a także – jeżeli jest to możliwe – planowane terminy usunięcia poszczególnych kategorii danych. Administrator musi też podać informacje o profilowaniu, czego nie ma w proponowanym rozporządzeniu. Względem podmiotu przetwarzającego stanowisko Rady określa, że musi odnotowywać w wykazie tylko np. kategorie przetwarzań dokonywanych w imieniu każdego z administratorów oraz – w miarę możliwości – ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.

14. ***Ewidencja czynności***

Ewidencjonowanie czynności jest ważne, by można było ustalić zasadność, datę oraz godzinę różnych operacji przetwarzania (takich jak zbieranie, przeglądanie, ujawnianie i przekazywanie) w zautomatyzowanych systemach przetwarzania. Ewidencja przeglądania i ujawniania ma też pozwolić na zidentyfikowanie osoby, która dane osobowe przeglądała czy ujawniła, oraz na zidentyfikowanie odbiorcy. Tak jak w decyzji ramowej ewidencję wolno wykorzystywać wyłącznie do weryfikacji zgodności przetwarzania danych z prawem, do monitorowania własnej działalności oraz do zapewniania integralności i bezpieczeństwa danych osobowych. Nowym elementem proponowanej dyrektywy jest to, że ewidencji można też używać na potrzeby postępowania karnego. Jednak dostosowanie zautomatyzowanych systemów przetwarzania do nowych przepisów będzie bardzo kłopotliwe, długotrwałe i kosztowne. Dlatego stanowisko Rady pozwala wyjątkowo wydłużyć okres wdrożeniowy (przeznaczony na to, by dostosować systemy utworzone przed wejściem proponowanej dyrektywy w życie), jeżeli takie dostosowanie wymaga niewspółmiernie dużego wysiłku. W wyjątkowych okolicznościach przewiduje dodatkowe przedłużenie, jeżeli inaczej dostosowanie zautomatyzowanego systemu przetwarzania utworzonego przed wejściem proponowanej dyrektywy w życie spowodowałoby poważne problemy w funkcjonowaniu tego systemu.

15. ***Ocena skutków***

Pierwotny wniosek Komisji nie przewidywał oceny skutków dla ochrony danych. Niemniej w proponowanym rozporządzeniu jest artykuł o takiej ocenie, i dlatego w stanowisku Rady z pierwszego czytania dyrektywy taki artykuł również figuruje. Stanowisko Rady nakłada na administratora obowiązek dokonania oceny skutków. Administrator musi jej dokonać przed przetworzeniem, jeżeli może ono skutkować powstaniem wysokiego ryzyka naruszenia praw i wolności osób fizycznych.

Sytuacje, w których ocena skutków jest obowiązkowa, są w proponowanej dyrektywie sformułowane podobnie jak w proponowanym rozporządzeniu. Jednak wymagane elementy oceny są określone nie tak szczegółowo jak w proponowanym rozporządzeniu. Ocena musi zawierać co najmniej ogólny opis planowanych operacji przetwarzania, ocenę ryzyka naruszenia praw i wolności osób, których dane dotyczą, zabezpieczenia, środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazanie zgodności z przepisami proponowanej dyrektywy.

16. ***Inspektor ochrony danych***

Według stanowiska Rady państwa członkowskie muszą zapewnić, by administrator wyznaczył inspektora ochrony danych. Niemniej państwa członkowskie powinny móc z tego obowiązku zwolnić sądy i inne organy sądowe w ramach sprawowania przez nie wymiaru sprawiedliwości. Wyznaczenie inspektora ochrony danych ma służyć lepszemu przestrzeganiu proponowanej dyrektywy.

17. ***Przekazywanie danych***

Aby można było wymieniać dane z państwami trzecimi i organizacjami międzynarodowymi, trzeba dysponować przepisami o przekazywaniu danych. Jeżeli chodzi o ogólne zasady przekazywania danych osobowych, stanowisko Rady rozszerzyło warunki zaproponowane przez Komisję: organ odbierający musi być organem właściwym do realizacji celów określonych w art. 1 ust. 1, a w przypadku przesyłania lub udostępniania danych od innego państwa członkowskiego trzeba uzyskać jego uprzednią zgodę. Ponadto stanowisko Rady jasno stwierdza, że należy przestrzegać wszystkich przepisów rozdziału o przekazywaniu danych, tak aby nie został obniżony stopień ochrony osób fizycznych zapewniany proponowaną dyrektywą.

Artykuł o ogólnych zasadach daje administratorom do wyboru różne podstawy przekazywania danych osobowych, ułożone od najbardziej zalecanej – decyzji stwierdzającej odpowiedni stopień ochrony. Następne w kolejności jest przekazywanie z zastrzeżeniem odpowiednich zabezpieczeń, a po nim – przekazywanie na podstawie wyjątków obowiązujących w szczególnych sytuacjach. Artykuł o decyzjach stwierdzających odpowiedni stopień ochrony odnosi się jedynie do decyzji zapadłych na mocy proponowanej dyrektywy, a nie jak przedtem – do decyzji zapadłych na mocy rozporządzenia. Elementy, które Komisja musi uwzględnić przy ocenianiu, czy stopień ochrony jest odpowiedni, są w proponowanej dyrektywie takie same jak w proponowanym rozporządzeniu.

W kolejnych dwóch artykułach (o przekazywaniu z zastrzeżeniem odpowiednich zabezpieczeń i o wyjątkach w szczególnych sytuacjach) stanowisko Rady precyzuje, że oparte na nich przekazanie musi być udokumentowane, a dokumentacja musi zostać udostępniona organowi nadzorczemu. Określa też elementy, które należy zawrzeć w dokumentacji.

Stanowisko Rady dodaje też jedną podstawę przekazywania, która umożliwia właściwym organom (ale tylko publicznym, a nie organom czy podmiotom, którym prawo krajowe powierza wykonywanie uprawnień publicznych) przekazywanie danych osobowych odbiorcom mającym siedzibę w państwach trzecich. Możliwość ta stanowi wyjątek od ogólnej zasady, zgodnie z którą dane osobowe wolno przekazywać tylko wtedy, gdy administrator w państwie trzecim lub organizacji międzynarodowej jest organem właściwym do realizacji celów określonych w art. 1 ust. 1. Otóż wspomniane właściwe organy będą mogły w indywidualnych, konkretnych przypadkach – o ile tylko zachowane będą pozostałe przepisy dyrektywy i spełnione zostaną wyliczone wyczerpująco warunki – przekazywać dane osobowe takim odbiorcom bezpośrednio, gdyż umowy międzynarodowe nie zawsze pozwalają na szybką odpowiedź, która może jednak być konieczna. Odnośne warunki przewidują m.in., że przekazanie musi być ściśle niezbędne do wykonania zadania właściwego organu przekazującego zgodnie z prawem Unii lub prawem państwa członkowskiego do celów określonych w art. 1 ust. 1, że zdaniem właściwego organu przekazującego przekazanie organowi w państwie trzecim właściwemu do celów określonych w art. 1 ust. 1 byłoby nieskuteczne lub niewłaściwe (w szczególności dlatego, że nie mogłoby nastąpić w odpowiednim terminie) oraz że organ przekazujący musi poinformować odbiorcę o konkretnym celu lub celach, w których dane osobowe mają być przetwarzane. Dodany jest też obowiązek dokumentacyjny – podobnie jak przy przekazywaniu z zastrzeżeniem odpowiednich zabezpieczeń i na podstawie wyjątków w szczególnych sytuacjach. Takie przekazanie może być szczególnie użyteczne, gdy zachodzi pilna potrzeba przekazania danych osobowych w celu ratowania życia osobie mogącej paść ofiarą czynu zabronionego lub gdy jest to konieczne do zapobieżenia spodziewanemu popełnieniu czynu zabronionego, w tym dokonaniu ataku terrorystycznego.

18. ***Organy nadzorcze***

Aby zapewnić przestrzeganie przepisów proponowanej dyrektywy, organy nadzorcze będą monitorować stosowanie jej przepisów – a także przepisów proponowanego rozporządzenia. Przepisy o organach nadzorczych w proponowanej dyrektywie pochodzą w dużej mierze z proponowanego rozporządzenia. Państwom członkowskim wolno zapewnić, by organy nadzorcze powołane na mocy proponowanego rozporządzenia mogły również monitorować stosowanie proponowanej dyrektywy. Jednak proponowana dyrektywa nie zezwala, aby zdefiniowane w niej organy nadzorcze sprawowały nadzór nad operacjami przetwarzania dokonywanymi przez sądy w ramach sprawowania przez nie wymiaru sprawiedliwości. Państwa członkowskie powinny móc także zdecydować, że organy nadzorcze zdefiniowane w proponowanej dyrektywie nie mogą nadzorować operacji przetwarzania dokonywanych przez inne niezależne organy wymiaru sprawiedliwości w ramach sprawowania przez nie wymiaru sprawiedliwości. Nie oznacza to jednak, by przetwarzanie dokonywane przez te instancje nie podlegało żadnemu nadzorowi. Dlatego w odnośnym motywie wspomniano, że operacje przetwarzania dokonywane przez sądy i inne niezależne organy wymiaru sprawiedliwości powinny – zgodnie z Kartą praw podstawowych Unii Europejskiej – podlegać niezależnej kontroli.

19. ***Uprawnienia organów nadzorczych***

Stanowisko Rady przewiduje, że organy nadzorcze powinny mieć w każdym państwie członkowskim te same zadania i faktyczne uprawnienia, tak by mogły skutecznie, rzetelnie i spójnie monitorować przestrzeganie i wykonywanie proponowanej dyrektywy w całej Unii.

Stanowisko Rady dzieli uprawnienia organów nadzorczych (które to uprawnienia należy określić prawem) na trzy kategorie: skuteczne uprawnienia w zakresie prowadzenia postępowań, skuteczne uprawnienia naprawcze oraz skuteczne uprawnienia doradcze. Ponadto określa też uprawnienie, by wnosić do organów sądowych sprawy dotyczące naruszeń przepisów przyjętych na podstawie proponowanej dyrektywy.

20. ***Stosunek do uprzednio zawartych umów międzynarodowych***

W swoim stanowisku Rada przewiduje (podobnie jak w stanowisku z pierwszego czytania proponowanego rozporządzenia), że umowy międzynarodowe, które zostały zawarte przez państwa członkowskie przed datą wejścia proponowanej dyrektywy w życie i są zgodne z prawem Unii mającym zastosowanie przed datą jej wejścia w życie, pozostają w mocy do czasu ich zmiany, zastąpienia lub uchylenia. Jak stwierdza proponowane rozporządzenie, dzięki utrzymaniu takich umów administratorzy mają pewność prawa.

IV. **PODSUMOWANIE**

Stanowisko Rady jest odzwierciedleniem kompromisu osiągniętego w negocjacjach między Radą a Parlamentem Europejskim, w których pośredniczyła Komisja. Zatwierdzając stanowisko Rady bez poprawek, Parlament Europejski ustanawia wraz z Radą wysokie standardy ochrony danych na szczeblu zarówno wewnątrzkrajowym, jak i transgranicznym, umożliwiające lepszą współpracę organów ścigania.

ISSN 1977-1002 (wydanie elektroniczne)
ISSN 1725-5228 (wydanie papierowe)

Urząd Publikacji Unii Europejskiej
2985 Luksemburg
LUKSEMBURG

PL