I

(Akty ustawodawcze)

ROZPORZĄDZENIA

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/679

z dnia 27 kwietnia 2016 r.

w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)

(Tekst mający znaczenie dla EOG)

PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ,

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

uwzględniając wniosek Komisji Europejskiej,

po przekazaniu projektu aktu ustawodawczego parlamentom narodowym,

uwzględniając opinię Europejskiego Komitetu Ekonomiczno-Społecznego ([1]),

uwzględniając opinię Komitetu Regionów ([2]),

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą ([3]),

a także mając na uwadze, co następuje:

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

(2) Zasady i przepisy dotyczące ochrony osób fizycznych w związku z przetwarzaniem ich danych osobowych nie mogą – niezależnie od obywatelstwa czy miejsca zamieszkania takich osób – naruszać ich podstawowych praw i wolności, w szczególności prawa do ochrony danych osobowych. Niniejsze rozporządzenie ma na celu przyczyniać się do tworzenia przestrzeni wolności, bezpieczeństwa i sprawiedliwości oraz unii gospodarczej, do postępu społeczno-gospodarczego, do wzmacniania i konwergencji gospodarek na rynku wewnętrznym, a także do pomyślności ludzi.

(3) Celem dyrektywy Parlamentu Europejskiego i Rady 95/46/WE ([4]) jest zharmonizowanie ochrony podstawowych praw i wolności osób fizycznych w związku z czynnościami przetwarzania oraz zapewnienie swobodnego przepływu danych osobowych między państwami członkowskimi.

([1]) Dz.U. C 229 z 31.7.2012, s. 90.
([2]) Dz.U. C 391 z 18.12.2012, s. 127.
([3]) Stanowisko Parlamentu Europejskiego z dnia 12 marca 2014 r. (dotychczas nieopublikowane w Dzienniku Urzędowym) oraz stanowisko Rady w pierwszym czytaniu z dnia 8 kwietnia 2016 r. (dotychczas nieopublikowane w Dzienniku Urzędowym). Stanowisko Parlamentu Europejskiego z dnia 14 kwietnia 2016 r.
([4]) Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz.U. L 281 z 23.11.1995, s. 31).

(4) Przetwarzanie danych osobowych należy zorganizować w taki sposób, aby służyło ludzkości. Prawo do ochrony danych osobowych nie jest prawem bezwzględnym; należy je postrzegać w kontekście jego funkcji społecznej i wyważyć względem innych praw podstawowych w myśl zasady proporcjonalności. Niniejsze rozporządzenie nie narusza praw podstawowych, wolności i zasad uznanych w Karcie praw podstawowych – zapisanych w Traktatach – w szczególności prawa do poszanowania życia prywatnego i rodzinnego, domu oraz komunikowania się, ochrony danych osobowych, wolności myśli, sumienia i religii, wolności wypowiedzi i informacji, wolności prowadzenia działalności gospodarczej, prawa do skutecznego środka prawnego i dostępu do bezstronnego sądu oraz różnorodności kulturowej, religijnej i językowej.

(5) Integracja społeczno-gospodarcza wynikająca z funkcjonowania rynku wewnętrznego doprowadziła do znacznego zwiększenia transgranicznych przepływów danych osobowych. Wzrosła wymiana danych osobowych między podmiotami publicznymi i prywatnymi, w tym między osobami fizycznymi, zrzeszeniami i przedsiębiorstwami w Unii. Od organów krajowych państw członkowskich prawo Unii coraz częściej wymaga, by w celu wykonania swoich obowiązków lub w celu realizacji zadań w imieniu organu innego państwa członkowskiego współpracowały ze sobą i wymieniały się danymi osobowymi.

(6) Szybki postęp techniczny i globalizacja przyniosły nowe wyzwania w dziedzinie ochrony danych osobowych. Skala zbierania i wymiany danych osobowych znacząco wzrosła. Dzięki technologii zarówno przedsiębiorstwa prywatne, jak i organy publiczne mogą na niespotykaną dotąd skalę wykorzystywać dane osobowe w swojej działalności. Osoby fizyczne coraz częściej udostępniają informacje osobowe publicznie i globalnie. Technologia zmieniła gospodarkę i życie społeczne i powinna nadal ułatwiać swobodny przepływ danych osobowych w Unii oraz ich przekazywanie do państw trzecich i organizacji międzynarodowych, równocześnie zaś powinna zapewniać wysoki stopień ochrony danych osobowych.

(7) Przemiany te wymagają stabilnych, spójniejszych ram ochrony danych w Unii oraz zdecydowanego ich egzekwowania, gdyż ważna jest budowa zaufania, które pozwoli na rozwój gospodarki cyfrowej na rynku wewnętrznym. Osoby fizyczne powinny mieć kontrolę nad własnymi danymi osobowymi. Osoby fizyczne, podmioty gospodarcze i organy publiczne powinny zyskać większe poczucie pewności prawa i jego stosowania w praktyce.

(8) W zakresie, w jakim niniejsze rozporządzenie dopuszcza doprecyzowanie lub zawężenie jego przepisów przez prawo państw członkowskich, mogą one – o ile jest to niezbędne, by krajowe przepisy były spójne i zrozumiałe dla osób, do których mają zastosowanie – włączyć elementy niniejszego rozporządzenia do swego prawa krajowego.

(9) Cele i zasady dyrektywy 95/46/WE pozostają aktualne, jednak wdrażając ochronę danych w Unii, nie uniknięto fragmentaryzacji, niepewności prawnej oraz upowszechnienia się poglądu, że ochrona osób fizycznych jest znacznie zagrożona, w szczególności w związku z działaniami w internecie. Różnice w stopniu ochrony praw i wolności osób fizycznych w państwach członkowskich – w szczególności prawa do ochrony danych osobowych – w związku z przetwarzaniem danych osobowych mogą utrudniać swobodny przepływ danych osobowych w Unii. Mogą zatem stanowić przeszkodę w prowadzeniu działalności gospodarczej na szczeblu Unii, zakłócać konkurencję oraz utrudniać organom wykonywanie obowiązków nałożonych na nie prawem Unii. Różnice w stopniu ochrony wynikają z różnic we wdrażaniu i stosowaniu dyrektywy 95/46/WE.

(10) Aby zapewnić wysoki i spójny stopień ochrony osób fizycznych oraz usunąć przeszkody w przepływie danych osobowych w Unii, należy zapewnić równorzędny we wszystkich państwach członkowskich stopień ochrony praw i wolności osób fizycznych w związku z przetwarzaniem takich danych. Należy zapewnić spójne i jednolite w całej Unii stosowanie przepisów o ochronie podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych. Jeżeli chodzi o przetwarzanie danych osobowych w celu wypełnienia obowiązku prawnego, w celu wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi, państwa członkowskie powinny móc zachować lub wprowadzić krajowe przepisy doprecyzowujące stosowanie przepisów niniejszego rozporządzenia. Obok ogólnego, horyzontalnego prawa o ochronie danych wdrażającego dyrektywę 95/46/WE państwa członkowskie przyjęły uregulowania sektorowe w dziedzinach wymagających przepisów bardziej szczegółowych. Niniejsze rozporządzenie umożliwia też państwom członkowskim doprecyzowanie jego przepisów, w tym w odniesieniu do przetwarzania szczególnych kategorii danych osobowych (zwanych dalej „danymi wrażliwymi"). W tym względzie niniejsze rozporządzenie nie wyklucza możliwości określenia w prawie państwa członkowskiego okoliczności dotyczących konkretnych sytuacji związanych z przetwarzaniem danych, w tym dookreślenia warunków, które decydują o zgodności przetwarzania z prawem.

(11) Aby ochrona danych osobowych w Unii była skuteczna, należy wzmocnić i doprecyzować prawa osób, których dane dotyczą, oraz obowiązki podmiotów przetwarzających dane osobowe i decydujących o przetwarzaniu, jak również zapewnić równorzędne uprawnienia w zakresie monitorowania i egzekwowania przepisów o ochronie danych osobowych oraz równorzędne kary za naruszenia tych przepisów w państwach członkowskich.

(12) Art. 16 ust. 2 TFUE powierza Parlamentowi Europejskiemu i Radzie określenie zasad ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz zasad swobodnego przepływu takich danych.

(13) Aby zapewnić spójny stopień ochrony osób fizycznych w Unii oraz zapobiegać rozbieżnościom hamującym swobodny przepływ danych osobowych na rynku wewnętrznym, należy przyjąć rozporządzenie, które zagwarantuje podmiotom gospodarczym – w tym mikroprzedsiębiorstwom oraz małym i średnim przedsiębiorstwom – pewność prawa i przejrzystość, a osobom fizycznym we wszystkich państwach członkowskich ten sam poziom prawnie egzekwowalnych praw oraz obowiązków i zadań administratorów i podmiotów przetwarzających, które pozwoli spójnie monitorować przetwarzanie danych osobowych, a także które zapewni równoważne kary we wszystkich państwach członkowskich oraz skuteczną współpracę organów nadzorczych z różnych państw członkowskich. Aby rynek wewnętrzny mógł właściwie funkcjonować, swobodny przepływ danych osobowych w Unii nie jest ograniczany ani zakazany z powodów odnoszących się do ochrony osób fizycznych w związku z przetwarzaniem danych osobowych. Z uwagi na szczególną sytuację mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw niniejsze rozporządzenie przewiduje wyjątek dotyczący rejestrowania czynności przetwarzania dla podmiotów zatrudniających mniej niż 250 pracowników. Ponadto zachęca się instytucje i organy Unii, państwa członkowskie i ich organy nadzorcze, by stosując niniejsze rozporządzenie, uwzględniały szczególne potrzeby mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw. Rozumienie pojęcia mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw powinno opierać się na art. 2 załącznika do zalecenia Komisji 2003/361/WE ([1]).

(14) Ochrona zapewniana niniejszym rozporządzeniem powinna mieć zastosowanie do osób fizycznych – niezależnie od ich obywatelstwa czy miejsca zamieszkania – w związku z przetwarzaniem ich danych osobowych. Niniejsze rozporządzenie nie dotyczy przetwarzania danych osobowych dotyczących osób prawnych, w szczególności przedsiębiorstw będących osobami prawnymi, w tym danych o firmie i formie prawnej oraz danych kontaktowych osoby prawnej.

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

(16) Niniejsze rozporządzenie nie ma zastosowania do kwestii ochrony podstawowych praw i wolności ani do swobodnego przepływu danych osobowych w związku z działalnością nieobjętą zakresem prawa Unii, taką jak działalność dotycząca bezpieczeństwa narodowego. Niniejsze rozporządzenie nie ma zastosowania do przetwarzania danych osobowych przez państwa członkowskie w związku z działaniami związanymi ze wspólną polityką zagraniczną i bezpieczeństwa Unii.

(17) Do przetwarzania danych osobowych przez instytucje, organy i jednostki organizacyjne Unii ma zastosowanie rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 45/2001 ([2]). Rozporządzenie (WE) nr 45/2001 oraz inne unijne akty prawne mające zastosowanie do takiego przetwarzania danych osobowych należy dostosować do zasad i przepisów ustanowionych w niniejszym rozporządzeniu oraz stosować w świetle niniejszego rozporządzenia. Aby zapewnić solidne i spójne ramy ochrony danych w Unii, należy po przyjęciu niniejszego rozporządzenia dokonać koniecznych modyfikacji rozporządzenia (WE) nr 45/2001, tak by umożliwić jego stosowanie równocześnie z niniejszym rozporządzeniem.

(18) Niniejsze rozporządzenie nie ma zastosowania do przetwarzania danych osobowych przez osobę fizyczną w ramach działalności czysto osobistej lub domowej, czyli bez związku z działalnością zawodową lub handlową. Działalność osobista lub domowa może między innymi polegać na korespondencji i przechowywaniu adresów,

([1]) Zalecenie Komisji z dnia 6 maja 2003 r. dotyczące definicji mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw (C(2003) 1422) (Dz.U. L 124 z 20.5.2003, s. 36).

([2]) 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).

podtrzymywaniu więzi społecznych oraz działalności internetowej podejmowanej w ramach takiej działalności. Niniejsze rozporządzenie ma jednak zastosowanie do administratorów lub podmiotów przetwarzających, którzy udostępniają środki przetwarzania danych osobowych na potrzeby takiej działalności osobistej lub domowej.

(19) Ochrona osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy w ramach zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania lub ścigania czynów zabronionych, lub wykonywania kar, w tym w celu ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom, oraz swobodny przepływ takich danych podlegają szczególnemu aktowi prawnemu Unii. Niniejsze rozporządzenie nie powinno zatem mieć zastosowania do czynności przetwarzania w tych celach. Jeżeli jednak dane osobowe przetwarzane przez organy publiczne na mocy niniejszego rozporządzenia są wykorzystywane do tych celów, dane te powinny podlegać szczególnemu aktowi prawnemu Unii, mianowicie dyrektywie Parlamentu Europejskiego i Rady (UE) 2016/680 ([1]). Państwa członkowskie mogą powierzyć właściwym organom w rozumieniu dyrektywy (UE) 2016/680 zadania – które niekoniecznie służą zapobieganiu przestępczości, prowadzeniu postępowań przygotowawczych, wykrywaniu lub ściganiu czynów zabronionych, lub też wykonywaniu kar, w tym ochronie przed zagrożeniami dla bezpieczeństwa publicznego i zapobieganiu takim zagrożeniom – tak by przetwarzanie danych osobowych do tych innych celów, o ile objęte jest zakresem prawa Unii, wchodziło w zakres zastosowania niniejszego rozporządzenia.

Jeżeli chodzi o przetwarzanie danych osobowych przez te właściwe organy do celów wchodzących w zakres niniejszego rozporządzenia, państwa członkowskie powinny mieć możliwość zachowania lub wprowadzenia przepisów szczególnych dostosowujących stosowanie przepisów niniejszego rozporządzenia. W takich przepisach możliwe jest doprecyzowanie szczególnych wymogów przetwarzania danych przez te właściwe organy do tych innych celów, z uwzględnieniem konstytucyjnych, organizacyjnych i administracyjnych struktur danego państwa członkowskiego. Jeżeli przetwarzanie danych osobowych przez podmioty prywatne objęte jest zakresem stosowania niniejszego rozporządzenia, niniejsze rozporządzenie powinno na określonych warunkach umożliwiać państwom członkowskim ograniczenie w swoich przepisach niektórych obowiązków i praw, o ile takie ograniczenie stanowi w demokratycznym społeczeństwie niezbędny i proporcjonalny środek chroniący określone, ważne interesy, w tym bezpieczeństwo publiczne oraz zapobieganie przestępczości, prowadzenie postępowań przygotowawczych, wykrywanie lub ściganie czynów zabronionych, lub też wykonywanie kar, w tym ochronę przed zagrożeniami dla bezpieczeństwa publicznego i zapobieganie takim zagrożeniom. Jest to istotne na przykład w związku z przeciwdziałaniem praniu pieniędzy lub w działalności laboratoriów kryminalistycznych.

(20) Niniejsze rozporządzenie ma zastosowanie między innymi do działań sądów i innych organów wymiaru sprawiedliwości, niemniej prawo Unii lub prawo państwa członkowskiego może doprecyzować operacje i procedury przetwarzania danych osobowych przez sądy i inne organy wymiaru sprawiedliwości. Właściwość organów nadzorczych nie powinna dotyczyć przetwarzania danych osobowych przez sądy w ramach sprawowania wymiaru sprawiedliwości – tak by chronić niezawisłość sprawowania wymiaru sprawiedliwości. Powinna istnieć możliwość powierzenia nadzoru nad takimi operacjami przetwarzania danych specjalnym organom w systemie wymiaru sprawiedliwości państwa członkowskiego, organy te powinny w szczególności zapewnić przestrzeganie przepisów niniejszego rozporządzenia, zwiększać w wymiarze sprawiedliwości wiedzę o jego obowiązkach wynikających z niniejszego rozporządzenia oraz rozpatrywać skargi związane z takim operacjami przetwarzania danych.

(21) Niniejsze rozporządzenie pozostaje bez uszczerbku dla stosowania dyrektywy Parlamentu Europejskiego i Rady 2000/31/WE ([2]), w szczególności dla zasad odpowiedzialności usługodawców będących pośrednikami, o których to zasadach mowa w art. 12–15 tej dyrektywy. Dyrektywa ta ma przyczyniać się do właściwego funkcjonowania rynku wewnętrznego przez zapewnienie swobodnego przepływu usług społeczeństwa informacyjnego między państwami członkowskimi.

(22) Przetwarzanie danych osobowych w kontekście działalności prowadzonej przez jednostkę organizacyjną administratora lub podmiotu przetwarzającego w Unii powinno odbywać się zgodnie z niniejszym rozporządzeniem, niezależnie od tego, czy samo przetwarzanie ma miejsce w Unii. Pojęcie „jednostka organizacyjna" zakłada skuteczne i faktyczne prowadzenie działalności poprzez stabilne struktury. Forma prawna takich struktur, niezależnie od tego, czy chodzi o oddział czy spółkę zależną posiadającą osobowość prawną, nie jest w tym względzie czynnikiem decydującym.

([1]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, swobodnego przepływu tych danych i oraz uchylenia decyzji ramowej Rady 2008/977/WSiSW (zob. s. 89 niniejszego Dziennika Urzędowego).

([2]) Dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym) (Dz.U. L 178 z 17.7.2000, s. 1).

(23) Aby osoby fizyczne nie zostały pozbawione ochrony przysługującej im na mocy niniejszego rozporządzenia, przetwarzanie danych osobowych osób, których dane dotyczą, znajdujących się w Unii, przez administratora lub podmiot przetwarzający, którzy nie posiadają jednostki organizacyjnej w Unii, powinno podlegać niniejszemu rozporządzeniu, jeżeli czynności przetwarzania wiążą się z oferowaniem takim osobom towarów lub usług, niezależnie od tego, czy pociąga to za sobą płatność. Aby stwierdzić, czy administrator lub podmiot przetwarzający oferują towary lub usługi znajdującym się w Unii osobom, których dane dotyczą, należy ustalić, czy jest oczywiste, że administrator lub podmiot przetwarzający planują oferować usługi osobom, których dane dotyczą, w co najmniej jednym państwie członkowskim Unii. O ile do ustalenia takiego zamiaru nie wystarczy sama dostępność w Unii strony internetowej administratora, podmiotu przetwarzającego, pośrednika, adresu poczty elektronicznej lub innych danych kontaktowych ani posługiwanie się językiem powszechnie stosowanym w państwie trzecim, w którym jednostkę organizacyjną ma administrator, o tyle potwierdzeniem oczywistości faktu, że administrator planuje oferować w Unii towary lub usługi osobom, których dane dotyczą, mogą być czynniki takie, jak posługiwanie się językiem lub walutą powszechnie stosowanymi w co najmniej jednym państwie członkowskim oraz możliwość zamówienia towarów i usług w tym języku lub wzmianka o klientach lub użytkownikach znajdujących się w Unii.

(24) Przetwarzanie danych osobowych znajdujących się w Unii osób, których dane dotyczą, przez administratora lub podmiot przetwarzający, którzy nie mają jednostki organizacyjnej w Unii, powinno podlegać niniejszemu rozporządzeniu także w przypadkach, gdy wiąże się z monitorowaniem zachowania takich osób, których dane dotyczą, o ile zachowanie to ma miejsce w Unii. Aby stwierdzić, czy czynność przetwarzania można uznać za „monitorowanie zachowania" osób, których dane dotyczą, należy ustalić, czy osoby fizyczne są obserwowane w internecie, w tym także czy później potencjalnie stosowane są techniki przetwarzania danych polegające na profilowaniu osoby fizycznej, w szczególności w celu podjęcia decyzji jej dotyczącej lub przeanalizowania lub prognozowania jej osobistych preferencji, zachowań i postaw.

(25) Niniejsze rozporządzenie powinno mieć zastosowanie do administratora niemającego jednostki organizacyjnej w Unii także w przypadkach, gdy na mocy prawa międzynarodowego publicznego stosuje się prawo państwa członkowskiego, na przykład na terenie misji dyplomatycznej lub placówki konsularnej państwa członkowskiego.

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

(27) Niniejsze rozporządzenie nie ma zastosowania do danych osobowych osób zmarłych. Państwa członkowskie mogą przyjąć przepisy o przetwarzaniu danych osobowych osób zmarłych.

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

(29) Aby zachęcić do stosowania pseudonimizacji podczas przetwarzania danych osobowych, należy umożliwić stosowanie u tego samego administratora środków pseudonimizacyjnych niewykluczających ogólnej analizy, o ile administrator ten zastosował środki techniczne i organizacyjne niezbędne do tego, by niniejsze rozporządzenie zostało wdrożone w zakresie danego przetwarzania i by dodatkowe informacje pozwalające przypisać dane osobowe konkretnej osobie, której dane dotyczą, były przechowywane osobno. Administrator przetwarzający dane osobowe powinien wskazać osoby uprawnione.

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

(31) Organy publiczne, którym ujawnia się dane osobowe w związku z ich prawnym obowiązkiem sprawowania funkcji publicznej (takich jak organy podatkowe, organy celne, finansowe 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 określonego postępowania w interesie ogólnym zgodnie z prawem Unii lub prawem państwa członkowskiego. Żądanie ujawnienia danych osobowych, z którym występują takie organy publiczne, powinno zawsze mieć formę pisemną, być uzasadnione, mieć charakter wyjątkowy, nie powinno dotyczyć całego zbioru danych ani prowadzić do połączenia zbiorów danych. Przetwarzając otrzymane dane osobowe, takie organy powinny przestrzegać mających zastosowanie przepisów o ochronie danych, zgodnie z celami przetwarzania.

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

(33) W momencie zbierania danych często nie da się w pełni zidentyfikować celu przetwarzania danych osobowych na potrzeby badań naukowych. Dlatego osoby, których dane dotyczą, powinny móc wyrazić zgodę na niektóre obszary badań naukowych, o ile badania te są zgodne z uznanymi normami etycznymi w zakresie badań naukowych. Osoby, których dane dotyczą, powinny móc wyrazić zgodę tylko na niektóre obszary badań lub elementy projektów badawczych, o ile umożliwia to zamierzony cel.

(34) Dane genetyczne należy zdefiniować jako dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, uzyskane z analizy próbki biologicznej danej osoby fizycznej, w szczególności z analizy chromosomów, kwasu dezoksyrybonukleinowego (DNA) lub kwasu rybonukleinowego (RNA) lub z analizy innych elementów umożliwiających pozyskanie równoważnych informacji.

(35) Do danych osobowych dotyczących zdrowia należy zaliczyć wszystkie dane o stanie zdrowia osoby, której dane dotyczą, ujawniające informacje o przeszłym, obecnym lub przyszłym stanie fizycznego lub psychicznego zdrowia osoby, której dane dotyczą. Do danych takich należą informacje o danej osobie fizycznej zbierane podczas jej rejestracji do usług opieki zdrowotnej lub podczas świadczenia jej usług opieki zdrowotnej, jak to określa dyrektywa Parlamentu Europejskiego i Rady 2011/24/UE ([1]); numer, symbol lub oznaczenie przypisane danej osobie fizycznej w celu jednoznacznego zidentyfikowania tej osoby fizycznej do celów zdrowotnych; informacje pochodzące z badań laboratoryjnych lub lekarskich części ciała lub płynów ustrojowych, w tym danych genetycznych i próbek biologicznych; oraz wszelkie informacje, na przykład o chorobie, niepełnosprawności, ryzyku choroby, historii medycznej, leczeniu klinicznym lub 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.

(36) Główną jednostką organizacyjną administratora w Unii powinno być miejsce, w którym znajduje się jego centralna administracja w Unii, chyba że decyzje co do celów i sposobów przetwarzania danych osobowych zapadają w innej jednostce organizacyjnej administratora w Unii, w którym to przypadku za główną jednostkę organizacyjną należy uznać tą drugą jednostkę organizacyjną. Główną jednostkę organizacyjną administratora w Unii należy określać na podstawie obiektywnych kryteriów; powinna ona oznaczać skuteczne i faktycznie

([1]) 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).

zarządzanie za pośrednictwem stabilnych struktur polegające na podejmowaniu najważniejszych decyzji co do celów i sposobów przetwarzania. Kryterium to nie powinno zależeć od faktu, czy przetwarzanie danych osobowych odbywa się w tej lokalizacji. Obecność i wykorzystywanie środków technicznych i technologii do przetwarzania danych osobowych lub do czynności przetwarzania nie stanowią same w sobie o głównej jednostce organizacyjnej, nie są więc kryteriami decydującymi o jej określeniu. Główną jednostką organizacyjną podmiotu przetwarzającego powinno być miejsce, w którym znajduje się jego centralna administracja w Unii, a jeżeli nie ma on centralnej administracji w Unii – miejsce, w którym odbywają się główne czynności przetwarzania w Unii. Jeżeli sprawa dotyczy zarówno administratora, jak i podmiotu przetwarzającego, właściwym wiodącym organem nadzorczym powinien pozostać organ nadzorczy państwa członkowskiego, w którym administrator ma główną jednostkę organizacyjną, ale organ nadzorczy podmiotu przetwarzającego powinien być uznawany za organ nadzorczy, którego sprawa dotyczy, i powinien uczestniczyć w procedurze współpracy przewidzianej w niniejszym rozporządzeniu. Organy nadzorcze państwa członkowskiego lub państw członkowskich, w których podmiot przetwarzający ma co najmniej jedną jednostkę organizacyjną, nie powinny być w żadnym przypadku uznawane za organy nadzorcze, których sprawa dotyczy, jeżeli projekt decyzji dotyczy wyłącznie administratora. Jeżeli przetwarzania dokonuje grupa przedsiębiorstw, za jej główną jednostkę organizacyjną należy uznać główną jednostkę organizacyjną przedsiębiorstwa sprawującego kontrolę, chyba że cel i sposoby przetwarzania określa inne przedsiębiorstwo.

(37) Grupa przedsiębiorstw powinna obejmować przedsiębiorstwo sprawujące kontrolę oraz przedsiębiorstwa kontrolowane, przy czym przedsiębiorstwo sprawujące kontrolę powinno być przedsiębiorstwem, które może wywierać dominujący wpływ na pozostałe przedsiębiorstwa ze względu na przykład na strukturę właścicielską, udział finansowy lub przepisy regulujące jego działalność, lub też uprawnienia do nakazywania wdrożenia przepisów o ochronie danych osobowych. Za grupę przedsiębiorstw należy uznać przedsiębiorstwo kontrolujące przetwarzanie danych osobowych w przedsiębiorstwach powiązanych z nim, wraz z tymi przedsiębiorstwami.

(38) Szczególnej ochrony danych osobowych wymagają dzieci, gdyż mogą one być mniej świadome ryzyka, konsekwencji, zabezpieczeń i praw przysługujących im w związku z przetwarzaniem danych osobowych. Taka szczególna ochrona powinna mieć zastosowanie przede wszystkim do wykorzystywania danych osobowych dzieci do celów marketingowych lub do tworzenia profili osobowych lub profili użytkownika oraz do zbierania danych osobowych dotyczących dzieci, gdy korzystają one z usług skierowanych bezpośrednio do nich. Zgoda osoby sprawującej władzę rodzicielską lub opiekę nie powinna być konieczna w przypadku usług profilaktycznych lub doradczych oferowanych bezpośrednio dziecku.

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

(40) Aby przetwarzanie danych było zgodne z prawem, powinno się odbywać na podstawie zgody osoby, której dane dotyczą, lub na innej uzasadnionej podstawie przewidzianej prawem: albo w niniejszym rozporządzeniu, albo

w innym akcie prawnym Unii lub w prawie państwa członkowskiego, o których mowa w niniejszym rozporządzeniu, w tym musi się ono odbywać z poszanowaniem obowiązku prawnego, któremu podlega administrator, lub z poszanowaniem umowy, której stroną jest osoba, której dane dotyczą, lub w celu podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy.

(41) W przypadku gdy w niniejszym rozporządzeniu jest mowa o podstawie prawnej lub akcie prawnym, niekoniecznie wymaga to przyjęcia aktu prawnego przez parlament, z zastrzeżeniem wymogów wynikających z porządku konstytucyjnego danego państwa członkowskiego. Taka podstawa prawna lub taki akt prawny powinny być jasne i precyzyjne, a ich zastosowanie przewidywalne dla osób im podlegających – jak wymaga tego orzecznictwo Trybunału Sprawiedliwości Unii Europejskiej (zwanego dalej „Trybunałem Sprawiedliwości") i Europejskiego Trybunału Praw Człowieka.

(42) Jeśli przetwarzanie odbywa się na podstawie zgody osoby, której dane dotyczą, administrator powinien być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na operację przetwarzania. W szczególności w przypadku pisemnego oświadczenia składanego w innej sprawie powinny istnieć gwarancje, że osoba, której dane dotyczą, jest świadoma wyrażenia zgody oraz jej zakresu. Zgodnie z dyrektywą Rady 93/13/EWG ([1]) oświadczenie o wyrażeniu zgody przygotowane przez administratora powinno mieć zrozumiałą i łatwo dostępną formę, być sformułowane jasnym i prostym językiem i nie powinno zawierać nieuczciwych warunków. Aby wyrażenie zgody było świadome, osoba, której dane dotyczą, powinna znać przynajmniej tożsamość administratora oraz zamierzone cele przetwarzania danych osobowych. Wyrażenia zgody nie należy uznawać za dobrowolne, jeżeli osoba, której dane dotyczą, nie ma rzeczywistego lub wolnego wyboru oraz nie może odmówić ani wycofać zgody bez niekorzystnych konsekwencji.

(43) Aby zapewnić dobrowolność, zgoda nie powinna stanowić ważnej podstawy prawnej przetwarzania danych osobowych w szczególnej sytuacji, w której istnieje wyraźny brak równowagi między osobą, której dane dotyczą, a administratorem, w szczególności gdy administrator jest organem publicznym i dlatego jest mało prawdopodobne, by w tej konkretnej sytuacji zgodę wyrażono dobrowolnie we wszystkich przypadkach. Zgody nie uważa się za dobrowolną, jeżeli nie można jej wyrazić z osobna na różne operacje przetwarzania danych osobowych, mimo że w danym przypadku byłoby to stosowne, lub jeżeli od zgody uzależnione jest wykonanie umowy – w tym świadczenie usługi – mimo że do jej wykonania zgoda nie jest niezbędna.

(44) Przetwarzanie powinno być zgodne z prawem, jeżeli jest ono niezbędne w związku z zawarciem umowy lub zamiarem zawarcia umowy.

(45) Jeżeli przetwarzanie odbywa się w celu wypełnienia obowiązku prawnego, któremu podlega administrator, lub jeżeli jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej, podstawę przetwarzania powinno stanowić prawo Unii lub prawo państwa członkowskiego. Niniejsze rozporządzenie nie nakłada wymogu, aby dla każdego indywidualnego przetwarzania istniało szczegółowe uregulowanie prawne. Wystarczyć może to, że dane uregulowanie prawne stanowi podstawę różnych operacji przetwarzania wynikających z obowiązku prawnego, któremu podlega administrator, lub że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej. Prawo Unii lub prawo państwa członkowskiego powinno określać także cel przetwarzania. Ponadto prawo to może doprecyzowywać ogólne warunki określone w niniejszym rozporządzeniu dotyczące zgodności przetwarzania z prawem, określać sposoby wskazywania administratora, rodzaj danych osobowych podlegających przetwarzaniu, osoby, których dane dotyczą, podmioty, którym można ujawniać dane osobowe, ograniczenia celu, okres przechowywania oraz inne środki zapewniające zgodność z prawem i rzetelność przetwarzania. Prawo Unii lub prawo państwa członkowskiego powinno określać także, czy administratorem wykonującym zadanie realizowane w interesie publicznym lub w ramach sprawowania władzy publicznej powinien być organ publiczny czy inna osoba fizyczna lub prawna podlegająca prawu publicznemu lub prawu prywatnemu, na przykład zrzeszenie zawodowe, jeżeli uzasadnia to interes publiczny, w tym cele zdrowotne, takie jak zdrowie publiczne, ochrona socjalna oraz zarządzanie usługami opieki zdrowotnej.

(46) Przetwarzanie danych osobowych należy uznać za zgodne z prawem również w przypadkach, gdy jest niezbędne do ochrony interesu, który ma istotne znaczenie dla życia osoby, której dane dotyczą, lub innej osoby fizycznej. Żywotny interes innej osoby fizycznej powinien zasadniczo być podstawą przetwarzania danych osobowych

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

wyłącznie w przypadkach, gdy ewidentnie przetwarzania tego nie da się oprzeć na innej podstawie prawnej. Niektóre rodzaje przetwarzania mogą służyć zarówno ważnemu interesowi publicznemu, jak i żywotnym interesom osoby, której dane dotyczą, na przykład gdy przetwarzanie jest niezbędne do celów humanitarnych, w tym monitorowania epidemii i ich rozprzestrzeniania się lub w nadzwyczajnych sytuacjach humanitarnych, w szczególności w przypadku klęsk żywiołowych i katastrof spowodowanych przez człowieka.

(47) Podstawą prawną przetwarzania mogą być prawnie uzasadnione interesy administratora, w tym administratora, któremu mogą zostać ujawnione dane osobowe, lub strony trzeciej, o ile w świetle rozsądnych oczekiwań osób, których dane dotyczą, opartych na ich powiązaniach z administratorem nadrzędne nie są interesy lub podstawowe prawa i wolności osoby, której dane dotyczą. Taki prawnie uzasadniony interes może istnieć na przykład w przypadkach, gdy zachodzi istotny i odpowiedni rodzaj powiązania między osobą, której dane dotyczą, a administratorem, na przykład gdy osoba, której dane dotyczą, jest klientem administratora lub działa na jego rzecz. Aby stwierdzić istnienie prawnie uzasadnionego interesu, należałoby w każdym przypadku przeprowadzić dokładną ocenę, w tym ocenę tego, czy w czasie i w kontekście, w którym zbierane są dane osobowe, osoba, której dane dotyczą, ma rozsądne przesłanki by spodziewać się, że może nastąpić przetwarzanie danych w tym celu. Interesy i prawa podstawowe osoby, której dane dotyczą, mogą być nadrzędne wobec interesu administratora danych w szczególności w przypadkach, gdy dane osobowe są przetwarzane w sytuacji, w której osoby, których dane dotyczą, nie mają rozsądnych przesłanek, by spodziewać się dalszego przetwarzania. Ponieważ dla organów publicznych podstawę prawną przetwarzania danych osobowych powinien określić ustawodawca, prawnie uzasadniony interes administratora nie powinien mieć zastosowania jako podstawa prawna do przetwarzania, którego dokonują organy publiczne w ramach realizacji swoich zadań. Prawnie uzasadnionym interesem administratora, którego sprawa dotyczy, jest również przetwarzanie danych osobowych bezwzględnie niezbędne do zapobiegania oszustwom. Za działanie wykonywane w prawnie uzasadnionym interesie można uznać przetwarzanie danych osobowych do celów marketingu bezpośredniego.

(48) Administratorzy, którzy są częścią grupy przedsiębiorstw lub instytucji powiązanych z podmiotem centralnym, mogą mieć prawnie uzasadniony interes w przesyłaniu danych osobowych w ramach grupy przedsiębiorstw do wewnętrznych celów administracyjnych, co dotyczy też przetwarzania danych osobowych klientów lub pracowników. Pozostaje to bez wpływu na ogólne zasady przekazywania danych osobowych w ramach grupy przedsiębiorstw przedsiębiorstwu mieszczącemu się w państwie trzecim.

(49) Przetwarzanie danych osobowych w zakresie bezwzględnie niezbędnym i proporcjonalnym do zapewnienia bezpieczeństwa sieci i informacji – tj. zapewnienia odporności sieci lub systemu informacyjnego na danym poziomie poufności na przypadkowe zdarzenia albo niezgodne z prawem lub nieprzyjazne działania naruszające dostępność, autentyczność, integralność i poufność przechowywanych lub przesyłanych danych osobowych – oraz bezpieczeństwa związanych z nimi usług oferowanych lub udostępnianych poprzez te sieci i systemy przez organy publiczne, zespoły reagowania na zagrożenia komputerowe, zespoły reagowania na komputerowe incydenty naruszające bezpieczeństwo, dostawców sieci i usług łączności elektronicznej oraz dostawców technologii i usług w zakresie bezpieczeństwa jest prawnie uzasadnionym interesem administratora, którego sprawa dotyczy. Może to obejmować na przykład zapobieganie nieuprawnionemu dostępowi do sieci łączności elektronicznej i rozprowadzaniu złośliwych kodów, przerywanie ataków typu „odmowa usługi", a także przeciwdziałanie uszkodzeniu systemów komputerowych i systemów łączności elektronicznej.

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

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

Jeżeli osoba, której dane dotyczą, wyraziła zgodę lub jeżeli przetwarzanie ma za podstawę prawo Unii lub prawo państwa członkowskiego stanowiące w demokratycznym społeczeństwie niezbędny i proporcjonalny środek, który zapewnia w szczególności realizację ważnych celów leżących w ogólnym interesie publicznym, administrator powinien móc dokonać dalszego przetwarzania danych osobowych, bez względu na jego zgodność z pierwotnymi celami. W każdym przypadku należy zapewnić stosowanie zasad przewidzianych w niniejszym rozporządzeniu, w szczególności stosowanie zasady informowania osoby, której dane dotyczą, o tych innych celach oraz o jej prawach, w tym prawie do sprzeciwu. Wskazanie przez administratora ewentualnych czynów zabronionych czy zagrożeń dla bezpieczeństwa publicznego oraz przesłanie w indywidualnym przypadku – lub w różnych przypadkach związanych z tym samym czynem zabronionym lub zagrożeniem dla bezpieczeństwa publicznego – odpowiednich danych osobowych właściwemu organowi należy uznać za zrealizowanie przez administratora prawnie uzasadnionego interesu. Jednak takie przesłanie w prawnie uzasadnionym interesie administratora lub dalsze przetwarzanie danych osobowych powinno być zabronione, jeżeli jest niezgodne z prawnym, zawodowym lub innym wiążącym obowiązkiem zachowania tajemnicy.

(51) Dane osobowe, które z racji swego charakteru są szczególnie wrażliwe w świetle podstawowych praw i wolności, wymagają szczególnej ochrony, gdyż kontekst ich przetwarzania może powodować poważne ryzyko dla podstawowych praw i wolności. Do takich danych osobowych powinny zaliczać się dane osobowe ujawniające pochodzenie rasowe lub etniczne, przy czym użycie w niniejszym rozporządzeniu terminu „pochodzenie rasowe" nie oznacza, że Unia akceptuje teorie sugerujące istnienie osobnych ras ludzkich. Przetwarzanie fotografii nie powinno zawsze stanowić przetwarzania szczególnych kategorii danych osobowych, gdyż fotografie są objęte definicją „danych biometrycznych" tylko w przypadkach, gdy są przetwarzane specjalnymi metodami technicznymi, umożliwiającymi jednoznaczną identyfikację osoby fizycznej lub potwierdzenie jej tożsamości. Takich danych osobowych nie należy przetwarzać, chyba że niniejsze rozporządzenie dopuszcza ich przetwarzanie w szczególnych przypadkach, przy czym należy uwzględnić, że prawo państw członkowskich może obejmować przepisy szczegółowe o ochronie danych dostosowujące zastosowanie przepisów niniejszego rozporządzenia tak, by można było wypełnić obowiązki prawne lub wykonać zadanie realizowane w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi. Oprócz wymogów szczegółowych mających zastosowanie do takiego przetwarzania, zastosowanie powinny mieć zasady ogólne i inne przepisy niniejszego rozporządzenia, w szczególności jeżeli chodzi o warunki zgodności przetwarzania z prawem. Należy wyraźnie przewidzieć wyjątki od ogólnego zakazu przetwarzania takich szczególnych kategorii danych osobowych, m.in. w razie wyraźnej zgody osoby, której dane dotyczą, lub ze względu na szczególne potrzeby, w szczególności gdy przetwarzanie danych odbywa się w ramach uzasadnionych działań niektórych zrzeszeń lub fundacji, których celem jest umożliwienie korzystania z podstawowych wolności.

(52) Należy również zezwolić na wyjątki od zakazu przetwarzania szczególnych kategorii danych osobowych – o ile przewiduje to prawo Unii lub prawo państwa członkowskiego i podlega to odpowiednim zabezpieczeniom chroniącym dane osobowe i inne prawa podstawowe – jeżeli uzasadnia to interes publiczny, w szczególności polegający na przetwarzaniu danych osobowych w dziedzinie prawa pracy, prawa zabezpieczenia społecznego, w tym emerytur, oraz do celów bezpieczeństwa, monitorowania i ostrzegania zdrowotnego, zapobiegania chorobom zakaźnym i innym poważnym zagrożeniom zdrowotnym. Taki wyjątek może być przewidziany ze względu na cele zdrowotne, w tym związane ze zdrowiem publicznym oraz zarządzaniem usługami opieki zdrowotnej, w szczególności zapewnianiem jakości i ekonomiczności procedur stosowanych do rozstrzygania roszczeń w sprawie świadczeń i usług w ramach systemu ubezpieczeń zdrowotnych, lub ze względu na cele archiwalne w interesie publicznym, cele badań naukowych lub historycznych lub cele statystyczne. Należy także przewidzieć wyjątek pozwalający przetwarzać takie dane osobowe, jeżeli jest to niezbędne do ustalenia, dochodzenia lub obrony roszczeń w postępowaniu sądowym, administracyjnym lub też innym postępowaniu pozasądowym.

(53) Szczególne kategorie danych osobowych zasługujące na większą ochronę powinny być przetwarzane do celów zdrowotnych wyłącznie w przypadkach, gdy jest to niezbędne do realizacji tych celów z korzyścią dla osób fizycznych i ogółu społeczeństwa, w szczególności w kontekście zarządzania usługami i systemami opieki zdrowotnej i zabezpieczenia społecznego, w tym przetwarzania takich danych przez organy zarządcze i centralne krajowe organy ds. zdrowia do celów kontroli jakości, pozyskiwania informacji zarządczych oraz ogólnego krajowego i lokalnego nadzoru nad systemem opieki zdrowotnej i zabezpieczenia społecznego oraz zapewniania ciągłości opieki zdrowotnej lub zabezpieczenia społecznego oraz transgranicznej opieki zdrowotnej lub do celów bezpieczeństwa, monitorowania i ostrzegania zdrowotnego lub do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, które mają podstawę w prawie Unii lub prawie państwa członkowskiego i służą interesowi publicznemu, a także na potrzeby analiz prowadzonych w interesie publicznym w dziedzinie zdrowia publicznego. Niniejsze rozporządzenie powinno zatem przewidywać zharmonizowane warunki przetwarzania szczególnych kategorii danych osobowych dotyczących zdrowia, ze względu na szczególne potrzeby, w szczególności gdy dane takie są przetwarzane w określonych

celach zdrowotnych przez osoby podlegające prawnemu obowiązkowi zachowania tajemnicy zawodowej. Prawo Unii lub prawo państwa członkowskiego powinny przewidywać konkretne, odpowiednie środki chroniące prawa podstawowe i dane osobowe osób fizycznych. Państwa członkowskie powinny móc zachować lub wprowadzić dalsze warunki, w tym ograniczenia, przetwarzania danych genetycznych, danych biometrycznych lub danych dotyczących zdrowia. Warunki te nie powinny jednak utrudniać swobodnego przepływu danych osobowych w Unii, jeżeli odnoszą się do transgranicznego przetwarzania takich danych.

(54) Niezbędne z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego może być przetwarzanie szczególnych kategorii danych osobowych bez zgody osoby, której dane dotyczą. Przetwarzanie takie powinno podlegać konkretnym, odpowiednim środkom chroniącym prawa i wolności osób fizycznych. W tym kontekście „zdrowie publiczne" należy interpretować zgodnie z definicją z rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 1338/2008 ([1]), czyli jako wszystkie elementy związane ze zdrowiem, mianowicie stan zdrowia, w tym zachorowalność i niepełnosprawność, czynniki warunkujące stan zdrowia, potrzeby w zakresie opieki zdrowotnej, zasoby opieki zdrowotnej, oferowane usługi opieki zdrowotnej i powszechny dostęp do nich, wydatki na opiekę zdrowotną i sposób jej finansowania oraz przyczyny zgonów. Przetwarzanie danych dotyczących zdrowia z uwagi na względy interesu publicznego nie powinno skutkować przetwarzaniem danych osobowych do innych celów przez strony trzecie, takie jak pracodawcy, czy zakłady ubezpieczeń i banki.

(55) Przetwarzanie danych osobowych przez organy publiczne do celów – określonych w prawie konstytucyjnym lub prawie międzynarodowym publicznym – oficjalnie uznanych związków wyznaniowych odbywa się w interesie publicznym.

(56) Jeżeli w ramach działań związanych z wyborami funkcjonowanie systemu demokratycznego w państwie członkowskim wymaga zbierania przez partie polityczne danych osobowych dotyczących poglądów politycznych obywateli, można zezwolić na przetwarzanie tych danych z uwagi na względy interesu publicznego pod warunkiem ustanowienia odpowiednich zabezpieczeń.

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

(58) Zasada przejrzystości wymaga, by wszelkie informacje kierowane do ogółu społeczeństwa lub osoby, której dane dotyczą, były zwięzłe, łatwo dostępne i zrozumiałe, by były formułowane jasnym i prostym językiem, a w stosownych przypadkach, dodatkowo wizualizowane. Informacje te mogą być przekazywane w formie elektronicznej, na przykład za pomocą strony internetowej, gdy są kierowane do ogółu społeczeństwa. Dotyczy to w szczególności sytuacji, gdy duża liczba podmiotów i złożoność technologiczna działań sprawiają, że osobie, której dane dotyczą, trudno jest dowiedzieć się i zrozumieć, czy dotyczące jej dane osobowe są zbierane, przez kogo oraz w jakim celu, na przykład w przypadku reklamy w internecie. Zważywszy że dzieci zasługują na szczególną ochronę, wszelkie informacje i komunikaty – gdy przetwarzanie dotyczy dziecka – powinny być sformułowane tak jasnym i prostym językiem, by dziecko mogło je bez trudu zrozumieć.

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

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

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

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

(62) Nałożenie obowiązku udzielenia informacji nie jest jednak konieczne, jeżeli osoba, której dane dotyczą, dysponuje już tymi informacjami, jeżeli utrwalenie lub ujawnienie danych są wyraźnie przewidziane prawem, lub jeżeli poinformowanie osoby, której dane dotyczą, okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku. Sytuacja braku możliwości lub niewspółmiernie dużego wysiłku może zachodzić w szczególności przypadku, gdy przetwarzanie służy celom archiwalnym w interesie publicznym, celom badań naukowych lub historycznych lub celom statystycznym. Uwzględnić przy tym należy liczbę osób, których dane dotyczą, okres przechowywania danych oraz wszelkie przyjęte odpowiednie zabezpieczenia.

(63) Każda osoba fizyczna powinna mieć prawo dostępu do zebranych danych jej dotyczących oraz powinna mieć możliwość łatwego wykonywania tego prawa w rozsądnych odstępach czasu, by mieć świadomość przetwarzania i móc zweryfikować zgodność przetwarzania z prawem. Obejmuje to prawo dostępu osób, których dane dotyczą, do danych dotyczących ich zdrowia, na przykład do danych w dokumentacji medycznej zawierającej takie informacje, jak diagnoza, wyniki badań, oceny dokonywane przez lekarzy prowadzących, stosowane terapie czy przeprowadzone zabiegi. Dlatego też każda osoba, której dane dotyczą, powinna mieć prawo do wiedzy i informacji, w szczególności w zakresie celów, w jakich dane osobowe są przetwarzane, w miarę możliwości okresu, przez jaki dane osobowe są przetwarzane, odbiorców danych osobowych, założeń ewentualnego zautomatyzowanego przetwarzania danych osobowych oraz, przynajmniej w przypadku profilowania, konsekwencji takiego przetwarzania. W miarę możliwości administrator powinien mieć możliwość udzielania zdalnego dostępu do bezpiecznego systemu, który zapewni osobie, której dane dotyczą, bezpośredni dostęp do jej danych osobowych. Prawo to nie powinno negatywnie wpływać na prawa lub wolności innych osób, w tym tajemnice handlowe lub własność intelektualną, w szczególności na prawa autorskie chroniące oprogramowanie. Względy te nie powinny jednak skutkować odmową udzielenia osobie, której dane dotyczą, jakichkolwiek informacji. Jeżeli administrator przetwarza duże ilości informacji o osobie, której dane dotyczą, powinien on mieć możliwość zażądania, przed podaniem informacji, by osoba, której dane dotyczą, sprecyzowała informacje lub czynności przetwarzania, których dotyczy jej żądanie.

(64) Administrator powinien skorzystać z wszelkich rozsądnych środków w celu zweryfikowania tożsamości żądającej dostępu osoby, której dane dotyczą, w szczególności w kontekście usług internetowych i identyfikatorów internetowych. Administrator nie powinien zatrzymywać danych osobowych wyłącznie w celu reagowania na ewentualne żądania.

(65) Każda osoba fizyczna powinna mieć prawo do sprostowania danych osobowych jej dotyczących oraz prawo do „bycia zapomnianym", jeżeli zatrzymywanie takich danych narusza niniejsze rozporządzenie, prawo Unii lub prawo państwa członkowskiego, któremu podlega administrator. Osoba, której dane dotyczą, powinna w szczególności mieć prawo do tego, by jej dane osobowe zostały usunięte i przestały być przetwarzane, jeżeli dane te nie są już niezbędne do celów, w których były zbierane lub w inny sposób przetwarzane, jeżeli osoba, której dane dotyczą, cofnęła zgodę lub jeżeli wniosła sprzeciw wobec przetwarzania danych osobowych jej dotyczących, lub jeżeli przetwarzanie jej danych osobowych nie jest z innego powodu zgodne z niniejszym rozporządzeniem. Prawo to ma znaczenie w przypadkach, gdy osoba, której dane dotyczą, wyraziła zgodę jako dziecko, gdy nie była w pełni świadoma ryzyka związanego z przetwarzaniem, a w późniejszym czasie chce usunąć takie dane osobowe, w szczególności z internetu. Osoba, której dane dotyczą, powinna móc wykonywać

to prawo, mimo że już nie jest dzieckiem. Niemniej dalsze zatrzymywanie danych osobowych powinno być uznane za zgodne z prawem, jeżeli jest niezbędne do korzystania z wolności wypowiedzi i informacji, do wywiązania się z obowiązku prawnego, do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi, z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego, do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych lub do ustalenia, dochodzenia lub obrony roszczeń.

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

(67) Wśród metod pozwalających ograniczyć przetwarzanie danych osobowych mogą się znaleźć między innymi: czasowe przeniesienie wybranych danych osobowych do innego systemu przetwarzania, uniemożliwienie użytkownikom dostępu do wybranych danych, lub czasowe usunięcie opublikowanych danych ze strony internetowej. W zautomatyzowanych zbiorach danych przetwarzanie należy zasadniczo ograniczyć środkami technicznymi w taki sposób, by dane osobowe nie podlegały dalszemu przetwarzaniu ani nie mogły być zmieniane. Fakt ograniczenia przetwarzania danych osobowych należy wyraźnie zaznaczyć w systemie.

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

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

(70) Jeżeli dane osobowe są przetwarzane do celów marketingu bezpośredniego, osoba, której dane dotyczą, powinna mieć prawo wnieść w dowolnym momencie, bezpłatnie sprzeciw wobec tego przetwarzania, pierwotnego lub dalszego – w tym profilowania, o ile jest ono powiązane z marketingiem bezpośrednim. Prawo to powinno zostać wyraźnie podane do wiadomości osobie, której dane dotyczą, oraz powinno być przedstawione jasno i oddzielnie od wszelkich innych informacji.

(71) Osoba, której dane dotyczą, powinna mieć prawo do tego, by nie podlegać decyzji – mogącej obejmować określone środki – która ocenia jej czynniki osobowe, opiera się wyłącznie na przetwarzaniu zautomatyzowanym i wywołuje wobec osoby, której dane dotyczą, skutki prawne lub w podobny sposób znacząco na nią wpływa, jak na przykład automatyczne odrzucenie elektronicznego wniosku kredytowego czy elektroniczne metody rekrutacji bez interwencji ludzkiej. Do takiego przetwarzania zalicza się „profilowanie" – które polega na dowolnym zautomatyzowanym przetwarzaniu danych osobowych pozwalającym ocenić czynniki osobowe osoby fizycznej, a w szczególności analizować lub prognozować aspekty dotyczące efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się osoby, której dane dotyczą – o ile wywołuje skutki prawne względem tej osoby lub w podobny sposób znacząco na nią wpływa. Niemniej podejmowanie decyzji na podstawie takiego przetwarzania, w tym profilowania, powinno być dozwolone, w przypadku gdy jest to wyraźnie dopuszczone prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator, w tym do celów monitorowania i zapobiegania – zgodnie z uregulowaniami, standardami i zaleceniami instytucji Unii lub krajowych podmiotów nadzorujących – oszustwom i uchylaniu się od podatków oraz do zapewniania bezpieczeństwa i niezawodności usług świadczonych przez administratora, lub gdy jest niezbędne do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a administratorem, lub gdy osoba, której dane dotyczą, wyraziła wyraźną zgodę. Przetwarzanie takie powinno zawsze podlegać odpowiednim zabezpieczeniom, obejmującym informowanie osoby, której dane dotyczą, prawo do uzyskania interwencji człowieka, prawo do wyrażenia własnego stanowiska, prawo do uzyskania wyjaśnienia co do decyzji wynikłej z takiej oceny oraz prawo do zakwestionowania takiej decyzji. Takie przetwarzanie nie powinno dotyczyć dzieci.

Aby zapewnić rzetelność i przejrzystość przetwarzania wobec osoby, której dane dotyczą, mając na uwadze konkretne okoliczności i kontekst przetwarzania danych osobowych, administrator powinien stosować odpowiednie matematyczne lub statystyczne procedury profilowania, wdrożyć środki techniczne i organizacyjne zapewniające w szczególności korektę powodujcych nieprawidłowości w danych osobowych i maksymalne zmniejszenie ryzyka błędów, zabezpieczyć dane osobowe w sposób uwzględniający potencjalne ryzyko dla interesów i praw osoby, której dane dotyczą, oraz zapobiegający m.in. skutkom w postaci dyskryminacji osób fizycznych z uwagi na pochodzenie rasowe lub etniczne, poglądy polityczne, wyznanie lub przekonania, przynależność do związków zawodowych, stan genetyczny lub zdrowotny, orientację seksualną lub skutkujący środkami mającymi taki efekt. Zautomatyzowane podejmowanie decyzji i profilowanie oparte na szczególnych kategoriach danych osobowych powinny być dozwolone wyłącznie przy zachowaniu szczególnych warunków.

(72) Profilowanie podlega przepisom niniejszego rozporządzenia dotyczącym przetwarzania danych osobowych, takim jak przepisy określające podstawy prawne przetwarzania lub zasady ochrony danych. Europejska Rada Ochrony Danych ustanowiona niniejszym rozporządzeniem powinna mieć możliwość wydawania wskazówek w tym względzie.

(73) W prawie Unii lub w prawie państwa członkowskiego można przewidzieć ograniczenia dotyczące określonych zasad oraz prawa do informacji, dostępu do danych osobowych i ich sprostowania lub usuwania, prawa do przenoszenia danych, prawa do sprzeciwu, decyzji opartych na profilowaniu, zawiadamiania osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych oraz określonych powiązanych obowiązków administratorów, o ile jest to niezbędne i proporcjonalne w społeczeństwie demokratycznym, by zapewnić bezpieczeństwo publiczne, w tym ochronę życia ludzkiego – w szczególności w ramach reakcji na klęski żywiołowe lub katastrofy spowodowane przez człowieka – zapobieganie przestępczości, prowadzenie postępowań przygotowawczych, ściganie czynów zabronionych, lub wykonywanie kar, w tym ochronę przed zagrożeniami dla bezpieczeństwa publicznego i zapobieganie takim zagrożeniom lub zapobieganie naruszeniom zasad etyki w zawodach regulowanych, ochronę innych ważnych celów leżących w ogólnym interesie publicznym Unii lub państwa członkowskiego, w szczególności ważnego interesu gospodarczego lub finansowego Unii lub państwa członkowskiego, prowadzenie rejestrów publicznych z uwagi na względy ogólnego interesu publicznego, dalsze przetwarzanie zarchiwizowanych danych osobowych w celu dostarczenia konkretnych informacji o postawie politycznej w ramach dawnych systemów państw totalitarnych lub ochronę osoby, której dane dotyczą, lub praw i wolności innych osób, w tym cele w dziedzinie ochrony socjalnej, zdrowia publicznego i cele humanitarne. Ograniczenia te powinny być zgodne z wymogami Karty praw podstawowych oraz Europejskiej konwencji o ochronie praw człowieka i podstawowych wolności.

(74) Należy nałożyć na administratora obowiązki i ustanowić odpowiedzialność prawną administratora za przetwarzanie danych osobowych przez niego samego lub w jego imieniu. W szczególności administrator powinien mieć obowiązek wdrożenia odpowiednich i skutecznych środków oraz powinien być w stanie wykazać, że czynności przetwarzania są zgodne z niniejszym rozporządzeniem oraz, że są skuteczne. Środki te powinny uwzględniać charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw i wolności osób fizycznych.

(75) Ryzyko naruszenia praw lub wolności osób, o różnym prawdopodobieństwie i wadze zagrożeń, może wynikać z przetwarzania danych osobowych mogącego prowadzić do uszczerbku fizycznego lub szkód majątkowych lub niemajątkowych, w szczególności: jeżeli przetwarzanie może poskutkować dyskryminacją, kradzieżą tożsamości lub oszustwem dotyczącym tożsamości, stratą finansową, naruszeniem dobrego imienia, naruszeniem poufności danych osobowych chronionych tajemnicą zawodową, nieuprawnionym odwróceniem pseudonimizacji lub wszelką inną znaczną szkodą gospodarczą lub społeczną; jeżeli osoby, których dane dotyczą, mogą zostać pozbawione przysługujących im praw i wolności lub możliwości sprawowania kontroli nad swoimi danymi osobowymi; jeżeli przetwarzane są dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, wyznanie lub przekonania światopoglądowe, lub przynależność do związków zawodowych oraz jeżeli przetwarzane są dane genetyczne, dane dotyczące zdrowia lub dane dotyczące seksualności lub wyroków skazujących i naruszeń prawa lub związanych z tym środków bezpieczeństwa; jeżeli oceniane są czynniki osobowe, w szczególności analizowane lub prognozowane aspekty dotyczące efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się – w celu tworzenia lub wykorzystywania profili osobistych; lub jeżeli przetwarzane są dane osobowe osób wymagających szczególnej opieki, w szczególności dzieci; jeżeli przetwarzanie dotyczy dużej ilości danych osobowych i wpływa na dużą liczbę osób, których dane dotyczą.

(76) Prawdopodobieństwo i powagę ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, należy określić poprzez odniesienie się do charakteru, zakresu, kontekstu i celów przetwarzania danych. Ryzyko należy oszacować na podstawie obiektywnej oceny, w ramach której stwierdza się, czy z operacjami przetwarzania danych wiąże się ryzyko lub wysokie ryzyko.

(77) Wskazówki co do tego, jak wdrożyć odpowiednie środki oraz wykazać przestrzeganie prawa przez administratora lub podmiot przetwarzający dane – w szczególności jeżeli chodzi o identyfikowanie ryzyka związanego z przetwarzaniem, o jego ocenę pod kątem źródła, charakteru, prawdopodobieństwa i wagi zagrożenia oraz o najlepsze praktyki pozwalające zminimalizować to ryzyko – mogą być przekazane w szczególności w formie zatwierdzonych kodeksów postępowania, zatwierdzonej certyfikacji, wytycznych Europejskiej Rady Ochrony Danych lub poprzez sugestie inspektora ochrony danych. Europejska Rada Ochrony Danych może wydawać wytyczne także w sprawie operacji przetwarzania, których nie uznaje się za mogące powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, i wskazywać, jakie środki mogą wystarczyć w takich przypadkach dla zaradzenia takiemu ryzyku.

(78) Ochrona praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych wymaga wdrożenia odpowiednich środków technicznych i organizacyjnych, by zapewnić spełnienie wymogów niniejszego rozporządzenia. Aby móc wykazać przestrzeganie niniejszego rozporządzenia, administrator powinien przyjąć wewnętrzne polityki i wdrożyć środki, które są zgodne w szczególności z zasadą uwzględniania ochrony danych w fazie projektowania oraz z zasadą domyślnej ochrony danych. Takie środki mogą polegać m.in. na minimalizacji przetwarzania danych osobowych, jak najszybszej pseudonimizacji danych osobowych, przejrzystości co do funkcji i przetwarzania danych osobowych, umożliwieniu osobie, której dane dotyczą, monitorowania przetwarzania danych, umożliwieniu administratorowi tworzenia i doskonalenia zabezpieczeń. Jeżeli opracowywane, projektowane, wybierane i użytkowane są aplikacje, usługi i produkty, które opierają się na przetwarzaniu danych osobowych albo przetwarzają dane osobowe w celu realizacji swojego zadania, należy zachęcać wytwórców tych produktów, usług i aplikacji, by podczas opracowywania i projektowania takich produktów, usług i aplikacji wzięli pod uwagę prawo do ochrony danych osobowych i z należytym uwzględnieniem stanu wiedzy technicznej zapewnili administratorom i podmiotom przetwarzającym możliwość wywiązania się ze spoczywających na nich obowiązków ochrony danych. Zasadę uwzględniania ochrony danych w fazie projektowania i zasadę domyślnej ochrony danych należy też brać pod uwagę w przetargach publicznych.

(79) 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 w ramach niniejszego rozporządzenia jasnego podziału obowiązków, także w sytuacji, gdy administrator określa cele i sposoby przetwarzania wspólnie z innymi administratorami lub gdy operacji przetwarzania dokonuje się w imieniu administratora.

(80) Gdy administrator lub podmiot przetwarzający niemający jednostki organizacyjnej w Unii przetwarza dane osobowe osób, których dane dotyczą, znajdujących się w Unii, a jego czynności przetwarzania wiążą się z oferowaniem towarów lub usług tym osobom w Unii (niezależnie od tego, czy wymaga od tych osób płatności) lub z monitorowaniem ich zachowania (o ile ma ono miejsce w Unii), to taki administrator lub podmiot przetwarzający powinien wyznaczyć przedstawiciela, chyba że przetwarzanie ma charakter sporadyczny, nie obejmuje – na dużą skalę – przetwarzania szczególnych kategorii danych osobowych, ani przetwarzania danych osobowych dotyczących wyroków skazujących i naruszeń prawa, i jest mało prawdopodobne, by ze względu na swój charakter, kontekst, zakres i cele powodowało ryzyko naruszenia praw lub wolności osób fizycznych, lub jeżeli

administrator jest organem lub podmiotem publicznym. Przedstawiciel powinien działać w imieniu administratora lub podmiotu przetwarzającego i może być adresatem ewentualnych działań organu nadzorczego. Administrator lub podmiot przetwarzający powinien wyznaczyć przedstawiciela w wyraźny sposób za pomocą pisemnego upoważnienia do podejmowania działań w jego imieniu w odniesieniu do obowiązków administratora lub podmiotu przetwarzającego wynikających z niniejszego rozporządzenia. Wyznaczenie przedstawiciela nie wpływa na obowiązki lub odpowiedzialność prawną administratora lub podmiotu przetwarzającego wynikającą z niniejszego rozporządzenia. Przedstawiciel powinien wykonywać swoje zadania zgodnie z upoważnieniem otrzymanym od administratora lub podmiotu przetwarzającego, w tym współpracować z właściwymi organami nadzorczymi w odniesieniu do wszelkich działań służących zapewnieniu przestrzegania niniejszego rozporządzenia. W razie jego nieprzestrzegania przez administratora lub podmiot przetwarzający wyznaczony przedstawiciel powinien zostać poddany działaniom egzekucyjnym.

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

(82) Dla zachowania zgodności z niniejszym rozporządzeniem, administrator lub podmiot przetwarzający powinni prowadzić rejestry czynności przetwarzania, za które są odpowiedzialni. Każdy administrator i każdy podmiot przetwarzający powinni mieć obowiązek współpracować z organem nadzorczym i na jego żądanie udostępniać mu te rejestry w celu monitorowania tych operacji przetwarzania.

(83) W celu zachowania bezpieczeństwa i zapobiegania przetwarzaniu niezgodnemu z niniejszym rozporządzeniem administrator lub podmiot przetwarzający powinni oszacować ryzyko właściwe dla przetwarzania oraz wdrożyć środki – takie jak szyfrowanie – minimalizujące to ryzyko. Środki takie powinny zapewnić odpowiedni poziom bezpieczeństwa, w tym poufność, oraz uwzględniać stan wiedzy technicznej oraz koszty ich wdrożenia w stosunku do ryzyka i charakteru danych osobowych podlegających ochronie. Oceniając ryzyko w zakresie bezpieczeństwa danych, należy wziąć pod uwagę ryzyko związane z przetwarzaniem danych osobowych – takie jak przypadkowe lub niezgodne z prawem zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych – i mogące w szczególności prowadzić do uszczerbku fizycznego, szkód majątkowych lub niemajątkowych.

(84) Aby poprawić przestrzeganie niniejszego rozporządzenia, gdy operacje przetwarzania mogą wiązać się z wysokim ryzykiem naruszenia praw lub wolności osób fizycznych, należy zobowiązać administratora do dokonania oceny skutków dla ochrony danych w celu oszacowania w szczególności źródła, charakteru, specyfiki i powagi tego ryzyka. Wyniki oceny należy uwzględnić przy określaniu odpowiednich środków, które należy zastosować, by wykazać, że przetwarzanie danych osobowych odbywa się zgodnie z niniejszym rozporządzeniem. Jeżeli ocena skutków dla ochrony danych wykaże, że operacje przetwarzania powodują wysokie ryzyko, którego administrator nie może zminimalizować odpowiednimi środkami z punktu widzenia dostępnej technologii i kosztów wdrożenia, przed przetwarzaniem należy skonsultować się z organem nadzorczym.

(85) Przy braku odpowiedniej i szybkiej reakcji naruszenie ochrony danych osobowych może skutkować powstaniem uszczerbku fizycznego, szkód majątkowych lub 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 zawodową lub wszelkie inne znaczne szkody gospodarcze lub

społeczne. 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 naruszenie to mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych. Jeżeli nie można dokonać zgłoszenia w terminie 72 godzin, zgłoszeniu powinno towarzyszyć wyjaśnienie przyczyn opóźnienia, a informacje mogą być przekazywane stopniowo, bez dalszej zbędnej zwłoki.

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

(87) Należy się upewnić, czy wdrożono wszelkie odpowiednie techniczne środki ochrony i wszelkie odpowiednie środki organizacyjne, by od razu stwierdzić naruszenie ochrony danych osobowych i szybko poinformować organ nadzorczy i osobę, której dane dotyczą. To, czy zawiadomienia dokonano bez zbędnej zwłoki, należy ustalić z uwzględnieniem w szczególności charakteru i wagi naruszenia ochrony danych osobowych, jego konsekwencji oraz niekorzystnych skutków dla osoby, której dane dotyczą. Takie zawiadomienie może skutkować interwencją organu nadzorczego, zgodnie z jego zadaniami i uprawnieniami określonymi w niniejszym rozporządzeniu.

(88) Przy określaniu szczegółowych przepisów o formie i procedurach mających zastosowanie do zawiadamiania o naruszeniu ochrony danych osobowych należy wziąć pod uwagę okoliczności naruszenia, w tym fakt, czy dane osobowe były zabezpieczone odpowiednimi technicznymi środkami ochrony skutecznie ograniczającymi prawdopodobieństwo oszustwa dotyczącego tożsamości lub innych form nadużycia. W przepisach tych i procedurach należy ponadto uwzględnić prawnie uzasadnione interesy organów ścigania, jeżeli przedwczesne ujawnienie mogłoby niepotrzebnie utrudnić badanie okoliczności naruszenia ochrony danych osobowych.

(89) Dyrektywa 95/46/WE przewidywała ogólny obowiązek zawiadamiania organów nadzorczych o przetwarzaniu danych osobowych. Obowiązek ten powodując jednak obciążenia administracyjne i finansowe i nie zawsze przyczyniał się do poprawy ochrony danych osobowych. Dlatego należy znieść te powszechne, ogólne obowiązki zawiadamiania i zastąpić je skutecznymi procedurami i mechanizmami koncentrującymi się w zamian na tych rodzajach operacji przetwarzania, które ze względu na swój charakter, zakres, kontekst i cele mogą powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych. Takie rodzaje operacji przetwarzania obejmują w szczególności operacje, które wiążą się w szczególności z użyciem nowych technologii lub które są nowe i nie zostały jeszcze poddane przez administratora ocenie skutków dla ochrony danych lub stały się niezbędne z uwagi na upływ czasu od pierwotnego przetwarzania.

(90) W takim przypadku administrator powinien przed przetwarzaniem dokonać oceny skutków dla ochrony danych, aby ocenić konkretne prawdopodobieństwo i powagę tego wysokiego ryzyka, uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz źródła ryzyka. Ocena skutków powinna w szczególności obejmować planowane środki, zabezpieczenia i mechanizmy mające minimalizować to ryzyko, zapewniać ochronę danych osobowych oraz wykazać przestrzeganie niniejszego rozporządzenia.

(91) Powinno to mieć zastosowanie w szczególności do operacji przetwarzania o dużej skali – które służą przetwarzaniu znacznej ilości danych osobowych na szczeblu regionalnym, krajowym lub ponadnarodowym i które mogą wpłynąć na dużą liczbę osób, których dane dotyczą, oraz które mogą powodować wysokie ryzyko, na przykład (ze względu na swój szczególny charakter) gdy zgodnie ze stanem wiedzy technicznej stosowana jest na dużą skalę nowa technologia – oraz do innych operacji przetwarzania powodujących wysokie ryzyko naruszenia praw lub wolności osób, których dane dotyczą, w szczególności gdy operacje te utrudniają osobom, których dane dotyczą, wykonywanie przysługujących im praw. Oceny skutków dla ochrony danych należy także dokonywać w przypadkach, w których dane osobowe przetwarza się w celu podjęcia decyzji wobec konkretnej osoby fizycznej po dokonaniu systematycznej, kompleksowej oceny czynników osobowych osób fizycznych na podstawie profilowania tych danych lub po przetworzeniu szczególnych kategorii danych osobowych, danych biometrycznych lub danych osobowych dotyczących wyroków skazujących, naruszeń prawa lub odnośnych

środków bezpieczeństwa. Ocena skutków dla ochrony danych jest niezbędna również w przypadku monitorowania na dużą skalę miejsc publicznie dostępnych – w szczególności za pomocą urządzeń optyczno-elektronicznych – lub wszelkich innych operacji, względem których właściwy organ nadzorczy uznaje, że przetwarzanie może powodować wysokie ryzyko naruszenia praw lub wolności osób, których dane dotyczą, w szczególności dlatego, że operacje te uniemożliwiają osobom, których dane dotyczą, wykonywanie prawa lub korzystania z usługi lub umowy lub mają systematyczny charakter i dużą skalę. Przetwarzanie danych osobowych nie powinno być uznawane za przetwarzanie na dużą skalę, jeżeli dotyczy danych osobowych pacjentów lub klientów i jest dokonywane przez pojedynczego lekarza, innego pracownika służby zdrowia lub prawnika. W takich przypadkach ocena skutków dla ochrony danych nie powinna być obowiązkowa.

(92) W niektórych okolicznościach rozsądnie i korzystnie byłoby nie ograniczać oceny skutków dla ochrony danych do pojedynczego projektu, na przykład w przypadkach gdy organy lub podmioty publiczne zamierzają ustanowić wspólną aplikację lub platformę przetwarzania lub gdy kilku administratorów planuje wprowadzić wspólną aplikację lub środowisko przetwarzania obejmujące sektor lub segment gospodarki lub szeroko rozpowszechnioną działalność horyzontalną.

(93) Przyjmując prawo, które ma być dla organu lub podmiotu publicznego podstawą do wykonywania zadań i ma regulować konkretną operację przetwarzania lub konkretny zestaw operacji, państwa członkowskie mogą uznać, że przed takimi czynnościami przetwarzania należy koniecznie przeprowadzić taką ocenę.

(94) Jeżeli ocena skutków dla ochrony danych wykaże, że przy braku zabezpieczeń, środków bezpieczeństwa oraz mechanizmów minimalizujących ryzyko przetwarzanie powodowałoby wysokie ryzyko naruszenia praw lub wolności osób fizycznych, a administrator wyraża opinię, że ryzyka tego nie da się zminimalizować środkami rozsądnymi z punktu widzenia dostępnych technologii i kosztów wdrożenia, wtedy przed rozpoczęciem czynności przetwarzania należy skonsultować się z organem nadzorczym. Takie wysokie ryzyko mogą powodować pewne rodzaje przetwarzania oraz zakres i częstotliwość przetwarzania, które mogą skutkować także szkodą lub ingerencją w prawa i wolności osoby fizycznej. Na wniosek o konsultacje organ nadzorczy powinien odpowiedzieć w określonym terminie. Jednak brak reakcji ze strony organu nadzorczego w tym terminie nie powinien wykluczać interwencji tego organu zgodnie z jego zadaniami i uprawnieniami ustanowionymi w niniejszym rozporządzeniu, w tym uprawnieniami do zakazania operacji przetwarzania. W ramach konsultacji można przedłożyć organowi nadzorczemu wyniki oceny skutków dla ochrony danych dokonanej w odniesieniu do danego przetwarzania, a w szczególności środki planowane w celu zminimalizowania ryzyka naruszenia praw lub wolności osób fizycznych.

(95) W razie potrzeby i na żądanie podmiot przetwarzający powinien pomagać administratorowi w zapewnieniu przestrzegania obowiązków wynikających z dokonania oceny skutków dla ochrony danych oraz z uprzednich konsultacji z organem nadzorczym.

(96) Konsultacji z organem nadzorczym należy dokonać również w trakcie przygotowywania aktu ustawodawczego lub wykonawczego przewidującego przetwarzanie danych osobowych, aby zapewnić zgodność zamierzonego przetwarzania z niniejszym rozporządzeniem, a w szczególności zminimalizować ewentualne ryzyko dla osoby, której dane dotyczą.

(97) Jeżeli przetwarzania dokonuje organ publiczny z wyjątkiem sądów lub niezależnych organów wymiaru sprawiedliwości w ramach sprawowania wymiaru sprawiedliwości lub jeżeli w sektorze prywatnym przetwarzania dokonuje administrator, którego główna działalność polega na operacjach przetwarzania wymagających regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę lub jeżeli główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa, to w monitorowaniu wewnętrznego przestrzegania niniejszego rozporządzenia administrator lub podmiot przetwarzający powinni być wspomagani przez osobę dysponującą wiedzą fachową na temat prawa i praktyk w dziedzinie ochrony danych. W sektorze prywatnym przetwarzanie danych osobowych jest główną działalnością

administratora, jeżeli oznacza jego zasadnicze, a nie poboczne czynności. Niezbędny poziom wiedzy fachowej należy ustalić w szczególności w świetle prowadzonych operacji przetwarzania danych oraz ochrony, której wymagają dane osobowe przetwarzane przez administratora lub podmiot przetwarzający. Tacy inspektorzy ochrony danych – bez względu na to, czy są pracownikami administratora – powinni być w stanie wykonywać swoje obowiązki i zadania w sposób niezależny.

(98) Należy zachęcać zrzeszenia lub inne organy reprezentujące kategorie administratorów lub podmiotów przetwarzających do sporządzania kodeksów postępowania, w granicach niniejszego rozporządzenia, by ułatwiać skuteczne stosowanie niniejszego rozporządzenia, z uwzględnieniem szczególnych cech przetwarzania prowadzonego w niektórych sektorach i szczególnych potrzeb mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw. W takich kodeksach można w szczególności dopasować obowiązki administratorów i podmiotów przetwarzających do ryzyka naruszenia praw lub wolności osób fizycznych, jakie może powodować przetwarzanie.

(99) Sporządzając kodeks postępowania bądź zmieniając go lub rozszerzając jego zakres, zrzeszenia i inne organy reprezentujące kategorie administratorów lub podmiotów przetwarzających powinny konsultować się z odpowiednimi stronami, których sprawa dotyczy, w tym jeżeli jest to wykonalne, z osobami, których dane dotyczą, oraz mieć na względzie uwagi i opinie otrzymane w ramach takich konsultacji.

(100) Aby zwiększyć przejrzystość i poprawić przestrzeganie niniejszego rozporządzenia, należy zachęcać do ustanowienia mechanizmów certyfikacji oraz do wprowadzenia znaków jakości i oznaczeń w dziedzinie ochrony danych, pozwalając w ten sposób osobom, których dane dotyczą, szybko ocenić stopień ochrony danych, której podlegają stosowne produkty i usługi.

(101) Przepływ danych osobowych do państw spoza Unii i do organizacji międzynarodowych oraz z takich państw i z takich organizacji jest niezbędnym warunkiem rozwoju handlu międzynarodowego i współpracy międzynarodowej. Wzrost takiego przepływu spowodował nowe wyzwania i problemy w dziedzinie ochrony danych osobowych. 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 zapewnianego w Unii niniejszym rozporządzeniem, także w przypadkach dalszego przekazywania danych osobowych: z państwa trzeciego lub organizacji międzynarodowej administratorom lub pomiotom przetwarzającym w tym samym lub w innym państwie trzecim lub tej samej lub innej organizacji międzynarodowej. W każdym przypadku przekazywanie danych do państw trzecich i organizacji międzynarodowych może się odbywać wyłącznie w pełnej zgodzie z niniejszym rozporządzeniem. Przekazywanie może mieć miejsce wyłącznie w przypadkach, gdy administrator lub podmiot przetwarzający przestrzegają warunków określonych w przepisach niniejszego rozporządzenia dotyczących przekazywania danych osobowych państwom trzecim lub organizacjom międzynarodowym – z zastrzeżeniem pozostałych przepisów niniejszego rozporządzenia.

(102) Niniejsze rozporządzenie pozostaje bez uszczerbku dla umów międzynarodowych między Unią a państwami trzecimi regulujących przekazywanie danych osobowych, w tym zawierających odpowiednie zabezpieczania dla osób, których dane dotyczą. Państwa członkowskie mogą zawierać umowy międzynarodowe przewidujące m.in. przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych, o ile umowy takie nie wpływają na niniejsze rozporządzenie ani na inne przepisy prawa Unii i o ile przewidują odpowiedni stopień ochrony podstawowych praw osób, których dane dotyczą.

(103) Komisja może stwierdzić ze skutkiem dla całej Unii, że państwo trzecie – lub terytorium lub 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 przekazywanie danych osobowych do tego państwa trzeciego lub tej organizacji międzynarodowej może się odbywać bez potrzeby uzyskania dodatkowego zezwolenia. Komisja może także zdecydować, wcześniej informując o tym państwo trzecie lub organizację międzynarodową i przedstawiając im uzasadnienie, o cofnięciu takiej decyzji.

(104) Zgodnie z podstawowymi wartościami, na których opiera się Unia, w szczególności z ochroną praw człowieka, Komisja powinna w swojej ocenie państwa trzeciego lub terytorium lub określonego sektora w państwie trzecim 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 prawo karne. Przy przyjmowaniu decyzji stwierdzających odpowiedni stopień ochrony w odniesieniu do terytorium lub w określonego sektora w państwie trzecim, 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 ochrony zapewnianemu w Unii, w szczególności w przypadkach, gdy dane osobowe są przetwarzane w jednym szczególnym 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 i egzekwowalne prawa oraz skuteczne administracyjne i sądowe środki zaskarżenia.

(105) Pozazobowiązaniami międzynarodowymipaństwa trzeciego lub organizacji międzynarodowej, Komisja powinna brać pod uwagę obowiązki wynikające z udziału państwa trzeciego lub organizacji międzynarodowej w systemach wielostronnych lub regionalnych, w szczególności 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. Oceniając stopień ochrony w państwach trzecich lub organizacjach międzynarodowych, Komisja powinna konsultować się z Europejską Radą Ochrony Danych.

(106) Komisja powinna monitorować obowiązywanie decyzji o stopniu ochrony w państwie trzecim, na terytorium lub w określonym sektorze w państwie trzecim lub w organizacji międzynarodowej, oraz monitorować funkcjonowanie decyzji przyjętych na podstawie art. 25 ust. 6 lub art. 26 ust. 4 dyrektywy 95/46/WE. W swoich decyzjach stwierdzających odpowiedni stopień ochrony Komisja powinna przewidzieć mechanizm okresowego przeglądu ich funkcjonowania. Taki okresowy przegląd powinna ona przeprowadzać w konsultacji z danym państwem trzecim lub daną organizacją międzynarodową i powinna w nim uwzględniać wszelkie mające znaczenie zmiany w tym państwie trzecim lub tej organizacji międzynarodowej. Prowadząc monitorowanie i dokonując okresowych przeglądów, Komisja powinna uwzględnić stanowisko i wnioski Parlamentu Europejskiego i Rady, a także innych odpowiednich organów i źródeł. Komisja powinna w rozsądnym terminie ocenić funkcjonowanie decyzji wspomnianego drugiego typu i przekazać wszelkie odpowiednie wnioski komitetowi w rozumieniu rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 182/2011 ([1]) ustanowionemu na mocy niniejszego rozporządzenia, Parlamentowi Europejskiemu i Radzie.

(107) Komisja może uznać, 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 niniejszego rozporządzenia dotyczące przekazywania z zastrzeżeniem odpowiednich zabezpieczeń, w tym wiążących reguł korporacyjnych oraz wyjątków w odniesieniu do szczególnych sytuacji. W takim przypadku należy przewidzieć konsultacje 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.

(108) W razie braku stwierdzenia odpowiedniego stopnia ochrony danych administrator lub podmiot przetwarzający powinni zastosować środki rekompensujące brak ochrony danych w państwie trzecim, zapewniając osobie, której dane dotyczą, odpowiednie zabezpieczenia. Takie odpowiednie zabezpieczenia mogą polegać na skorzystaniu z wiążących reguł korporacyjnych, standardowych klauzul ochrony danych przyjętych przez Komisję, standardowych klauzul ochrony danych przyjętych przez organ nadzorczy lub klauzul umownych dopuszczonych przez organ nadzorczy. Zabezpieczenia te powinny zapewniać, by przestrzegane były wymogi ochrony danych oraz prawa osób, których dane dotyczą, takie same jak w przypadku przetwarzania wewnątrzunijnego, w tym zapewniać dostępność egzekwowalnych praw osoby, której dane dotyczą, i skutecznych środków ochrony prawnej – w tym prawa do skutecznych administracyjnych lub sądowych środków zaskarżenia i do żądania odszkodowania – w Unii lub w państwie trzecim. Powinny one dotyczyć w szczególności przestrzegania ogólnych zasad związanych z przetwarzaniem danych osobowych oraz zasad uwzględniania ochrony danych w fazie projektowania i domyślnej ochrony danych. Również organy lub podmioty publiczne mogą przekazywać dane organom lub podmiotom publicznym w państwach trzecich lub organizacjom międzynarodowym o analogicznych obowiązkach lub funkcjach, w tym na podstawie przepisów, które powinny znaleźć się w uzgodnieniach administracyjnych, takich jak protokoły ustaleń, i które powinny przewidywać egzekwowalne i skuteczne prawa osób, których dane dotyczą. Jeżeli zabezpieczenia zawarte są w niewiążących prawnie uzgodnieniach administracyjnych, należy uzyskać zezwolenie właściwego organu nadzorczego.

(109) Możliwość korzystania przez administratora lub podmiot przetwarzający ze standardowych klauzul ochrony danych przyjętych przez Komisję lub organ nadzorczy nie powinna stanowić dla administratora lub podmiotu przetwarzającego przeszkody, by standardowe klauzule ochrony danych włączyć do szerszej umowy, takiej jak umowa między wspomnianym podmiotem przetwarzającym a innym podmiotem przetwarzającym, ani by dodać

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

inne klauzule lub dodatkowe zabezpieczenia, pod warunkiem że nie są one bezpośrednio lub pośrednio sprzeczne ze standardowymi klauzulami umownymi przyjętymi przez Komisję lub organ nadzorczy ani nie naruszają podstawowych praw lub wolności osób, których dane dotyczą. Należy zachęcać administratorów i podmioty przetwarzające, by w drodze zobowiązań umownych przewidywały dodatkowe zabezpieczenia, stanowiące uzupełnienie dla standardowych klauzul ochrony.

(110) Grupa przedsiębiorstw lub grupa przedsiębiorców prowadzących wspólną działalność gospodarczą powinna móc korzystać z zatwierdzonych wiążących reguł korporacyjnych przy międzynarodowym przekazywaniu danych z Unii do organizacji w tej samej grupie przedsiębiorstw lub w grupie przedsiębiorców prowadzących wspólną działalność gospodarczą, pod warunkiem, że w takich regułach korporacyjnych są ujęte wszystkie podstawowe zasady i egzekwowalne prawa zapewniające odpowiednie zabezpieczenia na potrzeby przekazywania danych osobowych lub na potrzeby określonych kategorii przekazań danych osobowych.

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

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

(113) Przekazanie, które można uznać za niepowtarzające się i dotyczące tylko ograniczonej liczby osób, których dane dotyczą, może być także dopuszczalne ze względu na ważne prawnie uzasadnione interesy realizowane przez administratora, o ile charakteru nadrzędnego nie mają interesy lub prawa i wolności osoby, której dane dotyczą, i administrator ocenił wszelkie okoliczności związane z przekazaniem danych. Administrator powinien zwrócić szczególną uwagę na charakter danych osobowych, cel i czas trwania proponowanej operacji przetwarzania lub proponowanych operacji przetwarzania oraz na sytuację w państwie pochodzenia, państwie trzecim i państwie ostatecznego przeznaczenia, a także powinien zapewnić odpowiednie zabezpieczenia poszanowania podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem ich danych osobowych. Takie przekazanie powinno być dopuszczalne w nielicznych przypadkach – gdy nie ma zastosowania żadna z pozostałych podstaw umożliwiających przekazanie. Gdy chodzi o cele badań naukowych lub historycznych lub cele statystyczne, należy wziąć pod uwagę uzasadnione oczekiwania społeczne co do rozwoju wiedzy. Administrator powinien informować o przekazaniu organ nadzorczy oraz osobę, której dane dotyczą.

(114) W każdym przypadku, jeżeli Komisja nie podjęła decyzji stwierdzającej odpowiedni stopień ochrony danych w państwie trzecim, administrator lub podmiot przetwarzający powinni zastosować rozwiązania, które pozwolą osobom, których dane dotyczą, dysponować – gdy przekazanie już dojdzie do skutku – egzekwowalnymi i skutecznymi prawami względem przetwarzania ich danych w Unii, tak że osoby te nadal będą mogły korzystać z podstawowych praw i zabezpieczeń.

(115) Niektóre państwa trzecie przyjmują ustawy, rozporządzenia i inne akty prawne mające bezpośrednio regulować czynności przetwarzania podejmowane przez osoby fizyczne i prawne podlegające jurysdykcji państw członkowskich. Może to obejmować wyroki sądów lub trybunałów czy decyzje organów administracyjnych państwa trzeciego nakazujące administratorowi lub podmiotowi przetwarzającemu przekazać lub ujawnić dane osobowe, które niemają za podstawę umowy międzynarodowej – na przykład umowy o wzajemnej pomocy prawnej – obowiązującej między wzywającym państwem trzecim a Unią lub państwem członkowskim. Transgraniczne stosowanie tych ustaw, rozporządzeń i innych aktów prawnych może naruszać prawo międzynarodowe i uniemożliwiać zapewnienie osobom fizycznym ochrony zapewnianej niniejszym rozporządzeniem przez Unię. Przekazywanie danych powinno być dopuszczalne wyłącznie w przypadkach, gdy spełnione są warunki przekazywania do państw trzecich ustanowione w niniejszym rozporządzeniu. Tak może być m.in. w przypadkach, gdy ujawnienie jest niezbędne ze względu na ważny interes publiczny uznany w prawie Unii lub w prawie państwa członkowskiego, któremu podlega administrator.

(116) Transgraniczne przekazywanie danych osobowych poza Unią może spowodować wzrost ryzyka, że osoby fizyczne nie będą mogły wykonywać prawa do ochrony danych osobowych, w szczególności w celu ochrony przed niezgodnym z prawem wykorzystaniem lub ujawnieniem tych informacji. Jednocześnie organy nadzorcze mogą uznać, że nie są w stanie rozpatrzyć skargi lub przeprowadzić postępowania w sprawie działalności, która ma miejsce poza granicami ich państwa. Ich starania na rzecz współpracy w kontekście transgranicznym mogą także zostać zakłócone przez niewystarczające uprawnienia prewencyjne lub zaradcze, niespójne systemy prawne oraz przeszkody praktyczne, takie jak ograniczone środki. Należy więc upowszechniać ściślejszą współpracę między organami nadzorującymi ochronę danych, by pomóc im wymieniać informacje i prowadzić postępowania z ich międzynarodowymi odpowiednikami. Aby stworzyć mechanizmy współpracy międzynarodowej, ułatwiające i przewidujące wzajemną międzynarodową pomoc w egzekwowaniu ustawodawstwa z zakresu ochrony danych osobowych, Komisja i organy nadzorcze powinny w ramach działań związanych z wykonywaniem swoich uprawnień wymieniać się informacjami i współpracować z właściwymi organami państw trzecich na zasadzie wzajemności i zgodnie z niniejszym rozporządzeniem.

(117) Zasadniczym elementem ochrony osób fizycznych w związku z przetwarzaniem danych osobowych jest utworzenie w państwach członkowskich organów nadzorczych, uprawnionych do wypełniania zadań i wykonywania uprawnień w sposób całkowicie niezależny. Aby uwzględnić swoją strukturę konstytucyjną, organizacyjną i administracyjną, państwa członkowskie powinny mieć możliwość utworzenia więcej niż jednego organu nadzorczego.

(118) Niezależność organów nadzorczych nie powinna oznaczać, że organy te nie mogą podlegać mechanizmom kontroli lub monitorowania pod kątem wydatków ani kontroli sądowej.

(119) Jeżeli państwo członkowskie utworzy kilka organów nadzorczych, powinno przewidzieć przepisy określające mechanizmy zapewniające skuteczny udział tych organów w stosowaniu mechanizmu spójności. Takie państwo członkowskie powinno w szczególności wyznaczyć organ nadzorczy, który pełnił będzie funkcję pojedynczego punktu kontaktowego do celów skutecznego udziału tych organów w stosowaniu mechanizmu, aby zapewnić sprawną i płynną współpracę z innymi organami nadzorczymi, Europejską Radą Ochrony Danych oraz Komisją.

(120) 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 krajowego lub państwowego.

(121) Ogólne warunki pełnienia funkcji członka organu nadzorczego powinny zostać określone w prawie każdego państwa członkowskiego i powinny w szczególności zapewniać, by członków tego organu powoływał przy zastosowaniu procedury zapewniającej przejrzystość parlament, rząd lub głowa 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. Organ nadzorczy powinien dysponować własnym personelem, który jest dobierany przez ten organ nadzorczy lub niezależny organ utworzony na mocy prawa państwa członkowskiego i powinien działać pod wyłącznym kierownictwem członka lub członków tego organu nadzorczego.

(122) Każdy organ nadzorczy powinien być właściwy na terytorium swojego państwa członkowskiego do wykonywania uprawnień i wypełniania zadań powierzonych mu w myśl niniejszego rozporządzenia. Powinno to dotyczyć w szczególności przetwarzania w ramach działalności jednostki organizacyjnej administratora lub podmiotu przetwarzającego na terytorium tego państwa członkowskiego, przetwarzania danych osobowych przez organy publiczne lub podmioty prywatne działające w interesie publicznym, przetwarzania mającego

wpływ na osoby, których dane dotyczą, na tym terytorium lub przetwarzania dokonywanego przez administratora lub podmiot przetwarzający niemających jednostek organizacyjnych w Unii, jeżeli zwracają się oni do osób, których dane dotyczą, mających miejsce zamieszkania na tym terytorium. Powinno to dotyczyć rozpatrywania skarg wnoszonych przez osoby, których dane dotyczą, prowadzenia postępowań w sprawie stosowania niniejszego rozporządzenia oraz uświadamiania ryzyka, zasad, zabezpieczeń i praw związanych z przetwarzaniem danych osobowych.

(123) Organy nadzorcze powinny monitorować stosowanie przepisów niniejszego rozporządzenia oraz przyczyniać się do jego spójnego stosowania w całej Unii, aby chronić osoby fizyczne w związku z przetwarzaniem ich danych osobowych oraz ułatwiać swobodny przepływ danych osobowych na rynku wewnętrznym. W tym celu organy nadzorcze powinny współpracować ze sobą oraz z Komisją bez konieczności zawierania przez państwa członkowskie umów o wzajemnej pomocy lub współpracy.

(124) Jeżeli przetwarzanie danych osobowych odbywa się w ramach działalności jednostki organizacyjnej administratora lub podmiotu przetwarzającego w Unii, a administrator lub podmiot przetwarzający posiadają jednostki organizacyjne w więcej niż jednym państwie członkowskim lub jeżeli przetwarzanie, które odbywa się w ramach działalności pojedynczej jednostki organizacyjnej administratora lub podmiotu przetwarzającego w Unii, znacznie wpływa lub może znacznie wpłynąć na osoby, których dane dotyczą, w więcej niż jednym państwie członkowskim, organem wiodącym powinien być organ nadzorczy głównej jednostki organizacyjnej administratora lub podmiotu przetwarzającego lub pojedynczej jednostki organizacyjnej administratora lub podmiotu przetwarzającego. Powinien on współpracować z innymi organami, których sprawa dotyczy, z uwagi na to, że administrator lub podmiot przetwarzający mają jednostkę organizacyjną na terytorium ich państwa członkowskiego, że odnotowuje się znaczny wpływ na osoby, których dane dotyczą, mające miejsce zamieszkania na tym terytorium lub że wniesiono do tych organów skargę. Także w przypadkach, gdy skargę wniosła osoba, której dane dotyczą, niemająca miejsca zamieszkania w tym państwie członkowskim, organ nadzorczy, do którego wniesiono skargę, powinien być uznawany za organ nadzorczy, którego sprawa dotyczy. W ramach zadania, którym jest wydawanie wytycznych co do stosowania niniejszego rozporządzenia, Europejska Rada Ochrony Danych powinna mieć możliwość wydawania wytycznych w szczególności w sprawie kryteriów, które należy uwzględnić, by stwierdzić, czy dane przetwarzanie znacznie wpływa na osoby, których dane dotyczą, w więcej niż jednym państwie członkowskim, oraz w sprawie tego, czym jest mający znaczenie dla sprawy i uzasadniony sprzeciw.

(125) Wiodący organ nadzorczy powinien być właściwy do przyjmowania wiążących decyzji co do środków wdrażających uprawnienia powierzone mu zgodnie z niniejszym rozporządzeniem. Organ nadzorczy sprawujący funkcję organu wiodącego powinien ściśle angażować w proces decyzyjny organy nadzorcze, których sprawa dotyczy, i powinien go z nimi koordynować. Jeżeli na mocy decyzji skarga osoby, której dane dotyczą, ma zostać w całości lub w części odrzucona, decyzję tę powinien przyjmować organ nadzorczy, do którego wniesiono skargę.

(126) Decyzja powinna być uzgadniana wspólnie przez wiodący organ nadzorczy i organy nadzorcze, których sprawa dotyczy, powinna być skierowana do głównej lub pojedynczej jednostki organizacyjnej administratora lub podmiotu przetwarzającego i powinna być wiążąca dla administratora i podmiotu przetwarzającego. Administrator lub podmiot przetwarzający powinien zastosować wszelkie niezbędne środki, by zapewnić zgodność z niniejszym rozporządzeniem i zastosować się do decyzji doręczonej przez wiodący organ nadzorczy głównej jednstce organizacyjnej administratora lub podmiotu przetwarzającego w odniesieniu do czynności przetwarzania w Unii.

(127) Każdy organ nadzorczy niepełniący funkcji wiodącego organu nadzorczego powinien być właściwy w sprawach lokalnych, gdy administrator lub podmiot przetwarzający posiadają jednostki organizacyjne w więcej niż jednym państwie członkowskim, ale przedmiot danego przetwarzania dotyczy wyłącznie przetwarzania prowadzonego w pojedynczym państwie członkowskim i wyłącznie osób, których dane dotyczą, w tym pojedynczym państwie członkowskim, na przykład gdy chodzi o przetwarzanie danych osobowych pracowników w szczególowym kontekście zatrudnienia w państwie członkowskim. W takim przypadku organ nadzorczy powinien niezwłocznie poinformować o sprawie wiodący organ nadzorczy. Po otrzymaniu informacji wiodący organ nadzorczy powinien postanowić, czy zajmie się daną sprawą zgodnie z przepisami niniejszego rozporządzenia dotyczącymi współpracy między wiodącym organem nadzorczym a innymi organami nadzorczymi, których sprawa dotyczy („mechanizm kompleksowej współpracy"), czy też powinien się nią zająć na szczeblu lokalnym organ nadzorczy, który o niej poinformował. Podejmując decyzję, czy zająć się sprawą, wiodący organ nadzorczy powinien uwzględnić, czy w państwie członkowskim, którego organ nadzorczy przekazał mu informacje, znajduje się jednostka organizacyjna administratora lub podmiotu przetwarzającego – aby zapewnić skuteczne wykonanie decyzji względem administratora lub podmiotu przetwarzającego. Jeżeli wiodący organ nadzorczy postanowi

zająć się daną sprawą, organ nadzorczy, który przekazał mu informacje, powinien mieć możliwość przedłożenia projektu decyzji, którą wiodący organ nadzorczy powinien w jak największym stopniu uwzględnić, przygotowując projekt swojej decyzji w ramach mechanizmu kompleksowej współpracy.

(128) Przepisy dotyczące wiodącego organu nadzorczego i mechanizmu kompleksowej współpracy nie powinny mieć zastosowania, gdy organy publiczne lub podmioty prywatne dokonują przetwarzania w interesie publicznym. W takich przypadkach jedynym organem nadzorczym właściwym do wykonywania uprawnień przyznanych zgodnie z niniejszym rozporządzeniem powinien być organ nadzorczy państwa członkowskiego, w którym organ publiczny lub podmiot prywatny posiadają jednostkę organizacyjną.

(129) Aby zapewnić spójne monitorowanie i egzekwowanie niniejszego rozporządzenia w całej Unii, organy nadzorcze powinny mieć w każdym państwie członkowskim te same zadania i faktyczne uprawnienia, w tym uprawnienia do prowadzenia postępowań wyjaśniających, naprawcze, uprawnienia do nakładania kar oraz do udzielania zezwoleń i doradcze, w szczególności w przypadku skarg osób fizycznych, i – bez uszczerbku dla uprawnień organów prokuratorskich na mocy prawa państwa członkowskiego – uprawnienia do zgłaszania naruszeń niniejszego rozporządzenia organom wymiaru sprawiedliwości oraz do udziału w postępowaniu sądowym. Wśród tych uprawnień powinno być także uprawnienie do wprowadzania czasowego lub definitywnego ograniczenia przetwarzania, w tym zakazania przetwarzania. Państwa członkowskie mogą określić także inne zadania związane z ochroną danych osobowych na mocy niniejszego rozporządzenia. Swoje uprawnienia organy nadzorcze powinny wykonywać zgodnie z odpowiednimi zabezpieczeniami proceduralnymi przewidzianymi w prawie Unii i prawie państwa członkowskiego, bezstronnie, sprawiedliwie i w rozsądnym terminie. W szczególności każdy środek powinien być odpowiedni, niezbędny i proporcjonalny, aby zapewnić przestrzeganie niniejszego rozporządzenia – z uwzględnieniem okoliczności danej sprawy, z poszanowaniem prawa do wysłuchania danej osoby przed zastosowaniem indywidualnego środka, który miałby niekorzystnie na nią wpłynąć, i bez nadmiernych kosztów i niedogodności dla danej osoby. Uprawnienia do prowadzenia postępowań wyjaśniających, jeżeli chodzi o dostęp do pomieszczeń, należy wykonywać zgodnie ze szczegółowymi wymogami przepisów państwa członkowskiego dotyczących postępowania, takimi jak wymóg uzyskania uprzedniego zezwolenia sądu. Każdy prawnie wiążący środek organu nadzorczego powinien być sporządzony na piśmie, mieć jasny i jednoznaczny charakter, wskazywać organ nadzorczy, który wydał środek, i datę wydania środka, nosić podpis szefa lub członka organu nadzorczego przez niego upoważnionego, podawać powody zastosowania środka oraz informować o prawie do skutecznego środka ochrony prawnej. Nie powinno to wykluczać dodatkowych wymogów na mocy przepisów państwa członkowskiego dotyczących postępowania. Wydanie prawnie wiążącej decyzji oznacza, że może ona być przedmiotem kontroli sądowej w państwie członkowskim organu nadzorczego, który ją wydał.

(130) Jeżeli organ nadzorczy, do którego wniesiono skargę, nie jest wiodącym organem nadzorczym, wiodący organ nadzorczy powinien ściśle współpracować z organem nadzorczym, do którego wniesiono skargę, zgodnie z przepisami o współpracy i spójności ustanowionymi w niniejszym rozporządzeniu. W takim przypadku wiodący organ nadzorczy powinien, w przypadkach gdy stosuje środki mające wywołać skutki prawne, w tym nakłada administracyjne kary pieniężne, w jak największym stopniu brać pod uwagę opinię organu nadzorczego, do którego wniesiono skargę, ten zaś powinien pozostać właściwy do przeprowadzenia postępowania wyjaśniającego na terytorium własnego państwa członkowskiego będąc w kontakcie z wiodącym organem nadzorczym.

(131) Jeżeli funkcję wiodącego organu nadzorczego wobec czynności przetwarzania prowadzonych przez administratora lub podmiot przetwarzający powinien pełnić inny organ nadzorczy, ale konkretny przedmiot skargi lub ewentualnego naruszenia dotyczy wyłącznie czynności przetwarzania prowadzonych przez administratora lub podmiot przetwarzający w państwie członkowskim, w którym wniesiono skargę lub wykryto ewentualne naruszenie, a sprawa nie wpływa znacznie lub najprawdopodobniej nie wpłynie znacznie na osoby, których dane dotyczą, w innych państwach członkowskich, wtedy organ nadzorczy, do którego wniesiono skargę lub który wykrył lub w inny sposób dowiedział się o sytuacjach mogących skutkować ewentualnymi naruszeniami niniejszego rozporządzenia, powinien dążyć do polubownego rozwiązania z administratorem, a jeżeli okaże się ono niemożliwe, skorzystać z pełni przysługujących mu uprawnień. Powinno to dotyczyć także: konkretnego przetwarzania, które odbywa się na terytorium państwa członkowskiego organu nadzorczego lub odnosi się do osób, których dane dotyczą, na terytorium tego państwa członkowskiego; przetwarzania, które odbywa się w ramach oferowania towarów lub usług konkretnie osobom, których dane dotyczą, na terytorium państwa członkowskiego organu nadzorczego; lub przetwarzania wymagającego oceny z uwagi na stosowne obowiązki prawne wynikające z prawa państwa członkowskiego.

(132) Na uświadamiające działania organów nadzorczych skierowane do opinii publicznej powinny się składać m.in. konkretne środki adresowane do administratorów i podmiotów przetwarzających, w tym do mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw, a także do osób fizycznych, w szczególności w ramach edukacji.

(133) Organy nadzorcze powinny się wzajemnie wspierać w wykonywaniu swoich zadań oraz świadczyć sobie wzajemną pomoc, by zapewnić spójne stosowanie i egzekwowanie niniejszego rozporządzenia na rynku wewnętrznym. Organ nadzorczy, który występuje z wnioskiem o wzajemną pomoc, może przyjąć środek tymczasowy, jeżeli nie uzyska odpowiedzi w terminie miesiąca od otrzymania wniosku o udzielenie wzajemnej pomocy przez wezwany organ nadzorczy.

(134) Każdy organ nadzorczy powinien w stosownych przypadkach uczestniczyć we wspólnych operacjach organów nadzorczych. Wezwany organ nadzorczy powinien mieć obowiązek udzielenia odpowiedzi w określonym terminie.

(135) Aby zapewnić spójne stosowanie niniejszego rozporządzenia w całej Unii, należy ustanowić mechanizm spójności na potrzeby współpracy między organami nadzorczymi. Mechanizm ten powinien mieć zastosowanie w szczególności w przypadkach, gdy organ nadzorczy zamierza przyjąć środek mający wywoływać skutki prawne w odniesieniu do operacji przetwarzania, które znacznie wpływają na istotną liczbę osób, których dane dotyczą, w kilku państwach członkowskich. Powinien mieć zastosowanie także w przypadkach, gdy organ nadzorczy, którego sprawa dotyczy, lub Komisja zwracają się z wnioskiem o rozwiązanie danej kwestii w ramach mechanizmu spójności. Mechanizm ten powinien pozostawać bez uszczerbku dla środków, które Komisja może zastosować w ramach wykonywania uprawnień przysługujących jej na mocy traktatów.

(136) W ramach stosowania mechanizmu spójności Europejska Rada Ochrony Danych powinna w określonym terminie wydawać opinie, jeżeli tak postanowią większością głosów jej członkowie lub jeżeli zwróci się do niej z takim wnioskiem organ nadzorczy, którego sprawa dotyczy, lub Komisja. Europejska Rada Ochrony Danych powinna być także umocowana do przyjmowania prawnie wiążących decyzji w razie sporów między organami nadzorczymi. W tym celu powinna wydawać, zasadniczo większością dwóch trzecich głosów swoich członków, prawnie wiążące decyzje w jasno określonych przypadkach, gdy wśród organów nadzorczych panują sprzeczne opinie – w szczególności w ramach mechanizmu współpracy między wiodącym organem nadzorczym a organami nadzorczymi, których sprawa dotyczy – co do meritum sprawy, w szczególności tego, czy doszło do naruszenia niniejszego rozporządzenia.

(137) Może wystąpić pilna potrzeba podjęcia działań w celu ochrony praw i wolności osób, których dane dotyczą, w szczególności gdy istnieje ryzyko, że wyegzekwowanie prawa przysługującego osobie, której dane dotyczą, może być znacznie utrudnione. Organ nadzorczy powinien w związku z tym mieć możliwość przyjmowania na swoim terytorium należycie uzasadnionych środków tymczasowych o określonym okresie obowiązywania, który nie powinien przekraczać trzech miesięcy.

(138) Jeżeli zastosowanie takiego mechanizmu jest obowiązkowe, to od jego zastosowania powinna zależeć zgodność z prawem środka, którym organ nadzorczy chce wywołać skutki prawne. W innych przypadkach o znaczeniu transgranicznym należy stosować mechanizm współpracy między wiodącym organem nadzorczym a organami nadzorczymi, których sprawa dotyczy, oraz można świadczyć wzajemną pomoc i prowadzić wspólne operacje między organami nadzorczymi, których sprawa dotyczy, na zasadzie dwustronnej lub wielostronnej bez uruchamiania mechanizmu spójności.

(139) Aby wspierać spójne stosowanie niniejszego rozporządzenia, należy utworzyć – jako niezależny organ Unii – Europejską Radę Ochrony Danych. Rada ta, by móc realizować swoje cele, powinna mieć osobowość prawną. Europejską Radę Ochrony Danych powinien reprezentować jej przewodniczący. Powinna ona zastąpić Grupę Roboczą ds. Ochrony Osób Fizycznych w zakresie Przetwarzania Danych Osobowych, powołaną na mocy dyrektywy 95/46/WE. W jej skład powinni wchodzić szefowie organów nadzorczych wszystkich państw członkowskich oraz Europejski Inspektor Ochrony Danych lub ich przedstawiciele. Komisja powinna uczestniczyć bez prawa głosu w działaniach Europejskiej Rady Ochrony Danych, a Europejski Inspektor Ochrony Danych – bez prawa głosu w niektórych sprawach. Europejska Rada Ochrony Danych powinna przyczyniać się do spójnego stosowania niniejszego rozporządzenia w całej Unii, m.in. poprzez doradzanie Komisji – w szczególności w sprawie stopnia ochrony w państwach trzecich lub organizacjach międzynarodowych – i propagowanie współpracy organów nadzorczych w całej Unii. Wypełniając swoje zadania, Europejska Rada Ochrony Danych powinna działać w sposób niezależny.

(140) Europejską Radę Ochrony Danych powinien wspierać sekretariat, zapewniany przez Europejskiego Inspektora Ochrony Danych. Personel Europejskiego Inspektora Ochrony Danych wykonujący zadania, które niniejsze rozporządzenie powierza Europejskiej Radzie Ochrony Danych, powinien wykonywać swoje zadania wyłącznie pod kierunkiem przewodniczącego Europejskiej Rady Ochrony Danych i jemu podlegać.

(141) Każda osoba, której dane dotyczą, powinna mieć prawo wniesienia skargi do jednego organu nadzorczego oraz prawo do skutecznego środka ochrony prawnej przed sądem, zgodnie z art. 47 Karty praw podstawowych, w szczególności w państwie członkowskim, w którym ma miejsce zwykłego pobytu, a jeżeli uzna, że jej prawa wynikające z niniejszego rozporządzenia są naruszane, lub jeżeli organ nadzorczy nie reaguje na skargę,

częściowo lub w całości ją odrzuca lub oddala, lub nie podejmuje działania, choć jest to niezbędne do ochrony praw tej osoby. Postępowanie wyjaśniające na podstawie skargi powinno być prowadzone – z zastrzeżeniem kontroli sądowej – w zakresie odpowiadającym konkretnej sprawie. Organ nadzorczy powinien w rozsądnym terminie poinformować osobę, której dane dotyczą, o postępach i wynikach rozpatrywania skargi. Jeżeli dana sprawa wymaga 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 zastosować takie środki jak udostępnienie formularza skargi, który można wypełnić także elektronicznie, przy czym nie należy wykluczać innych sposobów komunikacji.

(142) Jeżeli osoba, której dane dotyczą, uzna, że naruszane są jej prawa wynikające z niniejszego rozporządzenia, powinna mieć ona prawo zlecić podmiotowi, organizacji lub zrzeszeniu – które nie mają charakteru zarobkowego, zostały ustanowione zgodnie z prawem państwa członkowskiego, mają statutowo na celu interes publiczny i działają w dziedzinie ochrony danych osobowych – wniesienie skargi w swoim imieniu do organu nadzorczego, wykonanie prawa do środka ochrony prawnej przed sądem w imieniu osób, których dane dotyczą lub – o ile taką możliwość przewiduje prawo państwa członkowskiego – żądanie odszkodowania w imieniu osób, których dane dotyczą. Państwo członkowskie może wymagać, by taki podmiot, taka organizacja lub takie zrzeszenie niezależnie od zlecenia otrzymanego od osoby, której dane dotyczą, miały prawo wniesienia w tym państwie członkowskim skargi oraz miały prawo do skutecznego środka ochrony prawnej przed sądem, jeżeli mają powody, by uznać, że w wyniku przetwarzania danych osobowych w sposób naruszający niniejsze rozporządzenie naruszone zostały prawa osoby, której dane dotyczą. Takiemu podmiotowi, takiej organizacji lub takiemu zrzeszeniu nie może przysługiwać prawo do występowania o odszkodowanie w imieniu osoby, której dane dotyczą, jeżeli nie zostały do tego umocowane przez tę osobę.

(143) Każda osoba fizyczna lub prawna ma prawo wnieść do Trybunału Sprawiedliwości skargę o unieważnienie decyzji Europejskiej Rady Ochrony Danych na warunkach przewidzianych w art. 263 TFUE. Organy nadzorcze, których sprawa dotyczy, chcące takie decyzje zaskarżyć – jako adresaci takich decyzji – muszą wnieść skargę w terminie dwóch miesięcy od notyfikowania im tych decyzji, zgodnie art. 263 TFUE. Jeżeli decyzje Europejskiej Rady Ochrony Danych bezpośrednio i indywidualnie dotyczą administratora, podmiotu przetwarzającego lub skarżącego, ten ostatni może wnieść skargę o unieważnienie tych decyzji w terminie dwóch miesięcy od ich publikacji na stronie internetowej Europejskiej Rady Ochrony Danych, zgodnie z art. 263 TFUE. Z zastrzeżeniem prawa wynikającego z art. 263 TFUE, każda osoba fizyczna lub prawna powinna mieć prawo do skutecznego środka ochrony prawnej przed właściwym sądem krajowym wobec decyzji organu nadzorczego wywołującej skutki prawne wobec tej osoby. Taka decyzja może dotyczyć w szczególności wykonywania przez organ nadzorczy uprawnień do prowadzenia postępowań wyjaśniających, uprawnień naprawczych i do wydawania zezwoleń lub oddalania lub odrzucania skarg. Prawo do skutecznego środka ochrony prawnej przed sądem nie dotyczy jednak niewiążących prawnie środków przyjętych przez organy nadzorcze, takich jak wydawane przez nie opinie czy zalecenia. Skarga przeciwko organowi nadzorczemu powinna być wnoszona do sądu 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 mających znaczenie dla rozstrzygnięcia sprawy.

Jeżeli organ nadzorczy odrzuci lub oddali skargę, skarżący może wnieść odwołanie do sądu tego samego państwa członkowskiego. W kontekście środków ochrony prawnej przed sądem dotyczących stosowania niniejszego rozporządzenia sądy krajowe uznające, że decyzja w tej kwestii jest niezbędna do wydania wyroku, mogą, a w przypadku przewidzianym w art. 267 TFUE – muszą, zwrócić się do Trybunału Sprawiedliwości o orzeczenie w trybie prejudycjalnym w sprawie wykładni prawa Unii, w tym niniejszego rozporządzenia. Ponadto jeżeli decyzja organu nadzorczego wdrażająca decyzję Europejskiej Rady Ochrony Danych zostanie zaskarżona przed sądem krajowym, a przedmiotem będzie ważność decyzji Europejskiej Rady Ochrony Danych, sąd krajowy nie jest uprawniony do stwierdzenia nieważności decyzji Europejskiej Rady Ochrony Danych, ale jeżeli uważa tę decyzję za nieważną, musi przekazać sprawę jej ważności Trybunałowi Sprawiedliwości zgodnie z art. 267 TFUE i jego wykładnią dokonaną przez Trybunał Sprawiedliwości. Sąd krajowy nie może jednak przekazać Trybunałowi Sprawiedliwości sprawy ważności decyzji Europejskiej Rady Ochrony Danych na wniosek osoby fizycznej lub prawnej, która miała możliwość wnieść skargę o unieważnienie tej decyzji, w szczególności gdy decyzja ta bezpośrednio i indywidualnie jej dotyczyła, ale nie zrobiła tego w terminie przewidzianym w art. 263 TFUE.

(144) Jeżeli sąd, przed którym toczy się postępowanie przeciwko decyzji organu nadzorczego, ma powody przypuszczać, że przed sądem właściwym innego państwa członkowskiego wszczęto postępowanie w sprawie tego samego przetwarzania – na przykład w tym samym przedmiocie w związku z przetwarzaniem prowadzonym przez tego samego administratora lub przez ten sam podmiot przetwarzający lub odnośnie do tej samej przyczyny – powinien skontaktować się z tym sądem, aby potwierdzić, czy takie powiązane postępowanie się odbywa. Jeżeli przed sądem w innym państwie członkowskim toczy się powiązane postępowanie, każdy sąd inny niż sąd, przed którym jako pierwszym wszczęto postępowanie, może zawiesić postępowanie lub może – na

wniosek jednej ze stron – stwierdzić brak swojej jurysdykcji na rzecz sądu, przed którym jako pierwszym wszczęto postępowanie, jeżeli sąd ten ma jurysdykcję w danej sprawie, a jego prawo zezwala na połączenie takich powiązanych postępowań. Postępowania uznaje się za powiązane, jeżeli związek między nimi jest tak ścisły, że celowe jest ich łączne rozpatrzenie i rozstrzygnięcie, tak by uniknąć ryzyka zapadnięcia sprzecznych orzeczeń w odrębnych postępowaniach.

(145) W przypadku postępowania przeciwko administratorowi lub podmiotowi przetwarzającemu skarżący powinien mieć możliwość wybrania, do którego sądu chce wnieść skargę: do sądu w państwie członkowskim, w którym administrator lub podmiot przetwarzający posiadają jednostkę organizacyjną, czy do sądu w państwie członkowskim, w którym osoba, której dane dotyczą, ma miejsce zamieszkania, o ile administrator nie jest organem publicznym państwa członkowskiego działającym w ramach wykonywania swoich uprawnień publicznych.

(146) Za szkodę, którą dana osoba poniosła wskutek przetwarzania w sposób naruszający niniejsze rozporządzenie, powinno przysługiwać odszkodowanie od administratora lub podmiotu przetwarzającego. Administrator lub podmiot przetwarzający powinni jednak zostać zwolnieni z odpowiedzialności prawnej, jeżeli udowodnią, że szkoda w żadnym razie nie powstała z ich winy. Pojęcie szkody należy interpretować szeroko, w świetle orzecznictwa Trybunału Sprawiedliwości, w sposób w pełni odzwierciedlający cele niniejszego rozporządzenia. Nie ma to wpływu na roszczenia z tytułu szkód wynikających z naruszenia innych przepisów prawa Unii lub prawa państwa członkowskiego. Przetwarzanie dokonywane w sposób naruszający niniejsze rozporządzenie obejmuje także przetwarzanie, które narusza akty delegowane i wykonawcze przyjęte na mocy niniejszego rozporządzenia oraz prawo państwa członkowskiego doprecyzowujące niniejsze rozporządzenie. Osoby, których dane dotyczą, powinny uzyskać pełne i skuteczne odszkodowanie za poniesione szkody. Jeżeli administratorzy lub podmioty przetwarzające uczestniczą w tym samym przetwarzaniu, każdy administrator lub podmiot przetwarzający powinien odpowiadać prawnie za całość szkody. Jeżeli jednak zostaną włączeni do jednego postępowania sądowego zgodnie z prawem państwa członkowskiego, odszkodowaniem można obarczyć każdego z administratorów i każdy z podmiotów przetwarzających stosownie do ich winy za szkodę wynikłą z przetwarzania, o ile osobie, której dane dotyczą, zapewnione zostanie pełne i skuteczne odszkodowanie za poniesioną szkodę. Każdy administrator lub podmiot przetwarzający, który wypłacił pełne odszkodowanie, może następnie dochodzić roszczeń regresowych wobec innych administratorów lub podmiotów przetwarzających uczestniczących w tym samym przetwarzaniu.

(147) Jeżeli niniejsze rozporządzenie przewiduje szczegółowe przepisy o jurysdykcji – w szczególności odnośnie do postępowań w zakresie środków ochrony prawnej przed sądem, w tym odszkodowania, przeciwko administratorowi lub podmiotowi przetwarzającemu –ogólne przepisy o jurysdykcji, takie jak rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1215/2012 ([1]), nie powinny naruszać stosowania takich szczegółowych przepisów.

(148) Aby egzekwowanie przepisów niniejszego rozporządzenia było skuteczniejsze, należy za jego naruszenie nakładać sankcje, w tym administracyjne kary pieniężne – oprócz lub zamiast odpowiednich środków nakładanych na mocy niniejszego rozporządzenia przez organ nadzorczy. Jeżeli naruszenie jest niewielkie lub jeżeli grożąca kara pieniężna stanowiłaby dla osoby fizycznej nieproporcjonalne obciążenie, można zamiast tego udzielić upomnienia. Powinno się jednak zwrócić należytą uwagę na charakter, wagę oraz czas trwania naruszenia, na to, czy naruszenie nie było umyślne, na działania podjęte dla zminimalizowania szkody, na stopień odpowiedzialności lub wszelkie mające znaczenie wcześniejsze naruszenia, na sposób, w jaki organ nadzorczy dowiedział się o naruszeniu, na przestrzeganie środków nałożonych na administratora lub podmiot przetwarzający, na stosowanie kodeksów postępowania oraz wszelkie inne czynniki obciążające lub łagodzące. Nakładanie sankcji, w tym administracyjnych kar pieniężnych, powinno podlegać odpowiednim zabezpieczeniom proceduralnym zgodnym z ogólnymi zasadami prawa Unii i z Kartą praw podstawowych, w tym skutecznej ochronie prawnej i prawu do rzetelnego procesu.

(149) Państwa członkowskie powinny mieć możliwość ustanawiania przepisów przewidujących sankcje karne za naruszenie niniejszego rozporządzenia, w tym za naruszenie krajowych przepisów przyjętych na jego mocy i w jego granicach. Sankcje karne mogą również obejmować pozbawienie zysków wynikających z naruszenia niniejszego rozporządzenia. Jednak nałożenie sankcji karnych za naruszenie takich krajowych przepisów oraz nałożenie sankcji administracyjnych nie powinno prowadzić do naruszenia zasady *ne bis in idem*, zgodnie z wykładnią Trybunału Sprawiedliwości.

(150) W celu wzmocnienia i zharmonizowania sankcji administracyjnych za naruszenie niniejszego rozporządzenia każdy organ nadzorczy powinien być uprawniony do nakładania administracyjnych kar pieniężnych. W niniejszym rozporządzeniu należy wymienić rodzaje naruszeń oraz wskazać górną granicę i kryteria ustalania związanych z nimi administracyjnych kar pieniężnych, które właściwy organ nadzorczy powinien określać

([1]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1215/2012 z dnia 12 grudnia 2012 r. w sprawie jurysdykcji i uznawania orzeczeń sądowych oraz ich wykonywania w sprawach cywilnych i handlowych (Dz.U. L 351 z 20.12.2012, s. 1).

indywidualnie dla każdego przypadku z uwzględnieniem wszystkich stosownych okoliczności danej sytuacji, z należytym uwzględnieniem w szczególności charakteru, wagi, czasu trwania naruszenia i jego konsekwencji, a także środków podjętych w celu zastosowania się do obowiązków wynikających z niniejszego rozporządzenia oraz w celu zapobieżenia konsekwencjom naruszenia lub w celu zminimalizowania tych konsekwencji. Jeżeli administracyjna kara pieniężna jest nakładana na przedsiębiorstwo, to „przedsiębiorstwo" należy do tych celów rozumieć zgodnie z art. 101 i 102 TFUE. Jeżeli administracyjna kara pieniężna jest nakładana na osobę niebędącą przedsiębiorstwem, organ nadzorczy, ustalając właściwą wysokość kary pieniężnej, powinien wziąć pod uwagę ogólny poziom dochodów w danym państwie członkowskim oraz sytuację ekonomiczną tej osoby. Aby wspierać spójne stosowanie administracyjnych kar pieniężnych, można także użyć mechanizmu spójności. Państwa członkowskie powinny określić, czy i w jakim zakresie administracyjnym karom pieniężnym powinny podlegać organy publiczne. Nałożenie administracyjnej kary pieniężnej lub wydanie ostrzeżenia nie wpływa na stosowanie innych uprawnień organów nadzorczych ani innych sankcji na mocy niniejszego rozporządzenia.

(151) Systemy prawne Danii i Estonii nie przewidują administracyjnych kar pieniężnych określonych w niniejszym rozporządzeniu. Przepisy o administracyjnych karach pieniężnych można stosować tak, że w Danii właściwy sąd krajowy będzie nakładać grzywnę jako sankcję karną, a w Estonii organ nadzorczy będzie nakładać grzywnę w ramach postępowania o wykroczenie, pod warunkiem że takie stosowanie przepisów w tych państwach członkowskich będzie mieć skutek równoważny administracyjnej karze pieniężnej nakładanej przez organ nadzorczy. Dlatego właściwy sąd krajowy powinien brać pod uwagę zalecenie organu nadzorczego, który postuluje nałożenie grzywny. Nakładane grzywny muszą być w każdym przypadku skuteczne, proporcjonalne i odstraszające.

(152) W sytuacjach, w których niniejsze rozporządzenie nie harmonizuje sankcji administracyjnych, lub w razie potrzeby w innych przypadkach, na przykład w razie poważnego naruszenia niniejszego rozporządzenia, państwa członkowskie powinny wdrożyć system przewidujący skuteczne, proporcjonalne i odstraszające sankcje. Charakter takich sankcji (karny lub administracyjny) powinno określać prawo państwa członkowskiego.

(153) Prawo państw członkowskich powinno godzić przepisy regulujące wolność wypowiedzi i informacji, w tym wypowiedzi dziennikarskiej, akademickiej, artystycznej lub literackiej, z prawem do ochrony danych osobowych na mocy niniejszego rozporządzenia. Przetwarzanie danych osobowych jedynie do celów dziennikarskich lub do celów wypowiedzi akademickiej, artystycznej lub literackiej powinno podlegać wyjątkom lub odstępstwom od niektórych przepisów niniejszego rozporządzenia, jeżeli jest to niezbędne, by pogodzić prawo do ochrony danych osobowych z prawem do wolności wypowiedzi i informacji, przewidzianymi w art. 11 Karty praw podstawowych. Powinno mieć to zastosowanie w szczególności do przetwarzania danych osobowych w dziedzinie audiowizualnej oraz w archiwach i bibliotekach prasowych. Państwa członkowskie powinny więc przyjąć akty prawne określające odstępstwa i wyjątki niezbędne do zapewnienia równowagi między tymi prawami podstawowymi. Państwa członkowskie powinny przyjąć takie odstępstwa i wyjątki w odniesieniu do zasad ogólnych, praw przysługujących osobie, której dane dotyczą, administratora i podmiotu przetwarzającego, przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych, niezależnych organów nadzorczych, współpracy i spójności oraz szczególnych sytuacji przetwarzania danych. Jeżeli odstępstwa i wyjątki różnią się zależnie od państwa członkowskiego, zastosowanie powinno mieć prawo państwa członkowskiego, któremu podlega administrator. Aby uwzględnić, jak ważna dla każdego demokratycznego społeczeństwa jest wolność wypowiedzi, pojęcia dotyczące tej wolności, takie jak dziennikarstwo, należy interpretować szeroko.

(154) Niniejsze rozporządzenie pozwala uwzględnić przy stosowaniu jego przepisów zasadę publicznego dostępu do dokumentów urzędowych. Publiczny dostęp do dokumentów urzędowych można uznać za interes publiczny. Organ publiczny lub podmiot publiczny powinny móc publicznie ujawniać dane osobowe z dokumentów przez siebie przechowywanych, jeżeli takie ujawnienie jest przewidziane przepisami prawa Unii lub prawa państwa członkowskiego, któremu organ ten lub podmiot podlegają. Przepisy takie powinny godzić publiczny dostęp do dokumentów urzędowych i ponowne wykorzystywanie informacji sektora publicznego z prawem do ochrony danych osobowych, i dlatego mogą przewidywać niezbędne uwzględnienie prawa do ochrony danych osobowych na podstawie niniejszego rozporządzenia. Wzmianka o organach i podmiotach publicznych powinna w tym kontekście dotyczyć wszystkich organów lub innych podmiotów objętych prawem państwa członkowskiego dotyczącym publicznego dostępu do dokumentów. Dyrektywa Parlamentu Europejskiego i Rady 2003/98/WE ([1]) nie narusza ani w żaden sposób nie wpływa na stopień ochrony osób fizycznych w związku z przetwarzaniem

([1]) Dyrektywa 2003/98/WE Parlamentu Europejskiego i Rady z dnia 17 listopada 2003 r. w sprawie ponownego wykorzystywania informacji sektora publicznego (Dz.U. L 345 z 31.12.2003, s. 90).

danych osobowych wynikający z przepisów prawa Unii i prawa państwa członkowskiego, a w szczególności nie zmienia obowiązków i praw przewidzianych w niniejszym rozporządzeniu. Dyrektywa ta nie powinna mieć zastosowania w szczególności do dokumentów, do których – w ramach systemów dostępu – dostęp jest wykluczony lub ograniczony z powodu ochrony danych osobowych, ani do fragmentów dokumentów dostępnych w ramach tych systemów, ale zawierających dane osobowe, których ponowne wykorzystanie zostało określone w prawie jako niezgodne z prawem o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych.

(155) W prawie państwa członkowskiego lub w porozumieniach zbiorowych, w tym zakładowych porozumieniach z przedstawicielami pracowników, mogą być przewidziane przepisy szczegółowe o przetwarzaniu danych osobowych pracowników w związku z zatrudnieniem, w szczególności warunki, na których dane osobowe w związku z zatrudnieniem można przetwarzać za zgodą pracownika do celów procedury rekrutacyjnej, wykonywania umowy o pracę, w tym wykonywania obowiązków określonych w przepisach lub w porozumieniach zbiorowych, zarządzania, planowania i organizacji pracy, równości i różnorodności w miejscu pracy, bezpieczeństwa i higieny pracy oraz do celów indywidualnego lub zbiorowego wykonywania praw i korzystania ze świadczeń związanych z zatrudnieniem, a także do celów zakończenia stosunku pracy.

(156) Przetwarzanie danych osobowych do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych powinno podlegać odpowiednim zabezpieczeniom praw i wolności osoby, której dane dotyczą, zgodnie z niniejszym rozporządzeniem. Zabezpieczenia te powinny polegać na wdrożeniu środków technicznych i organizacyjnych zapewniających w szczególności poszanowanie zasady minimalizacji danych. Dalsze przetwarzanie danych osobowych do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych można prowadzić, jeżeli administrator ocenił, czy celów tych nie można osiągnąć przetwarzaniem danych osobowych, które albo od początku albo już dłużej nie pozwalają identyfikować osób, których dane dotyczą, pod warunkiem że istnieją odpowiednie zabezpieczenia (takie jak pseudonimizacja danych osobowych). Państwa członkowskie powinny ustanowić odpowiednie zabezpieczenia w odniesieniu do przetwarzania danych osobowych do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych. Państwa członkowskie powinny mieć możliwość ustanowienia– na określonych warunkach i z zastrzeżeniem odpowiednich zabezpieczeń dla osób, których dane dotyczą – szczegółowych uregulowań i wyjątków od wymogu udzielenia informacji oraz prawa do sprostowania lub usuwania danych osobowych, do „bycia zapomnianym", do ograniczenia przetwarzania i do przenoszenia danych oraz do sprzeciwu, gdy dane osobowe są przetwarzane do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych. Takie warunki i zabezpieczenia mogą skutkować szczegółowymi procedurami wykonywania tych praw przez osoby, których dane dotyczą – jeżeli jest to właściwe w świetle celów, którym służy konkretne przetwarzanie – oraz środkami technicznymi i organizacyjnymi mającymi ograniczyć przetwarzanie danych osobowych w myśl zasad proporcjonalności i konieczności. Przetwarzanie danych osobowych do celów naukowych powinno też być zgodne z innymi odpowiednimi przepisami, takimi jak przepisy o próbach klinicznych.

(157) Łącząc ze sobą informacje z rejestrów, naukowcy mogą uzyskać nową, wartościową wiedzę na przykład o częstych chorobach, takich jak choroba układu krążenia, rak czy depresja. Korzystając z rejestrów, można uściślić wyniki badań naukowych, gdyż będą się one opierać na większej próbie. W naukach społecznych badania oparte na rejestrach pozwalają naukowcom uzyskać kluczową wiedzę o długoterminowych współzależnościach wielu czynników społecznych, na przykład bezrobocia czy edukacji z innymi czynnikami bytowymi. Wyniki badań uzyskane z rejestrów dostarczają solidnej, dobrej jakościowo wiedzy, która może posłużyć do opracowywania i realizowania polityki opartej na wiedzy, podnieść jakość życia wielu osób, a także zwiększyć skuteczność usług społecznych itp. Dla ułatwienia badań naukowych dopuszcza się przetwarzanie danych osobowych do celów badań naukowych z zastrzeżeniem odpowiednich warunków i zabezpieczeń przewidzianych w prawie Unii lub w prawie państwa członkowskiego.

(158) Jeżeli dane osobowe są przetwarzane do celów archiwalnych, niniejsze rozporządzenie powinno mieć zastosowanie także do takiego przetwarzania; należy jednak pamiętać, że niniejsze rozporządzenie nie powinno mieć zastosowania do danych osobowych osób zmarłych. Organy lub podmioty publiczne lub podmioty prywatne posiadające wpisy będące przedmiotem interesu publicznego powinny zgodnie z prawem Unii lub prawem państwa członkowskiego mieć prawny obowiązek nabywania, ochrony, oszacowywania, systematyzowania, opisywania, przekazywania, promowania, rozpowszechniania i udostępniania wpisów o trwałej wartości dla ogólnego interesu publicznego. Państwa członkowskie powinny także mieć możliwość zezwolenia na dalsze przetwarzanie danych osobowych do celów archiwalnych, na przykład z myślą o dostarczeniu konkretnych informacji o postawie politycznej w dawnych systemach państw totalitarnych, o przypadkach ludobójstwa, zbrodniach przeciwko ludzkości (zwłaszcza holokauście) czy zbrodniach wojennych.

(159) Jeżeli dane osobowe są przetwarzane do celów badań naukowych, niniejsze rozporządzenie powinno mieć zastosowanie także do takiego przetwarzania. W niniejszym rozporządzeniu przetwarzanie danych osobowych do celów badań naukowych należy interpretować szeroko, obejmując tym pojęciem na przykład rozwój technologiczny i demonstrację, badania podstawowe, badania stosowane oraz badania finansowane ze środków prywatnych. Ponadto należy uwzględnić cel Unii określony w art. 179 ust. 1 TFUE, którym jest utworzenie europejskiej przestrzeni badawczej. Wyrażenie „do celów badań naukowych" powinno obejmować także badania prowadzone w interesie publicznym w dziedzinie zdrowia publicznego. Z uwagi na specyfikę przetwarzania danych osobowych do celów badań naukowych zastosowanie powinny mieć specjalne warunki, w szczególności w odniesieniu do publikacji lub innego ujawniania danych osobowych w kontekście celów badań naukowych. Jeżeli wynik badań naukowych, w szczególności w kontekście zdrowotnym, uzasadnia dalsze środki w interesie osoby, której dane dotyczą, do środków tych powinny mieć zastosowanie przepisy ogólne niniejszego rozporządzenia.

(160) Jeżeli dane osobowe są przetwarzane w celu badań historycznych, niniejsze rozporządzenie powinno mieć zastosowanie także do takiego przetwarzania. Powinno to dotyczyć m.in. badań historycznych i badań do celów genealogicznych; należy jednak pamiętać, że niniejsze rozporządzenie nie powinno mieć zastosowania do osób zmarłych.

(161) Do celów wyrażenia zgody na udział w badaniach naukowych podczas prób klinicznych zastosowanie powinny mieć stosowne przepisy rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 536/2014 ([1]).

(162) Jeżeli dane osobowe są przetwarzane do celów statystycznych, niniejsze rozporządzenie powinno mieć zastosowanie do takiego przetwarzania. Prawo Unii lub prawo państwa członkowskiego powinny – w granicach niniejszego rozporządzenia – określać treść statystyczną, kontrolę dostępu, warunki przetwarzania danych osobowych do celów statystycznych oraz odpowiednie środki mające chronić prawa i wolności osoby, której dane dotyczą, oraz gwarantować poufność statystyczną. Wyrażenie „cele statystyczne" oznacza każdą operację zbierania i przetwarzania danych osobowych niezbędnych do badań statystycznych lub do opracowywania wyników statystycznych. Z kolei wyniki statystyczne mogą następnie służyć do dalszych celów, m.in. do celów badań naukowych. Wyrażenie „cel statystyczny" sugeruje, że wynikiem przetwarzania do celów statystycznych nie są dane osobowe, lecz dane zbiorcze, i że wynik ten lub te dane osobowe nie służą za podstawę środków czy decyzji dotyczących konkretnych osób fizycznych.

(163) Należy chronić informacje poufne, które organy statystyczne Unii i państw członkowskich gromadzą do celów opracowywania oficjalnych statystyk europejskich i krajowych. Statystyki europejskie należy projektować, tworzyć i rozpowszechniać zgodnie z zasadami statystycznymi przewidzianymi w art. 338 ust. 2 TFUE, przy czym statystyki krajowe powinny być także zgodne z prawem państwa członkowskiego. Dalsze szczegółowe informacje o statystycznej poufności statystyki europejskiej zawiera rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 223/2009 ([2]).

(164) W odniesieniu do uprawnień organów nadzorczych do uzyskania od administratora lub podmiotu przetwarzającego dostępu do danych osobowych oraz do pomieszczeń, państwa członkowskie mogą – w granicach niniejszego rozporządzenia – przyjąć przepisy szczegółowe mające chronić obowiązek zachowania tajemnicy zawodowej lub innej równoważnej tajemnicy, o ile jest to niezbędne, by pogodzić prawo do ochrony danych osobowych z obowiązkiem zachowania tajemnicy zawodowej. Pozostaje to bez uszczerbku dla istniejących obowiązków państw członkowskich, by tam, gdzie tego wymaga prawo Unii, przyjąć przepisy o tajemnicy zawodowej.

(165) Niniejsze rozporządzenie nie narusza statusu przyznanego kościołom oraz związkom lub wspólnotom wyznaniowym na mocy prawa konstytucyjnego obowiązującego w państwach członkowskich i nie narusza tego statusu – jak uznano w art. 17 TFUE.

(166) Aby spełnić cele niniejszego rozporządzenia, mianowicie chronić podstawowe prawa i wolności osób fizycznych, w szczególności prawo do ochrony danych osobowych, oraz zagwarantować swobodny przepływ danych osobowych w Unii, należy przekazać Komisji uprawnienia do przyjmowania aktów zgodnie z art. 290 TFUE.

([1]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 536/2014 z dnia 16 kwietnia 2014 r. w sprawie badań klinicznych produktów leczniczych stosowanych u ludzi oraz uchylenia dyrektywy 2001/20/WE (Dz.U. L 158 z 27.5.2014, s. 1).

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

Akty delegowane powinny zostać w szczególności przyjęte w odniesieniu do kryteriów i wymogów obowiązujących w mechanizmach certyfikacji, w odniesieniu do informacji przedstawianych za pomocą standardowych znaków graficznych oraz w odniesieniu do procedur ustanawiania takich znaków. Szczególnie ważne jest, aby w czasie swoich prac przygotowawczych Komisja prowadziła odpowiednie konsultacje, w tym na szczeblu eksperckim. W trakcie przygotowywania i opracowywania aktów delegowanych Komisja powinna zapewnić jednoczesne, terminowe i odpowiednie przekazywanie stosownych dokumentów Parlamentowi Europejskiemu i Radzie.

(167) Aby zapewnić jednolite warunki wdrażania niniejszego rozporządzenia, należy powierzyć Komisji uprawnienia wykonawcze, tak jak to przewiduje niniejsze rozporządzenie. Uprawnienia te powinny być wykonywane zgodnie z rozporządzeniem (UE) nr 182/2011. W tym kontekście Komisja powinna rozważyć wprowadzenie szczególnych środków dla mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw.

(168) Procedurę sprawdzającą należy stosować do przyjmowania aktów wykonawczych w odniesieniu do: standardowych klauzul umownych między administratorami a podmiotami przetwarzającymi oraz między podmiotami przetwarzającymi; kodeksów postępowania; technicznych standardów i mechanizmów certyfikacji; odpowiedniego stopnia ochrony zapewnianego przez państwo trzecie, terytorium lub określony sektor w tym państwie trzecim lub organizację międzynarodową; standardowych klauzul ochrony danych; formatów i procedur wymiany informacji drogą elektroniczną między administratorami, pomiotami przetwarzającymi i organami nadzorczymi na potrzeby wiążących reguł korporacyjnych; wzajemnej pomocy; oraz uzgodnień w sprawie wymiany informacji drogą elektroniczną między organami nadzorczymi oraz między organami nadzorczymi a Europejską Radą Ochrony Danych.

(169) Komisja powinna przyjmować akty wykonawcze mające natychmiastowe zastosowanie, jeżeli z dostępnych dowodów wynika, że państwo trzecie, terytorium lub określony sektor w tym państwie trzecim lub organizacja międzynarodowa nie zapewniają odpowiedniego stopnia ochrony, i jeżeli zachodzi szczególnie pilna potrzeba działania.

(170) Ponieważ celu niniejszego rozporządzenia, mianowicie zapewnienia równoważnego stopnia ochrony osób fizycznych i swobodnego przepływu danych osobowych w całej Unii, nie mogą w wystarczającym stopniu osiągnąć państwa członkowskie, natomiast z uwagi na zakres i skutki proponowanego działania możliwe jest lepsze jego osiągnięcie na szczeblu unijnym, Unia może przyjąć środki zgodnie z zasadą pomocniczości, o której mowa w art. 5 Traktatu o Unii Europejskiej (TUE). Zgodnie z zasadą proporcjonalności określoną w tym samym artykule niniejsze rozporządzenie nie wykracza poza zakres niezbędny do osiągnięcia tego celu.

(171) Niniejszym rozporządzeniem należy uchylić dyrektywę 95/46/WE. Przetwarzanie, które w dniu rozpoczęcia stosowania niniejszego rozporządzenia już się toczy, powinno w terminie dwóch lat od wejścia niniejszego rozporządzenia w życie zostać dostosowane do jego przepisów. Jeżeli przetwarzanie ma za podstawę zgodę w myśl dyrektywy 95/46/WE, osoba, której dane dotyczą, nie musi ponownie wyrażać zgody, jeżeli pierwotny sposób jej wyrażenia odpowiada warunkom niniejszego rozporządzenia; dzięki temu administrator może kontynuować przetwarzanie po dacie rozpoczęcia stosowania niniejszego rozporządzenia. Decyzje przyjęte przez Komisję oraz zezwolenia wydane przez organy nadzorcze na podstawie dyrektywy 95/46/WE pozostają w mocy do czasu ich zmiany, zastąpienia lub uchylenia.

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

(173) Niniejsze rozporządzenie powinno mieć zastosowanie do wszystkich tych kwestii dotyczących ochrony podstawowych praw i wolności w związku z przetwarzaniem danych osobowych, które nie podlegają szczególnym obowiązkom mającym ten sam cel określonym w dyrektywie Parlamentu Europejskiego i Rady 2002/58/WE ([2]), w tym obowiązkom nałożonym na administratora oraz prawom osób fizycznych. Aby doprecyzować związek między niniejszym rozporządzeniem a dyrektywą 2002/58/WE, dyrektywę tę należy odpowiednio zmienić. Gdy niniejsze rozporządzenie zostanie przyjęte, dyrektywa 2002/58/WE powinna zostać poddana przeglądowi, w szczególności w celu zapewnienia jej spójności z niniejszym rozporządzeniem,

([1]) Dz.U. C 192 z 30.6.2012, s. 7.
([2]) Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz.U. L 201 z 31.7.2002, s. 37).

PRZYJMUJĄ NINIEJSZE ROZPORZĄDZENIE:

ROZDZIAŁ I

Przepisy ogólne

Artykuł 1

Przedmiot i cele

1. W niniejszym rozporządzeniu ustanowione zostają przepisy o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych oraz przepisy o swobodnym przepływie danych osobowych.

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

3. Nie ogranicza się ani nie zakazuje swobodnego przepływu danych osobowych w Unii z powodów odnoszących się do ochrony osób fizycznych w związku z przetwarzaniem danych osobowych.

Artykuł 2

Materialny zakres stosowania

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

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

a) w ramach działalności nieobjętej zakresem prawa Unii;

b) przez państwa członkowskie w ramach wykonywania działań wchodzących w zakres tytułu V rozdział 2 TUE;

c) przez osobę fizyczną w ramach czynności o czysto osobistym lub domowym charakterze;

d) przez właściwe organy do celów 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.

3. Do przetwarzania danych osobowych przez instytucje, organy i jednostki organizacyjne Unii zastosowanie ma rozporządzenie (WE) nr 45/2001. Rozporządzenie (WE) nr 45/2001 oraz inne unijne akty prawne mające zastosowanie do takiego przetwarzania danych osobowych zostają dostosowane do zasad i przepisów niniejszego rozporządzenia zgodnie z art. 98.

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

Artykuł 3

Terytorialny zakres stosowania

1. Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych w związku z działalnością prowadzoną przez jednostkę organizacyjną administratora lub podmiotu przetwarzającego w Unii, niezależnie od tego, czy przetwarzanie odbywa się w Unii.

2. Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych osób, których dane dotyczą, przebywających w Unii przez administratora lub podmiot przetwarzający niemających jednostek organizacyjnych w Unii, jeżeli czynności przetwarzania wiążą się z:

a) oferowaniem towarów lub usług takim osobom, których dane dotyczą, w Unii – niezależnie od tego, czy wymaga się od tych osób zapłaty; lub

b) monitorowaniem ich zachowania, o ile do zachowania tego dochodzi w Unii.

3. Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych przez administratora niemającego jednostki organizacyjnej w Unii, ale posiadającego jednostkę organizacyjną w miejscu, w którym na mocy prawa międzynarodowego publicznego ma zastosowanie prawo państwa członkowskiego.

Artykuł 4

Definicje

Na użytek niniejszego rozporządzenia:

1) „dane osobowe" oznaczają 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 lub jeden bądź 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, taką 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 zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;

7) „administrator" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania;

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

9) „odbiorca" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę 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;

10) „strona trzecia" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe;

11) „zgoda" osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;

12) „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;

13) „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;

14) „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, takie jak wizerunek twarzy lub dane daktyloskopijne;

15) „dane dotyczące zdrowia" oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia;

16) „główna jednostka organizacyjna" oznacza:

a) jeżeli chodzi o administratora posiadającego jednostki organizacyjne w więcej niż jednym państwie członkowskim – miejsce, w którym znajduje się jego centralna administracja w Unii, a jeżeli decyzje co do celów i sposobów przetwarzania danych osobowych zapadają w innej jednostce organizacyjnej tego administratora w Unii i ta jednostka organizacyjna ma prawo nakazać wykonanie takich decyzji, to za główną jednostkę organizacyjną uznaje się jednostkę organizacyjną, w której zapadają takie decyzje;

b) jeżeli chodzi o podmiot przetwarzający posiadający jednostki organizacyjne w więcej niż jednym państwie członkowskim – miejsce, w którym znajduje się jego centralna administracja w Unii lub, w przypadku gdy podmiot przetwarzający nie ma centralnej administracji w Unii – jednostkę organizacyjną podmiotu przetwarzającego w Unii, w której odbywają się główne czynności przetwarzania w ramach działalności jednostki organizacyjnej podmiotu przetwarzającego, w zakresie w jakim podmiot przetwarzający podlega szczególnym obowiązkom na mocy niniejszego rozporządzenia;

17) „przedstawiciel" oznacza osobę fizyczną lub prawną mającą miejsce zamieszkania lub siedzibę w Unii, która została wyznaczona na piśmie przez administratora lub podmiot przetwarzający na mocy art. 27 do reprezentowania administratora lub podmiotu przetwarzającego w zakresie ich obowiązków wynikających z niniejszego rozporządzenia;

18) „przedsiębiorca" oznacza osobę fizyczną lub prawną prowadzącą działalność gospodarczą, niezależnie od formy prawnej, w tym spółki osobowe lub zrzeszenia prowadzące regularną działalność gospodarczą;

19) „grupa przedsiębiorstw" oznacza przedsiębiorstwo sprawujące kontrolę oraz przedsiębiorstwa przez nie kontrolowane;

20) „wiążące reguły korporacyjne" oznaczają polityki ochrony danych osobowych stosowane przez administratora lub podmiot przetwarzający, którzy posiadają jednostkę organizacyjną na terytorium państwa członkowskiego, przy jednorazowym lub wielokrotnym przekazaniu danych osobowych administratorowi lub podmiotowi przetwarzającemu w co najmniej jednym państwie trzecim w ramach grupy przedsiębiorstw lub grupy przedsiębiorców prowadzących wspólną działalność gospodarczą;

21) „organ nadzorczy" oznacza niezależny organ publiczny ustanowiony przez państwo członkowskie zgodnie z art. 51;

22) „organ nadzorczy, którego sprawa dotyczy" oznacza organ nadzorczy, którego dotyczy przetwarzanie danych osobowych, ponieważ:

a) administrator lub podmiot przetwarzający posiadają jednostkę organizacyjną na terytorium państwa członkowskiego tego organu nadzorczego;

b) przetwarzanie znacznie wpływa lub może znacznie wpłynąć na osoby, których dane dotyczą, mające miejsce zamieszkania w państwie członkowskim tego organu nadzorczego; lub

c) wniesiono do niego skargę;

23) „transgraniczne przetwarzanie" oznacza:

a) przetwarzanie danych osobowych, które odbywa się w Unii w ramach działalności jednostek organizacyjnych w więcej, niż jednym państwie członkowskim administratora lub podmiotu przetwarzającego w Unii posiadającego jednostki organizacyjne w więcej niż jednym państwie członkowskim; albo

b) przetwarzanie danych osobowych, które odbywa się w Unii w ramach działalności pojedynczej jednostki organizacyjnej administratora lub podmiotu przetwarzającego w Unii, ale które znacznie wpływa lub może znacznie wpłynąć na osoby, których dane dotyczą, w więcej niż jednym państwie członkowskim;

24) „mający znaczenie dla sprawy i uzasadniony sprzeciw" oznacza sprzeciw wobec projektu decyzji dotyczącej tego, czy doszło do naruszenia niniejszego rozporządzenia lub czy planowane działanie wobec administratora lub podmiotu przetwarzającego jest zgodne z niniejszym rozporządzeniem, który to sprzeciw musi jasno wskazywać wagę wynikającego z projektu decyzji ryzyka naruszenia podstawowych praw lub wolności osób, których dane dotyczą, oraz gdy ma to zastosowanie – wagę ryzyka zakłócenia swobodnego przepływu danych osobowych w Unii;

25) „usługa społeczeństwa informacyjnego" oznacza usługę w rozumieniu art. 1 ust. 1 lit. b) dyrektywy Parlamentu Europejskiego i Rady (UE) 2015/1535 ([1]);

26) „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 5

Zasady dotyczące przetwarzania danych osobowych

1. Dane osobowe muszą być:

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

b) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 za niezgodne z pierwotnymi celami („ograniczenie celu");

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

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

([1]) Dyrektywa (UE) 2015/1535 Parlamentu Europejskiego i Rady z dnia 9 września 2015 r. ustanawiająca procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego (Dz.U. L 241 z 17.9.2015, s. 1).

e) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą („ograniczenie przechowywania");

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

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

Artykuł 6

Zgodność przetwarzania z prawem

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

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

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

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

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

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

f) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

Akapit pierwszy lit. f) nie ma zastosowania do przetwarzania, którego dokonują organy publiczne w ramach realizacji swoich zadań.

2. Państwa członkowskie mogą zachować lub wprowadzić bardziej szczegółowe przepisy, aby dostosować stosowanie przepisów niniejszego rozporządzenia w odniesieniu do przetwarzania służącego wypełnieniu warunków określonych w ust. 1 lit. c) i e); w tym celu mogą dokładniej określić szczegółowe wymogi przetwarzania i inne środki w celu zapewnienia zgodności przetwarzania z prawem i jego rzetelności, także w innych szczególnych sytuacjach związanych z przetwarzaniem przewidzianych w rozdziale IX.

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

a) w prawie Unii; lub

b) w prawie państwa członkowskiego, któremu podlega administrator.

Cel przetwarzania musi być określony w tej podstawie prawnej lub, w przypadku przetwarzania, o którym mowa w ust. 1 lit. e) – musi być ono niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi. Podstawa prawna może zawierać przepisy szczegółowe dostosowujące stosowanie przepisów niniejszego rozporządzenia, w tym: ogólne warunki zgodności z prawem przetwarzania przez administratora; rodzaj danych podlegających przetwarzaniu; osoby, których dane dotyczą; podmioty, którym można ujawnić dane osobowe; cele, w których można je ujawnić; ograniczenia celu; okresy przechowywania; oraz operacje i procedury przetwarzania, w tym środki zapewniające zgodność z prawem i rzetelność przetwarzania,

w tym w innych szczególnych sytuacjach związanych z przetwarzaniem, o których mowa w rozdziale IX. Prawo Unii lub prawo państwa członkowskiego muszą służyć realizacji celu leżącego w interesie publicznym, oraz być proporcjonalne do wyznaczonego, prawnie uzasadnionego celu.

4. Jeżeli przetwarzanie w celu innym niż cel, w którym dane osobowe zostały zebrane, nie odbywa się na podstawie zgody osoby, której dane dotyczą, ani prawa Unii lub prawa państwa członkowskiego stanowiących w demokratycznym społeczeństwie niezbędny i proporcjonalny środek służący zagwarantowaniu celów, o których mowa w art. 23 ust. 1, administrator – aby ustalić, czy przetwarzanie w innym celu jest zgodne z celem, w którym dane osobowe zostały pierwotnie zebrane – bierze pod uwagę między innymi:

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

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

c) charakter danych osobowych, w szczególności czy przetwarzane są szczególne kategorie danych osobowych zgodnie z art. 9 lub dane osobowe dotyczące wyroków skazujących i naruszeń prawa zgodnie z art. 10;

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

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

Artykuł 7

Warunki wyrażenia zgody

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

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

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

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

Artykuł 8

Warunki wyrażenia zgody przez dziecko w przypadku usług społeczeństwa informacyjnego

1. Jeżeli zastosowanie ma art. 6 ust. 1 lit. a), w przypadku usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku, zgodne z prawem jest przetwarzanie danych osobowych dziecka, które ukończyło 16 lat. Jeżeli dziecko nie ukończyło 16 lat, takie przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy zgodę wyraziła lub zaaprobowała ją osoba sprawująca władzę rodzicielską lub opiekę nad dzieckiem oraz wyłącznie w zakresie wyrażonej zgody.

Państwa członkowskie mogą przewidzieć w swoim prawie niższą granicę wiekową, która musi wynosić co najmniej 13 lat.

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

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

Artykuł 9

Przetwarzanie szczególnych kategorii danych osobowych

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

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

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

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

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

d) przetwarzania dokonuje się w ramach uprawnionej działalności prowadzonej z zachowaniem odpowiednich zabezpieczeń przez fundację, stowarzyszenie lub inny niezarobkowy podmiot o celach politycznych, światopoglądowych, religijnych lub związkowych, pod warunkiem że przetwarzanie dotyczy wyłącznie członków lub byłych członków tego podmiotu lub osób utrzymujących z nim stałe kontakty w związku z jego celami oraz że dane osobowe nie są ujawniane poza tym podmiotem bez zgody osób, których dane dotyczą;

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

f) przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy;

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

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

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

j) przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie, konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.

3. Dane osobowe, o których mowa w ust. 1, mogą być przetwarzane do celów, o których mowa w ust. 2 lit. h), jeżeli są przetwarzane przez – lub na odpowiedzialność – pracownika podlegającego obowiązkowi zachowania tajemnicy zawodowej na mocy prawa Unii lub prawa państwa członkowskiego, lub przepisów ustanowionych przez właściwe organy krajowe lub przez inną osobę również podlegającą obowiązkowi zachowania tajemnicy zawodowej na mocy prawa Unii lub prawa państwa członkowskiego, lub przepisów ustanowionych przez właściwe organy krajowe.

4. Państwa członkowskie mogą zachować lub wprowadzić dalsze warunki, w tym ograniczenia w odniesieniu do przetwarzania danych genetycznych, danych biometrycznych lub danych dotyczących zdrowia.

Artykuł 10

Przetwarzanie danych osobowych dotyczących wyroków skazujących i naruszeń prawa

Przetwarzania danych osobowych dotyczących wyroków skazujących oraz naruszeń prawa lub powiązanych środków bezpieczeństwa na podstawie art. 6 ust. 1 wolno dokonywać wyłącznie pod nadzorem władz publicznych lub jeżeli przetwarzanie jest dozwolone prawem Unii lub prawem państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw i wolności osób, których dane dotyczą. Wszelkie kompletne rejestry wyroków skazujących są prowadzone wyłącznie pod nadzorem władz publicznych.

Artykuł 11

Przetwarzanie niewymagające identyfikacji

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

2. Jeżeli w przypadkach, o których mowa w ust. 1 niniejszego artykułu, administrator może wykazać, że nie jest w stanie zidentyfikować osoby, której dane dotyczą, w miarę możliwości informuje o tym osobę, której dane dotyczą. W takich przypadkach zastosowania nie mają art. 15–20, chyba że osoba, której dane dotyczą, w celu wykonania praw przysługujących jej na mocy tych artykułów dostarczy dodatkowych informacji pozwalających ją zidentyfikować.

ROZDZIAŁ III

Prawa osoby, której dane dotyczą

Sekcja 1

Przejrzystość oraz tryb korzystania z praw

Artykuł 12

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

1. Administrator podejmuje odpowiednie środki, aby w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem – w szczególności gdy informacje są kierowane do dziecka – udzielić osobie, której dane dotyczą, wszelkich informacji, o których mowa w art. 13 i 14, oraz prowadzić z nią wszelką komunikację na mocy art. 15–22 i 34 w sprawie przetwarzania. Informacji udziela się na piśmie lub w inny sposób, w tym w stosownych przypadkach – elektronicznie. Jeżeli osoba, której dane dotyczą, tego zażąda, informacji można udzielić ustnie, o ile innymi sposobami potwierdzi się tożsamość osoby, której dane dotyczą.

2. Administrator ułatwia osobie, której dane dotyczą, wykonanie praw przysługujących jej na mocy art. 15–22. W przypadkach, o których mowa w art. 11 ust. 2, administrator nie odmawia podjęcia działań na żądanie osoby której dane dotyczą pragnącej wykonać prawa przysługujące jej na mocy art. 15–22, chyba że wykaże, iż nie jest w stanie zidentyfikować osoby, której dane dotyczą.

3. Administrator bez zbędnej zwłoki – a w każdym razie w terminie miesiąca od otrzymania żądania – udziela osobie, której dane dotyczą, informacji o działaniach podjętych w związku z żądaniem na podstawie art. 15–22. W razie potrzeby termin ten można przedłużyć o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań. W terminie miesiąca od otrzymania żądania administrator informuje osobę, której dane dotyczą o takim przedłużeniu terminu, z podaniem przyczyn opóźnienia. Jeśli osoba, której dane dotyczą, przekazała swoje żądanie elektronicznie, w miarę możliwości informacje także są przekazywane elektronicznie, chyba że osoba, której dane dotyczą, zażąda innej formy.

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

5. Informacje podawane na mocy art. 13 i 14 oraz komunikacja i działania podejmowane na mocy art. 15–22 i 34 są wolne od opłat. Jeżeli żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, administrator może:

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

b) odmówić podjęcia działań w związku z żądaniem.

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

6. Bez uszczerbku dla art. 11, jeżeli administrator ma uzasadnione wątpliwości co do tożsamości osoby fizycznej składającej żądanie, o którym mowa w art. 15–21, może zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby, której dane dotyczą.

7. Informacje, których udziela się osobom, których dane dotyczą, na mocy art. 13 i 14, można opatrzyć standardowymi znakami graficznymi, które w widoczny, zrozumiały i czytelny sposób przedstawią sens zamierzonego przetwarzania. Jeżeli znaki te są przedstawione elektronicznie, muszą się nadawać do odczytu maszynowego.

8. Komisji przysługuje prawo przyjmowania aktów delegowanych zgodnie z art. 92 w celu określenia informacji przedstawianych za pomocą znaków graficznych i procedur ustanowienia standardowych znaków graficznych.

Sekcja 2

Informacje i dostęp do danych osobowych

Artykuł 13

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

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

a) swoją tożsamość i dane kontaktowe oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe swojego przedstawiciela;

b) gdy ma to zastosowanie – dane kontaktowe inspektora ochrony danych;

c) cele przetwarzania danych osobowych, oraz podstawę prawną przetwarzania;

d) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f) – prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią;

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

f) gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych.

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

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

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

c) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;

d) informacje o prawie wniesienia skargi do organu nadzorczego;

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

f) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

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

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

Artykuł 14

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

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

a) swoją tożsamość i dane kontaktowe oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe swojego przedstawiciela;

b) gdy ma to zastosowanie – dane kontaktowe inspektora ochrony danych;

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

d) kategorie odnośnych danych osobowych;

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

f) gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych odbiorcy w państwie trzecim lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych.

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

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

b) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f) – prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią;

c) informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania oraz o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;

d) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;

e) informacje o prawie wniesienia skargi do organu nadzorczego;

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

g) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

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

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

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

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

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

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

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

b) udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku; w szczególności w przypadku przetwarzania do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, z zastrzeżeniem warunków i zabezpieczeń, o których mowa w art. 89 ust. 1, lub o ile obowiązek, o którym mowa w ust. 1 niniejszego artykułu, może uniemożliwić lub poważnie utrudnić realizację celów takiego przetwarzania. W takich przypadkach administrator podejmuje odpowiednie środki, by chronić prawa i wolności oraz prawnie uzasadnione interesy osoby, której dane dotyczą, w tym udostępnia informacje publicznie;

c) pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator, przewidującym odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą; lub

d) dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianym w prawie Unii lub w prawie państwa członkowskiego, w tym ustawowym obowiązkiem zachowania tajemnicy.

Artykuł 15

Prawo dostępu przysługujące osobie, której dane dotyczą

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

a) cele przetwarzania;

b) kategorie odnośnych danych osobowych;

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

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

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

f) informacje o prawie wniesienia skargi do organu nadzorczego;

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

h) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

2. Jeżeli dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej, osoba, której dane dotyczą, ma prawo zostać poinformowana o odpowiednich zabezpieczeniach, o których mowa w art. 46, związanych z przekazaniem.

3. Administrator dostarcza osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu. Za wszelkie kolejne kopie, o które zwróci się osoba, której dane dotyczą, administrator może pobrać opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych. Jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się powszechnie stosowaną drogą elektroniczną.

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

Sekcja 3

Sprostowanie i usuwanie danych

Artykuł 16

Prawo do sprostowania danych

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

Artykuł 17

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

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

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

b) osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie zgodnie z art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a), i nie ma innej podstawy prawnej przetwarzania;

c) osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 1 wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania lub osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 2 wobec przetwarzania;

d) dane osobowe były przetwarzane niezgodnie z prawem;

e) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator;

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

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

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

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

b) do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;

c) z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego zgodnie z art. 9 ust. 2 lit. h) oraz i) i art. 9 ust. 3;

d) do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1, o ile prawdopodobne jest, że prawo, o którym mowa w ust. 1, uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania; lub

e) do ustalenia, dochodzenia lub obrony roszczeń.

Artykuł 18

Prawo do ograniczenia przetwarzania

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

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

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

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

d) osoba, której dane dotyczą, wniosła sprzeciw na mocy art. 21 ust. 1 wobec przetwarzania – do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie administratora są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.

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

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

Artykuł 19

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

Administrator informuje o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania, których dokonał zgodnie z art. 16, art. 17 ust. 1 i art. 18, każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Administrator informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.

Artykuł 20

Prawo do przenoszenia danych

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

a) przetwarzanie odbywa się na podstawie zgody w myśl art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) lub na podstawie umowy w myśl art. 6 ust. 1 lit. b); oraz

b) przetwarzanie odbywa się w sposób zautomatyzowany.

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

3. Wykonanie prawa, o którym mowa w ust. 1 niniejszego artykułu, pozostaje bez uszczerbku dla art. 17. Prawo to nie ma zastosowania do przetwarzania, które jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.

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

Sekcja 4

Prawo do sprzeciwu oraz zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach

Artykuł 21

Prawo do sprzeciwu

1. Osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych opartego na art. 6 ust. 1 lit. e) lub f), w tym profilowania na podstawie tych przepisów. Administratorowi nie wolno już przetwarzać tych danych osobowych, chyba że wykaże on istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.

2. Jeżeli dane osobowe są przetwarzane na potrzeby marketingu bezpośredniego, osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania dotyczących jej danych osobowych na potrzeby takiego marketingu, w tym profilowania, w zakresie, w jakim przetwarzanie jest związane z takim marketingiem bezpośrednim.

3. Jeżeli osoba, której dane dotyczą, wniesie sprzeciw wobec przetwarzania do celów marketingu bezpośredniego, danych osobowych nie wolno już przetwarzać do takich celów.

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

5. W związku z korzystaniem z usług społeczeństwa informacyjnego i bez uszczerbku dla dyrektywy 2002/58/WE osoba, której dane dotyczą, może wykonać prawo do sprzeciwu za pośrednictwem zautomatyzowanych środków wykorzystujących specyfikacje techniczne.

6. Jeżeli dane osobowe są przetwarzane do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, osoba, której dane dotyczą, ma prawo wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.

Artykuł 22

Zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach, w tym profilowanie

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

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

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

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

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

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

4. Decyzje, o których mowa w ust. 2, nie mogą opierać się na szczególnych kategoriach danych osobowych, o których mowa w art. 9 ust. 1, chyba że zastosowanie ma art. 9 ust. 2 lit. a) lub g) i istnieją właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą.

Sekcja 5

Ograniczenia

Artykuł 23

Ograniczenia

1. Prawo Unii lub prawo państwa członkowskiego, któremu podlegają administrator danych lub podmiot przetwarzający, może aktem prawnym ograniczyć zakres obowiązków i praw przewidzianych w art. 12–22 i w art. 34, a także w art. 5 – o ile jego przepisy odpowiadają prawom i obowiązkom przewidzianym w art. 12–22 – jeżeli ograniczenie takie nie narusza istoty podstawowych praw i wolności oraz jest w demokratycznym społeczeństwie środkiem niezbędnym i proporcjonalnym, służącym:

a) bezpieczeństwu narodowemu;

b) obronie;

c) bezpieczeństwu publicznemu;

d) zapobieganiu przestępczości, prowadzeniu postępowań przygotowawczych, wykrywaniu lub ściganiu czynów zabronionych lub wykonywaniu kar, w tym ochronie przed zagrożeniami dla bezpieczeństwa publicznego i zapobieganiu takim zagrożeniom;

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

f) ochronie niezależności sądów i postępowania sądowego;

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

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

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

j) egzekucji roszczeń cywilnoprawnych.

2. W szczególności akt prawny, o którym mowa w ust. 1, musi zawierać szczegółowe przepisy przynajmniej – w stosownym przypadku – o:

a) celach przetwarzania lub kategorii przetwarzania;

b) kategoriach danych osobowych;

c) zakresie wprowadzonych ograniczeń;

d) zabezpieczeniach zapobiegających nadużyciom lub niezgodnemu z prawem dostępowi lub przekazywaniu;

e) określeniu administratora lub kategorii administratorów;

f) okresach przechowywania oraz mających zastosowanie zabezpieczeniach z uwzględnieniem charakteru, zakresu i celów przetwarzania lub kategorii przetwarzania;

g) ryzyka naruszenia praw lub wolności osoby, której dane dotyczą; oraz

h) prawie osób, której dane dotyczą, do uzyskania informacji o ograniczeniach, o ile nie narusza to celu ograniczenia.

ROZDZIAŁ IV

Administrator i podmiot przetwarzający

Sekcja 1

Obowiązki ogólne

Artykuł 24

Obowiązki administratora

1. Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane.

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

3. Stosowanie zatwierdzonych kodeksów postępowania, o których mowa wart. 40, lub zatwierdzonego mechanizmu certyfikacji, o którym mowa wart. 42, może być wykorzystane jako element dla stwierdzenia przestrzegania przez administratora ciążących na nim obowiązków.

Artykuł 25

Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych

1. Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania, administrator – zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania –wdraża odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi niniejszego rozporządzenia oraz chronić prawa osób, których dane dotyczą.

2. Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. W szczególności środki te zapewniają, by domyślnie dane osobowe nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych.

3. Wywiązywanie się z obowiązków, o których mowa w ust. 1 i 2 niniejszego artykułu, można wykazać między innymi poprzez wprowadzenie zatwierdzonego mechanizmu certyfikacji określonego w art. 42.

Artykuł 26

Współadministratorzy

1. Jeżeli co najmniej dwóch administratorów wspólnie ustala cele i sposoby przetwarzania, są oni współadministratorami. W drodze wspólnych uzgodnień współadministratorzy w przejrzysty sposób określają odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z niniejszego rozporządzenia, w szczególności w odniesieniu do wykonywania przez osobę, której dane dotyczą, przysługujących jej praw, oraz ich obowiązków w odniesieniu do podawania informacji, o których mowa w art. 13 i 14, chyba że przypadające im obowiązki i ich zakres określa prawo Unii lub prawo państwa członkowskiego, któremu administratorzy ci podlegają. W uzgodnieniach można wskazać punkt kontaktowy dla osób, których dane dotyczą.

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

3. Niezależnie od uzgodnień, o których mowa w ust. 1, osoba, której dane dotyczą, może wykonywać przysługujące jej prawa wynikające z niniejszego rozporządzenia wobec każdego z administratorów.

Artykuł 27

Przedstawiciele administratorów lub podmiotów przetwarzających niemających jednostki organizacyjnej w Unii

1. Jeżeli zastosowanie ma art. 3 ust. 2, administrator lub podmiot przetwarzający na piśmie wyznacza swojego przedstawiciela w Unii.

2. Obowiązek ustanowiony w ust. 1 niniejszego artykułu nie ma zastosowania w przypadku:

a) przetwarzania, które ma charakter sporadyczny, nie obejmuje – na dużą skalę – przetwarzania szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1, ani przetwarzania danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10, i jest mało prawdopodobne, by ze względu na swój charakter, kontekst, zakres i cele powodowało ryzyko naruszenia praw lub wolności osób fizycznych; lub

b) organu lub podmiotu publicznego.

3. Przedstawiciel musi mieć siedzibę w państwie członkowskim, w którym przebywają osoby, których dane dotyczą, których dane osobowe są przetwarzane w związku z oferowaniem im towarów lub usług lub których zachowanie jest monitorowane.

4. Przedstawiciel zostaje upoważniony przez administratora lub podmiot przetwarzający, by do celów zapewnienia przestrzegania niniejszego rozporządzenia mogły się do niego zwracać – oprócz lub zamiast do administratora lub podmiotu przetwarzającego – w szczególności organy nadzorcze i osoby, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem.

5. Wyznaczenie przedstawiciela przez administratora lub podmiot przetwarzający pozostaje bez uszczerbku dla postępowań, które mogą zostać wszczęte przeciwko samemu administratorowi lub podmiotowi przetwarzającemu.

Artykuł 28

Podmiot przetwarzający

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

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

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

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

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

c) podejmuje wszelkie środki wymagane na mocy art. 32;

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

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

f) uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga administratorowi wywiązać się z obowiązków określonych w art. 32–36;

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

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

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

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

5. Wystarczające gwarancje, o których mowa w ust. 1 i 4 niniejszego artykułu, podmiot przetwarzający może wykazać między innymi poprzez stosowanie zatwierdzonego kodeksu postępowania, o którym mowa w art. 40 lub zatwierdzonego mechanizmu certyfikacji, o którym mowa w art. 42.

6. Bez uszczerbku dla indywidualnych umów między administratorem a podmiotem przetwarzającym, umowa lub inny akt prawny, o których mowa w ust. 3 i 4 niniejszego artykułu, mogą się opierać w całości lub w części na standardowych klauzulach umownych, o których mowa w ust. 7 i 8 niniejszego artykułu, także gdy są one elementem certyfikacji udzielonej administratorowi lub podmiotowi przetwarzającemu zgodnie z art. 42 i 43.

7. Komisja może określić standardowe klauzule umowne dotyczące kwestii, o których mowa w ust. 3 i 4 niniejszego artykułu, zgodnie z procedurą sprawdzającą, o której mowa w art. 93 ust. 2.

8. Organ nadzorczy może przyjąć standardowe klauzule umowne dotyczące kwestii, o których mowa w ust. 3 i 4 niniejszego artykułu, zgodnie z mechanizmem spójności, o którym mowa w art. 63.

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

10. Bez uszczerbku dla art. 82, 83 i 84, jeżeli podmiot przetwarzający naruszy niniejsze rozporządzenie przy określaniu celów i sposobów przetwarzania, uznaje się go za administratora w odniesieniu do tego przetwarzania.

Artykuł 29

Przetwarzanie z upoważnienia administratora lub podmiotu przetwarzającego

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

Artykuł 30

Rejestrowanie czynności przetwarzania

1. Każdy administrator oraz – gdy ma to zastosowanie – przedstawiciel administratora prowadzą rejestr czynności przetwarzania danych osobowych, za które odpowiadają. W rejestrze tym zamieszcza się wszystkie następujące informacje:

a) imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także gdy ma to zastosowanie – przedstawiciela administratora oraz inspektora ochrony danych;

b) cele przetwarzania;

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

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

e) gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi, dokumentacja odpowiednich zabezpieczeń;

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

g) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1.

2. Każdy podmiot przetwarzający oraz – gdy ma to zastosowanie – przedstawiciel podmiotu przetwarzającego prowadzą rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora, zawierający następujące informacje:

a) imię i nazwisko lub nazwa oraz dane kontaktowe podmiotu przetwarzającego lub podmiotów przetwarzających oraz każdego administratora, w imieniu którego działa podmiot przetwarzający, a gdy ma to zastosowanie – przedstawiciela administratora lub podmiotu przetwarzającego oraz inspektora ochrony danych;

b) kategorie przetwarzań dokonywanych w imieniu każdego z administratorów;

c) gdy ma to zastosowanie –przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi, dokumentacja odpowiednich zabezpieczeń;

d) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1.

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

4. Administrator lub podmiot przetwarzający oraz – gdy ma to zastosowanie – przedstawiciel administratora lub podmiotu przetwarzającego udostępniają rejestr na żądanie organu nadzorczego.

5. Obowiązki, o których mowa w ust. 1 i 2, nie mają zastosowania do przedsiębiorcy lub podmiotu zatrudniającego mniej niż 250 osób, chyba że przetwarzanie, którego dokonują, może powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą, nie ma charakteru sporadycznego lub obejmuje szczególne kategorie danych osobowych, o których mowa w art. 9 ust. 1, lub dane osobowe dotyczące wyroków skazujących i naruszeń prawa, o czym mowa w art. 10.

Artykuł 31

Współpraca z organem nadzorczym

Administrator i podmiot przetwarzający oraz – gdy ma to zastosowanie – ich przedstawiciele na żądanie współpracują z organem nadzorczym w ramach wykonywania przez niego swoich zadań.

Sekcja 2

Bezpieczeństwo danych osobowych

Artykuł 32

Bezpieczeństwo przetwarzania

1. Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym między innymi w stosownym przypadku:

a) pseudonimizację i szyfrowanie danych osobowych;

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

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

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

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

3. Wywiązywanie się z obowiązków, o których mowa w ust. 1 niniejszego artykułu, można wykazać między innymi poprzez stosowanie zatwierdzonego kodeksu postępowania, o którym mowa w art. 40 lub zatwierdzonego mechanizmu certyfikacji, o którym mowa w art. 42.

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

Artykuł 33

Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu

1. W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 55, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

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

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

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

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

c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;

d) opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

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

5. Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu weryfikowanie przestrzegania niniejszego artykułu.

Artykuł 34

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

1. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.

2. Zawiadomienie, o którym mowa w ust. 1 niniejszego artykułu, jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki, o których mowa w art. 33 ust. 3 lit. b), c) i d).

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

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

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

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

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

Sekcja 3

Ocena skutków dla ochrony danych i uprzednie konsultacje

Artykuł 35

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 z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę.

2. Dokonując oceny skutków dla ochrony danych, administrator konsultuje się z inspektorem ochrony danych, jeżeli został on wyznaczony.

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

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

b) przetwarzania na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1, lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10; lub

c) systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.

4. Organ nadzorczy ustanawia i podaje do publicznej wiadomości wykaz rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny skutków dla ochrony danych na mocy ust. 1. Organ nadzorczy przekazuje te wykazy Europejskiej Radzie Ochrony Danych, o której mowa w art. 68.

5. Organ nadzorczy może także ustanowić i podać do wiadomości publicznej wykaz rodzajów operacji przetwarzania niepodlegających wymogowi dokonania oceny skutków dla ochrony danych. Organ nadzorczy przekazuje te wykazy Europejskiej Radzie Ochrony Danych.

6. Jeżeli wykazy, o których mowa w ust. 4 i 5, obejmują czynności przetwarzania związane z oferowaniem towarów lub usług osobom, których dane dotyczą, lub z monitorowaniem ich zachowania w kilku państwach członkowskich lub mogące znacznie wpłynąć na swobodny przepływ danych osobowych w Unii, przed przyjęciem takich wykazów właściwy organ nadzorczy stosuje mechanizm spójności, o którym mowa w art. 63.

7. Ocena zawiera co najmniej:

a) systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez administratora;

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

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

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

8. Oceniając – w szczególności do celów oceny skutków dla ochrony danych – skutki operacji przetwarzania wykonywanych przez administratora lub podmiot przetwarzający, uwzględnia się przestrzeganie przez takiego administratora lub taki podmiot przetwarzający zatwierdzonych kodeksów postępowania, o których mowa w art. 40.

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

10. Ust. 1–7 nie mają zastosowania, jeżeli przetwarzanie na mocy art. 6 ust. 1 lit. c) lub e) ma podstawę prawną w prawie Unii lub w prawie państwa członkowskiego, któremu podlega administrator, i prawo takie reguluje daną operację przetwarzania lub zestaw operacji, a oceny skutków dla ochrony danych dokonano już w ramach oceny skutków regulacji w związku z przyjęciem tej podstawy prawnej – chyba że państwa członkowskie uznają za niezbędne, by przed podjęciem czynności przetwarzania dokonać oceny skutków dla ochrony danych.

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

Artykuł 36

Uprzednie konsultacje

1. Jeżeli ocena skutków dla ochrony danych, o której mowa w art. 35, wskaże, że przetwarzanie powodowałoby wysokie ryzyko, gdyby administrator nie zastosował środków w celu zminimalizowania tego ryzyka, to przed rozpoczęciem przetwarzania administrator konsultuje się z organem nadzorczym.

2. Jeżeli organ nadzorczy jest zdania, że zamierzone przetwarzanie, o którym mowa w ust. 1, stanowiłoby naruszenie niniejszego rozporządzenia – w szczególności gdy administrator niedostatecznie zidentyfikował lub zminimalizował ryzyko – organ nadzorczy w terminie do ośmiu tygodni od wpłynięcia wniosku o konsultacje udziela administratorowi, a gdy ma to zastosowanie także podmiotowi przetwarzającemu pisemnego zalecenia i może skorzystać z dowolnego ze swoich uprawnień, o których mowa w art. 58. Okres ten można przedłużyć o sześć tygodni ze względu na złożony charakter zamierzonego przetwarzania. Organ nadzorczy informuje administratora, a gdy ma to zastosowanie także podmiot przetwarzający, o takim przedłużeniu w terminie miesiąca od wpłynięcia wniosku o konsultacje, z podaniem przyczyn tego opóźnienia. Bieg tych terminów można zawiesić, do czasu aż organ nadzorczy uzyska wszelkie informacje, których zażądał do celów konsultacji.

3. Konsultując się z organem nadzorczym zgodnie z ust. 1, administrator przedstawia mu:

a) gdy ma to zastosowanie – odpowiednie obowiązki administratora, współadministratorów oraz podmiotów przetwarzających uczestniczących w przetwarzaniu, w szczególności w przypadku przetwarzania w ramach grupy przedsiębiorstw;

b) cele i sposoby zamierzonego przetwarzania;

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

d) gdy ma to zastosowanie – dane kontaktowe inspektora ochrony danych;

e) ocenę skutków dla ochrony danych, o której mowa w art. 35; oraz

f) wszelkie inne informacje, których żąda organ nadzorczy.

4. Państwa członkowskie konsultują się z organem nadzorczym, przygotowując projekt aktu prawnego przyjmowanego przez parlament narodowy lub aktu wykonawczego opartego na takim akcie prawnym, jeżeli projekt dotyczy przetwarzania.

5. Niezależnie od ust. 1 prawo państwa członkowskiego może wymagać, by administratorzy konsultowali się z organem nadzorczym i uzyskiwali jego uprzednią zgodę na przetwarzanie danych osobowych przez administratora do celów wykonania zadania realizowanego przez administratora w interesie publicznym, w tym przetwarzania w związku z ochroną socjalną i zdrowiem publicznym.

Sekcja 4

Inspektor ochrony danych

Artykuł 37

Wyznaczenie inspektora ochrony danych

1. Administrator i podmiot przetwarzający wyznaczają inspektora ochrony danych, zawsze gdy:

a) przetwarzania dokonują organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości;

b) główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę; lub

c) główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1, oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10.

2. Grupa przedsiębiorstw może wyznaczyć jednego inspektora ochrony danych, o ile można będzie łatwo nawiązać z nim kontakt z każdej jednostki organizacyjnej.

3. Jeżeli administrator lub podmiot przetwarzający są organem lub podmiotem publicznym, dla kilku takich organów lub podmiotów można wyznaczyć – z uwzględnieniem ich struktury organizacyjnej i wielkości – jednego inspektora ochrony danych.

4. W przypadkach innych niż te, o których mowa w ust. 1, administrator, podmiot przetwarzający, zrzeszenia lub inne podmioty reprezentujące określone kategorie administratorów lub podmiotów przetwarzających mogą wyznaczyć lub jeżeli wymaga tego prawo Unii lub prawo państwa członkowskiego, wyznaczają inspektora ochrony danych. Inspektor ochrony danych może działać w imieniu takich zrzeszeń i innych podmiotów reprezentujących administratorów lub podmioty przetwarzające.

5. Inspektor ochrony danych jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, o których mowa w art. 39.

6. Inspektor ochrony danych może być członkiem personelu administratora lub podmiotu przetwarzającego lub wykonywać zadania na podstawie umowy o świadczenie usług.

7. Administrator lub podmiot przetwarzający publikują dane kontaktowe inspektora ochrony danych i zawiadamiają o nich organ nadzorczy.

Artykuł 38

Status inspektora ochrony danych

1. Administrator oraz podmiot przetwarzający zapewniają, by inspektor ochrony danych był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych.

2. Administrator oraz podmiot przetwarzający wspierają inspektora ochrony danych w wypełnianiu przez niego zadań, o których mowa w art. 39, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej.

3. Administrator oraz podmiot przetwarzający zapewniają, by inspektor ochrony danych nie otrzymywał instrukcji dotyczących wykonywania tych zadań. Nie jest on odwoływany ani karany przez administratora ani podmiot przetwarzający za wypełnianie swoich zadań. Inspektor ochrony danych bezpośrednio podlega najwyższemu kierownictwu administratora lub podmiotu przetwarzającego.

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

5. Inspektor ochrony danych jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań – zgodnie z prawem Unii lub prawem państwa członkowskiego.

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

Artykuł 39

Zadania inspektora ochrony danych

1. Inspektor ochrony danych ma następujące zadania:

a) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;

b) monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;

c) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35;

d) współpraca z organem nadzorczym;

e) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

2. Inspektor ochrony danych wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.

Sekcja 5

Kodeksy postępowania i certyfikacja

Artykuł 40

Kodeksy postępowania

1. Państwa członkowskie, organy nadzorcze, Europejska Rada Ochrony Danych oraz Komisja zachęcają do sporządzania kodeksów postępowania mających pomóc we właściwym stosowaniu niniejszego rozporządzenia – z uwzględnieniem specyfiki różnych sektorów dokonujących przetwarzania oraz szczególnych potrzeb mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw.

2. Zrzeszenia i inne podmioty reprezentujące określone kategorie administratorów lub podmioty przetwarzające mogą opracowywać lub zmieniać kodeksy postępowania lub rozszerzać ich zakres, aby doprecyzować zastosowanie niniejszego rozporządzenia, między innymi w odniesieniu do:

a) rzetelnego i przejrzystego przetwarzania;

b) prawnie uzasadnionych interesów realizowanych przez administratorów w określonych kontekstach;

c) zbierania danych osobowych;

d) pseudonimizacji danych osobowych;

e) informowania opinii publicznej i osób, których dane dotyczą;

f) wykonywania przez osoby, których dane dotyczą, przysługujących im praw;

g) informowania i ochrony dzieci oraz sposobu pozyskiwania zgody osoby sprawującej władzę rodzicielską lub opiekę nad dzieckiem;

h) środków i procedur, o których mowa w art. 24 i 25, oraz środków zapewniających bezpieczeństwo przetwarzania, o których mowa w art. 32;

i) zgłaszania organowi nadzorczemu naruszeń ochrony danych osobowych oraz zawiadamiania o takich naruszeniach osób, których dane dotyczą;

j) przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych; lub

k) postępowań pozasądowych oraz innych trybów rozstrzygania sporów w celu rozstrzygania sporów między administratorami a osobami, których dane dotyczą, w zakresie przetwarzania, bez uszczerbku dla praw osób, których dane dotyczą, na mocy art. 77 i 79.

3. Poza administratorami lub podmiotami przetwarzającymi, którzy podlegają niniejszemu rozporządzeniu, kodeksów postępowania zatwierdzonych na mocy ust. 5 niniejszego artykułu i powszechnie obowiązujących zgodnie z ust. 9 niniejszego artykułu, mogą przestrzegać także administratorzy lub podmioty przetwarzające, którzy zgodnie z art. 3 nie podlegają niniejszemu rozporządzeniu, w celu zapewnienia odpowiednich zabezpieczeń w ramach przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych na warunkach określonych w art. 46 ust. 2 lit. e). Tacy administratorzy lub takie podmioty przetwarzające podejmują wiążące i egzekwowalne zobowiązanie – w drodze umowy lub poprzez inne prawnie wiążące instrumenty – do stosowania tych odpowiednich zabezpieczeń, w tym w odniesieniu do praw osób, których dane dotyczą.

4. Kodeks postępowania, o którym mowa w ust. 2 niniejszego artykułu, przewiduje mechanizmy pozwalające podmiotowi, o którym mowa w art. 41 ust. 1, prowadzić obowiązkowe monitorowanie przestrzegania przepisów kodeksu przez administratorów lub podmioty przetwarzające, którzy podjęli się jego stosowania, bez uszczerbku dla zadań i uprawnień organów nadzorczych właściwych na mocy art. 55 lub 56.

5. Zrzeszenia i inne podmioty, o których mowa w ust. 2 niniejszego artykułu, chcące opracować kodeks postępowania lub zmienić lub rozszerzyć zakres kodeksu już obowiązującego przedkładają projekt kodeksu, zmiany lub rozszerzenia organowi nadzorczemu właściwemu na mocy art. 55. Organ nadzorczy wydaje opinię o zgodności projektu kodeksu, zmiany lub rozszerzenia z niniejszym rozporządzeniem i zatwierdza taki projekt kodeksu, zmiany lub rozszerzenia, jeżeli uzna, że stanowią one odpowiednie zabezpieczenia.

6. W przypadku zatwierdzenia zgodnie z ust. 5 projektu kodeksu, zmiany lub rozszerzenia, organ nadzorczy rejestruje i publikuje ten kodeks, o ile nie dotyczy on czynności przetwarzania prowadzonych w kilku państwach członkowskich.

7. Jeżeli projekt kodeksu postępowania dotyczy czynności przetwarzania prowadzonych w kilku państwach członkowskich, organ nadzorczy właściwy na mocy art. 55 przed zatwierdzeniem projektu kodeksu, zmiany lub rozszerzenia przedkłada go zgodnie z procedurą, o której mowa w art. 63, Europejskiej Radzie Ochrony Danych, która wydaje opinię o zgodności projektu kodeksu, zmiany lub rozszerzenia z niniejszym rozporządzeniem lub w sytuacji określonej w ust. 3 niniejszego artykułu opinię o tym, czy stanowią one odpowiednie zabezpieczenia.

8. Jeżeli opinia, o której mowa w ust. 7, potwierdza, że projekt kodeksu, zmiany lub rozszerzenia jest zgodny z niniejszym rozporządzeniem lub w sytuacji określonej w ust. 3 stanowią odpowiednie zabezpieczenia, Europejska Rada Ochrony Danych przedkłada tę opinię Komisji.

9. Komisja może, w drodze aktów wykonawczych, stwierdzić, że zatwierdzony kodeks postępowania, zmiana lub rozszerzenie przedłożone jej na mocy ust. 8 niniejszego artykułu są powszechnie obowiązujące w Unii. Te akty wykonawcze są przyjmowane zgodnie z procedurą sprawdzającą, o której mowa w art. 93 ust. 2.

10. Komisja zapewnia odpowiednie upowszechnianie zatwierdzonych kodeksów, których powszechne obowiązywanie stwierdziła zgodnie z ust. 9.

11. Europejska Rada Ochrony Danych gromadzi w rejestrze wszystkie zatwierdzone kodeksy podstępowania, zmiany i rozszerzenia i udostępnia je opinii publicznej za pomocą odpowiednich środków.

Artykuł 41

Monitorowanie zatwierdzonych kodeksów postępowania

1. Bez uszczerbku dla zadań i uprawnień właściwego organu nadzorczego wynikających z art. 57 i 58 monitorowaniem przestrzegania kodeksu postępowania na mocy art. 40 może się zajmować podmiot, który dysponuje odpowiednim poziomem wiedzy fachowej w dziedzinie będącej przedmiotem kodeksu i został akredytowany w tym celu przez właściwy organ nadzorczy.

2. Podmiot, o którym mowa w ust. 1, może zostać akredytowany w celu monitorowania przestrzegania kodeksu postępowania, jeżeli:

a) w sposób satysfakcjonujący wykazał on właściwemu organowi nadzorczemu swoją niezależność i wiedzę fachową w dziedzinie będącej przedmiotem kodeksu;

b) dysponuje procedurami, które pozwalają mu ocenić zdolność konkretnych administratorów i podmiotów przetwarzających do stosowania kodeksu, monitorować przestrzeganie przez nich jego przepisów oraz okresowo dokonywać przeglądu jego funkcjonowania;

c) dysponuje procedurami i strukturami, które pozwalają rozpatrywać skargi na naruszenie kodeksu przez administratora lub podmiot przetwarzający lub na sposób wdrożenia lub wdrażania kodeksu przez administratora lub podmiot przetwarzający oraz które pozwalają zapewnić przejrzystość tych procedur i struktur dla osób, których dane dotyczą, i opinii publicznej; oraz

d) w sposób satysfakcjonujący wykazał właściwemu organowi nadzorczemu, że jego zadania i obowiązki nie powodują konfliktu interesów.

3. Właściwy organ nadzorczy przedkłada proponowane kryteria akredytacji podmiotu, o którym mowa w ust. 1 niniejszego artykułu, Europejskiej Radzie Ochrony Danych zgodnie z mechanizmem spójności, o którym mowa w art. 63.

4. Bez uszczerbku dla zadań i uprawnień właściwego organu nadzorczego oraz przepisów rozdziału VIII podmiot, o którym mowa w ust. 1 niniejszego artykułu – z zastrzeżeniem odpowiednich zabezpieczeń – podejmuje odpowiednie działania w przypadku naruszenia kodeksu przez administratora lub podmiot przetwarzający, w tym zawiesza lub wyklucza administratora lub podmiot przetwarzający spośród stosujących kodeks. O działaniach tych i powodach ich podjęcia informuje on właściwy organ nadzorczy.

5. Właściwy organ nadzorczy cofa akredytację podmiotu, o którym mowa w ust. 1, jeżeli podmiot ten nie spełnia lub przestał spełniać warunki akredytacji lub jeżeli działania przez niego podejmowane nie są zgodne z niniejszym rozporządzeniem.

6. Niniejszy artykuł nie ma zastosowania do przetwarzania prowadzonego przez organy i podmioty publiczne.

Artykuł 42

Certyfikacja

1. Państwa członkowskie, organy nadzorcze, Europejska Rada Ochrony Danych oraz Komisja zachęcają – w szczególności na szczeblu Unii – do ustanawiania mechanizmów certyfikacji oraz znaków jakości i oznaczeń w zakresie ochrony danych osobowych mających świadczyć o zgodności z niniejszym rozporządzeniem operacji przetwarzania prowadzonych przez administratorów i podmioty przetwarzające. Przy tym uwzględnia się szczególne potrzeby mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw.

2. Mechanizmy certyfikacji oraz znaki jakości i oznaczenia w dziedzinie ochrony danych zatwierdzone na mocy ust. 5 niniejszego artykułu, które mają zastosowanie do administratorów lub podmiotów przetwarzających podlegających niniejszemu rozporządzeniu, mogą być ustanowione do wykazania odpowiednich zabezpieczeń przez administratorów lub podmioty przetwarzające, którzy zgodnie z art. 3 nie podlegają niniejszemu rozporządzeniu, w ramach przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych na warunkach określonych w art. 46 ust. 2 lit. f). Tacy administratorzy lub takie podmioty przetwarzające podejmują wiążące i egzekwowalne zobowiązania – w drodze umowy lub poprzez inne prawnie wiążące instrumenty – do stosowania tych odpowiednich zabezpieczeń, w tym w odniesieniu do praw osób, których dane dotyczą.

3. Certyfikacja jest dobrowolna, a proces jej uzyskania musi być przejrzysty.

4. Certyfikacja przewidziana w niniejszym artykule nie wpływa na spoczywający na administratorze lub podmiocie przetwarzającym obowiązek przestrzegania niniejszego rozporządzenia i pozostaje bez uszczerbku dla zadań i uprawnień organów nadzorczych właściwych na mocy art. 55 lub 56.

5. Certyfikacji przewidzianej w niniejszym artykule dokonują podmioty certyfikujące, o których mowa w art. 43, lub dokonuje jej właściwy organ nadzorczy – na podstawie kryteriów zatwierdzonych przez niego zgodnie z art. 58 ust. 3 lub przez Europejską Radę Ochrony Danych zgodnie z art. 63. W przypadku gdy kryteria są zatwierdzane przez Europejską Radę Ochrony Danych, może to skutkować wspólną certyfikacją, europejskim znakiem jakości ochrony danych.

6. Administrator lub podmiot przetwarzający, którzy poddają swoje przetwarzanie mechanizmowi certyfikacji, udzielają podmiotowi certyfikującemu, o którym mowa w art. 43, lub gdy ma to zastosowanie – właściwemu organowi nadzorczemu wszelkich informacji i wszelkiego dostępu do swoich czynności przetwarzania, które to informacje i dostęp są niezbędne do przeprowadzenia procedury certyfikacji.

7. Certyfikacji administratora lub podmiotu przetwarzającego udziela się na maksymalny okres 3 lat; certyfikację można przedłużyć na tych samych warunkach, o ile nadal spełnione są stosowne wymogi. W stosownym przypadku organy certyfikujące, o których mowa w art. 43, lub właściwy organ nadzorczy cofają certyfikację, jeżeli jej wymogi nie są spełnione lub przestały być spełniane.

8. Europejska Rada Ochrony Danych gromadzi w rejestrze wszystkie mechanizmy certyfikacji oraz znaki jakości i oznaczenia w dziedzinie ochrony danych i udostępnia je opinii publicznej za pomocą odpowiednich środków.

Artykuł 43

Podmiot certyfikujący

1. Bez uszczerbku dla zadań i uprawnień właściwego organu nadzorczego wynikających z art. 57 i 58 podmiot certyfikujący, który dysponuje odpowiednim poziomem wiedzy fachowej w dziedzinie ochrony danych dokonuje certyfikacji i jej przedłużenia po poinformowaniu organu nadzorczego w celu umożliwienia mu w razie potrzeby wykonywania uprawnień na mocy art. 58 ust. 2 lit. h) –. Państwa członkowskie zapewniają akredytację tych podmiotów certyfikujących przez:

a) organ nadzorczy właściwy zgodnie z art. 55 lub 56; lub

b) krajową jednostkę akredytującą określoną zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (WE) nr 765/2008 ([1]) – zgodnie z EN-ISO/IEC 17065/2012 – oraz zgodnie z dodatkowymi wymogami określonymi przez organ nadzorczy właściwy zgodnie z. 55 lub 56.

2. Podmioty certyfikujące, o których mowa w ust. 1, zostają akredytowane zgodnie z tym ustępem w przypadku gdy:

a) w sposób satysfakcjonujący wykazały właściwemu organowi nadzorczemu swoją niezależność i wiedzę fachową w dziedzinie podlegającej certyfikacji;

([1]) Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 765/2008 z dnia 9 lipca 2008 r. ustanawiające wymagania w zakresie akredytacji i nadzoru rynku odnoszące się do warunków wprowadzania produktów do obrotu i uchylające rozporządzenie (EWG) nr 339/93 (Dz.U. L 218 z 13.8.2008, s. 30).

b) zobowiązały się do przestrzegania kryteriów, o których mowa w art. 42 ust. 5 i które zostały zatwierdzone przez organ nadzorczy właściwy zgodnie z art. 55 lub 56 lub przez Europejską Radę Ochrony Danych zgodnie z art. 63;

c) dysponują procedurami wydawania, okresowego przeglądu i cofania certyfikacji, znaków jakości i oznaczeń w dziedzinie ochrony danych;

d) dysponują procedurami i strukturami, które pozwalają rozpatrywać skargi na naruszenie warunków certyfikacji przez administratora lub podmiot przetwarzający lub na sposób wdrożenia lub wdrażania certyfikacji przez administratora lub podmiot przetwarzający, oraz które zapewniają przejrzystość tych procedur i struktur dla osób, których dane dotyczą, i opinii publicznej; oraz

e) w sposób satysfakcjonujący wykażą właściwemu organowi nadzorczemu, że ich zadania i obowiązki nie powodują konfliktu interesów.

3. Akredytacja podmiotów certyfikujących, o których mowa w ust. 1 i 2 niniejszego artykułu, jest dokonywana na podstawie kryteriów zatwierdzonych przez organ nadzorczy właściwy zgodnie z art. 55 lub 56 lub przez Europejską Radę Ochrony Danych zgodnie z art. 63. W przypadku akredytacji na mocy ust. 1 lit. c) niniejszego artykułu wymogi te są uzupełnieniem wymogów przewidzianych w rozporządzeniu (WE) nr 765/2008 oraz przepisów technicznych określających metody i procedury podmiotów certyfikujących.

4. Podmioty certyfikujące, o których mowa w ust. 1, są odpowiedzialne za dokonanie właściwej oceny przed udzieleniem lub cofnięciem certyfikacji, bez uszczerbku dla spoczywającego na administratorze lub podmiocie przetwarzającym obowiązku przestrzegania niniejszego rozporządzenia. Akredytacji udziela się na maksymalny okres pięciu lat; można ją przedłużyć na tych samych warunkach, o ile podmiot certyfikujący spełnia wymogi określone w niniejszym artykule.

5. Podmioty certyfikujące, o których mowa w ust. 1, przedstawiają właściwemu organowi nadzorczemu powody udzielenia lub cofnięcia żądanej certyfikacji.

6. Organ nadzorczy w łatwo dostępny sposób podaje do wiadomości publicznej wymogi, o których mowa w ust. 3 niniejszego artykułu, oraz kryteria, o których mowa w art. 42 ust. 5. Organy nadzorcze przekazują te wymogi i kryteria także Europejskiej Radzie Ochrony Danych. Gromadzi ona w rejestrze wszystkie mechanizmy certyfikacji oraz znaki jakości w dziedzinie ochrony danych i udostępnia je opinii publicznej za pomocą odpowiednich środków.

7. Bez uszczerbku dla rozdziału VIII właściwy organ nadzorczy lub krajowa jednostka akredytująca cofają akredytację podmiotu certyfikującego zgodnie z ust. 1 niniejszego artykułu, w przypadku gdy podmiot ten nie spełnia lub przestał spełniać warunki akredytacji lub jeżeli działania podejmowane przez podmiot certyfikujący naruszają niniejsze rozporządzenie.

8. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 92 w celu doprecyzowania wymogów, które uwzględnia się w przypadku mechanizmów certyfikacji w dziedzinie ochrony danych, o których mowa w art. 42 ust. 1.

9. Komisja może przyjąć akty wykonawcze określające techniczne standardy mechanizmów certyfikacji oraz znaków jakości i oznaczeń w dziedzinie ochrony danych, a także sposoby upowszechniania i uznawania tych mechanizmów certyfikacji oraz znaków jakości i oznaczeń. Te akty wykonawcze są przyjmowane zgodnie z procedurą sprawdzającą, o której mowa w art. 93 ust. 2.

ROZDZIAŁ V

Przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych

Artykuł 44

Ogólna zasada przekazywania

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

Artykuł 45

Przekazywanie na podstawie decyzji stwierdzającej odpowiedni stopień ochrony

1. Przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej może nastąpić, gdy Komisja stwierdzi, że to państwo trzecie, terytorium lub określony sektor lub określone sektory 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 ustawodawstwo – 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 ustawodawstwa, 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 lub w organizacji międzynarodowej, orzecznictwo, a także istnienie skutecznych i egzekwowalnych praw osób, których dane dotyczą, oraz prawa osób, których dane dotyczą, których dane osobowe są przekazywane, do skutecznych administracyjnych i sądowych środków zaskarżenia;

b) istnienie i skuteczne działanie co najmniej jednego niezależnego organu nadzorczego w państwie trzecim lub w stosunku do organizacji międzynarodowej, 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 zaciągnięte przez dane państwo trzecie lub daną organizację międzynarodową lub inne obowiązki wynikające z prawnie wiążących konwencji lub instrumentów oraz z udziału w systemach wielostronnych lub regionalnych, w szczególności w dziedzinie ochrony danych osobowych.

3. Po dokonaniu oceny, czy stopień ochrony jest odpowiedni, Komisja może w drodze aktu wykonawczego przyjąć decyzję stwierdzającą, że państwo trzecie, terytorium lub określony sektor lub określone sektory w tym 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 gdy ma to zastosowanie 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. 93 ust. 2.

4. Komisja na bieżąco monitoruje zmiany w państwach trzecich i organizacjach międzynarodowych mogące wpłynąć na obowiązywanie decyzji przyjętych na mocy ust. 3 niniejszego artykułu oraz decyzji przyjętych na podstawie art. 25 ust. 6 dyrektywy 95/46/WE.

5. Jeżeli dostępne informacje na to wskazują, w szczególności po przeglądzie, o którym mowa w ust. 3 niniejszego artykułu, Komisja przyjmuje decyzję stwierdzającą, że państwo trzecie – lub terytorium lub jeden lub więcej określonych sektorów w tym 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. Te akty wykonawcze są przyjmowane zgodnie z procedurą sprawdzającą, o której mowa w art. 93 ust. 2.

W należycie uzasadnionych, szczególnie pilnych przypadkach Komisja przyjmuje zgodnie z procedurą, o której mowa w art. 93 ust. 3 akty wykonawcze mające natychmiastowe zastosowanie.

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

7. Decyzja przyjęta na mocy ust. 5 niniejszego artykułu pozostaje bez uszczerbku dla przekazywania danych osobowych do danego państwa trzeciego, terytorium lub określonego sektora lub określonych sektorów w tym państwie trzecim lub do danej organizacji międzynarodowej na mocy art. 46–49.

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

9. Decyzje przyjęte przez Komisję na mocy art. 25 ust. 6 dyrektywy 95/46/WE pozostają w mocy do czasu ich zmiany, zastąpienia lub uchylenia decyzją Komisji przyjętą zgodnie z ust. 3 lub 5 niniejszego artykułu.

Artykuł 46

Przekazywanie z zastrzeżeniem odpowiednich zabezpieczeń

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

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

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

b) wiążących reguł korporacyjnych zgodnie z art. 47;

c) standardowych klauzul ochrony danych przyjętych przez Komisję zgodnie z procedurą sprawdzającą, o której mowa w art. 93 ust. 2;

d) standardowych klauzul ochrony danych przyjętych przez organ nadzorczy i zatwierdzonych przez Komisję zgodnie z procedurą sprawdzającą, o której mowa w art. 93 ust. 2;

e) zatwierdzonego kodeksu postępowania zgodnie z art. 40 wraz z wiążącymi i egzekwowalnymi zobowiązaniami administratora lub podmiotu przetwarzającego w państwie trzecim do stosowania odpowiednich zabezpieczeń, w tym w odniesieniu do praw osób, których dane dotyczą; lub

f) zatwierdzonego mechanizmu certyfikacji zgodnie z art. 42 wraz z wiążącymi i egzekwowalnymi zobowiązaniami administratora lub podmiotu przetwarzającego w państwie trzecim do stosowania odpowiednich zabezpieczeń, w tym w odniesieniu do praw osób, których dane dotyczą.

3. Z zastrzeżeniem zezwolenia właściwego organu nadzorczego odpowiednie zabezpieczenia, o których mowa w ust. 1, można także zapewnić w szczególności za pomocą:

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

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

4. W przypadkach, o których mowa w ust. 3 niniejszego artykułu, organ nadzorczy stosuje mechanizm spójności, o którym mowa w art. 63.

5. Zezwolenia wydane przez państwo członkowskie lub organ nadzorczy na podstawie art. 26 ust. 2 dyrektywy 95/46/WE zachowują ważność do czasu ich zmiany, zastąpienia lub uchylenia w razie potrzeby przez ten organ. Decyzje przyjęte przez Komisję na mocy art. 26 ust. 4 dyrektywy 95/46/WE pozostają w mocy do czasu ich zmiany, zastąpienia lub uchylenia w razie potrzeby decyzją Komisji przyjętą zgodnie z ust. 2 niniejszego artykułu.

Artykuł 47

wiążące reguły korporacyjnych

1. Właściwy organ nadzorczy zatwierdza wiążące reguły korporacyjne zgodnie z mechanizmem spójności przewidzianym w art. 63, pod warunkiem że:

a) są one prawnie wiążące oraz mają zastosowanie do każdego z członków grupy przedsiębiorstw lub grupy przedsiębiorców prowadzących wspólną działalność gospodarczą, w tym ich pracowników, i są przez każdego z tych członków egzekwowane;

b) wyraźnie przyznają osobom, których dane dotyczą, egzekwowalne prawa w związku z przetwarzaniem ich danych osobowych; oraz

c) spełniają wymogi określone w ust. 2.

2. W wiążących regułach korporacyjnych, o których mowa w ust. 1, określone zostają co najmniej:

a) struktura i dane kontaktowe odnośnej grupy przedsiębiorstw lub grupy przedsiębiorców prowadzących wspólną działalność gospodarczą i każdego z jej członków;

b) jednorazowe lub wielokrotne przekazanie danych, w tym kategorie danych osobowych, rodzaj przetwarzania i jego cele, rodzaje osób, których dane dotyczą, oraz nazwa danego państwa trzeciego lub danych państw trzecich;

c) ich prawnie wiążący charakter, wewnętrzny i zewnętrzny;

d) zastosowanie ogólnych zasad ochrony danych – w szczególności ograniczenia celu, minimalizacji danych, ograniczonych okresów przechowywania, jakości danych, uwzględnianie ochrony danych w fazie projektowania oraz domyślnej ochrony danych, podstawa prawna przetwarzania, przetwarzanie szczególnych kategorii danych osobowych, środki zapewniające bezpieczeństwo danych, wymogi w zakresie dalszego przekazywania podmiotom niezwiązanym wiążącymi regułami korporacyjnymi;

e) prawa osób, których dane dotyczą, w związku z przetwarzaniem oraz sposoby wykonywania tych praw, w tym z prawa do niepodlegania decyzjom opartym wyłącznie na zautomatyzowanym przetwarzaniu – w tym profilowaniu – zgodnie z art. 22, prawa do wnoszenia skarg do właściwego organu nadzorczego i właściwych sądów państw członkowskich zgodnie z art. 79 oraz prawa do środka zaskarżenia, a w stosownych przypadkach – odszkodowania za naruszenie wiążących reguł korporacyjnych;

f) przyjęcie przez administratora lub podmiot przetwarzający posiadających jednostki organizacyjnej na terytorium państwa członkowskiego odpowiedzialności prawnej za naruszenie wiążących reguł korporacyjnych przez odnośnego członka niemającego jednostki organizacyjne w Unii; administrator lub podmiot przetwarzający są zwolnieni z tej odpowiedzialności – w całości lub w części – wyłącznie, gdy udowodni, że członek ten nie ponosi odpowiedzialności za wydarzenie, które doprowadziło do powstania szkody;

g) sposób, w jaki osobom, których dane dotyczą, podaje się – oprócz informacji, o których mowa w art. 13 i 14 – informacje o wiążących regułach korporacyjnych, w szczególności o postanowieniach, o których mowa w lit. d), e) i f) niniejszego ustępu;

h) zadania inspektora ochrony danych wyznaczonego zgodnie z art. 37 lub innej osoby lub podmiotu odpowiedzialnych za monitorowanie przestrzegania wiążących reguł korporacyjnych w ramach grupy przedsiębiorstw lub grupy przedsiębiorców prowadzących wspólną działalność gospodarczą oraz monitorowanie szkoleń i rozpatrywanie skarg;

i) procedury dotyczące skarg;

j) stosowane w grupie przedsiębiorstw lub w grupie przedsiębiorców prowadzących wspólną działalność gospodarczą mechanizmy zapewniające weryfikację przestrzegania wiążących reguł korporacyjnych. Mechanizmy takie obejmują audyty w zakresie ochrony danych oraz metody zapewniania działań naprawczych mających chronić prawa osób, których dane dotyczą. Wyniki takiej weryfikacji powinny być przekazywane osobie lub podmiotowi, o których mowa w lit. h), oraz zarządowi przedsiębiorstwa sprawującego kontrolę w grupie przedsiębiorstw lub organowi kierującemu grupą przedsiębiorców prowadzących wspólną działalność gospodarczą i powinny być dostępne na żądanie właściwego organu nadzorczego;

k) mechanizmy zgłaszania i rejestrowania zmian w zasadach i zgłaszania tych zmian organowi nadzorczemu;

l) mechanizm współpracy z organem nadzorczym zapewniający przestrzeganie zasad przez wszystkich członków grupy przedsiębiorstw lub grupy przedsiębiorców prowadzących wspólną działalność gospodarczą, w szczególności poprzez udostępnianie organowi nadzorczemu wyników weryfikacji środków, o której mowa w lit. j);

m) mechanizm zgłaszania właściwemu organowi nadzorczemu wszelkich wymogów prawnych, którym podlega w państwie trzecim członek grupy przedsiębiorstw lub grupy przedsiębiorców prowadzących wspólną działalność gospodarczą i które mogą mieć istotny niekorzystny wpływ na gwarancje przewidziane w wiążących regułach korporacyjnych; oraz

n) właściwe szkolenia z zakresu ochrony danych dla personelu mającego stały lub regularny dostęp do danych osobowych.

3. Komisja może określić format i procedury wymiany informacji między administratorami, podmiotami przetwarzającymi i organami nadzorczymi dotyczących wiążących reguł korporacyjnych w rozumieniu niniejszego artykułu. Te akty wykonawcze są przyjmowane zgodnie z procedurą sprawdzającą, o której mowa w art. 93 ust. 2.

Artykuł 48

Przekazywanie lub ujawnianie niedozwolone na mocy prawa Unii

Wyrok sądu lub trybunału oraz decyzja organu administracyjnego państwa trzeciego wymagające od administratora lub podmiotu przetwarzającego przekazania lub ujawnienia danych osobowych mogą zostać uznane lub być egzekwowalne wyłącznie, gdy opierają się na umowie międzynarodowej, takiej jak umowa o wzajemnej pomocy prawnej, obowiązującej między wzywającym państwem trzecim a Unią lub państwem członkowskim, bez uszczerbku dla innych podstaw przekazania na mocy niniejszego rozdziału.

Artykuł 49

Wyjątki w szczególnych sytuacjach

1. W razie braku decyzji stwierdzającej odpowiedni stopień ochrony określonej w art. 45 ust. 3 lub braku odpowiednich zabezpieczeń określonych w art. 46, w tym wiążących reguł korporacyjnych, jednorazowe lub wielokrotne przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej mogą nastąpić wyłącznie pod warunkiem, że:

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

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

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

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

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

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

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

Jeżeli przekazanie nie może się opierać na art. 45 ani 46, w tym na przepisach dotyczących wiążących reguł korporacyjnych, i nie ma zastosowania żaden z wyjątków mających zastosowanie w szczególnych sytuacjach zgodnie z akapitem pierwszym niniejszego ustępu, przekazanie do państwa trzeciego lub organizacji międzynarodowej może nastąpić wyłącznie, gdy przekazanie nie jest powtarzalne, dotyczy tylko ograniczonej liczby osób, których dane dotyczą, jest niezbędne ze względu na ważne prawnie uzasadnione interesy realizowane przez administratora, wobec których charakteru nadrzędnego nie mają interesy ani prawa i wolności osoby, której dane dotyczą a administrator ocenił wszystkie okoliczności przekazania danych i na podstawie tej oceny zapewnił odpowiednie zabezpieczenia w zakresie ochrony danych osobowych. Administrator informuje organ nadzorczy o przekazaniu. Poza informacjami, o których mowa w art. 13 i 14, administrator podaje osobie, której dane dotyczą, także informacje o przekazaniu i o ważnych prawnie uzasadnionych interesach realizowanych przez niego.

2. Przekazanie na mocy ust. 1 akapit pierwszy lit. g) nie obejmuje całości danych osobowych ani całych kategorii danych osobowych zawartych w rejestrze. Jeżeli rejestr jest dostępny dla osób mających prawnie uzasadniony interes, przekazanie następuje wyłącznie na żądanie tych osób lub gdy mają one być odbiorcami.

3. Ust. 1 akapit pierwszy lit. a), b), c) oraz ust. 1 akapit drugi tego ustepu nie mają zastosowania do działalności prowadzonej przez organy publiczne w ramach wykonywania przysługujących im uprawnień publicznych.

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

5. W razie braku decyzji stwierdzającej odpowiedni stopień ochrony prawo Unii lub prawo państwa członkowskiego może z uwagi na ważne względy interesu publicznego wyraźnie nakładać ograniczenia na przekazywanie konkretnych kategorii danych osobowych do państwa trzeciego lub organizacji międzynarodowej. Państwa członkowskie powiadamiają Komisję o takich przepisach.

6. Administrator lub podmiot przetwarzający dokumentują ocenę oraz odpowiednie zabezpieczenia, o których mowa w ust. 1 akapit drugi niniejszego artykułu, w rejestrach, o których mowa w art. 30.

Artykuł 50

Międzynarodowa współpraca na rzecz ochrony danych osobowych

Komisja i organy nadzorcze 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 postępowaniu wyjaśniającym oraz wymianę informacji – z zastrzeżeniem odpowiednich zabezpieczeń ochrony danych osobowych i innych podstawowych praw i wolności;

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

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

ROZDZIAŁ VI

Niezależne organy nadzorcze

Sekcja 1

Niezależny status

Artykuł 51

Organ nadzorczy

1. Każde państwo członkowskie zapewnia, by za monitorowanie stosowania niniejszego rozporządzenia odpowiadał co najmniej jeden niezależny organ publiczny w celu ochrony podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem oraz ułatwiania swobodnego przepływu danych osobowych w Unii (zwany dalej „organem nadzorczym").

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

3. Jeżeli w państwie członkowskim ustanowiono więcej niż jeden organ nadzorczy, państwo to wskazuje, który z nich ma reprezentować te organy w Europejskiej Radzie Ochrony Danych, oraz ustala mechanizm zapewniający przestrzeganie przez pozostałe organy przepisów o mechanizmie spójności, o którym mowa w art. 63.

4. Do dnia 25 maja 2018 r. każde państwo członkowskie zawiadamia Komisję o przepisach przyjętych na mocy niniejszego rozdziału, a następnie niezwłocznie o każdej kolejnej zmianie mającej na nie wpływ.

Artykuł 52

Niezależność

1. Każdy organ nadzorczy podczas wypełniania swoich zadań i wykonywania swoich uprawnień zgodnie z niniejszym rozporządzeniem działa w sposób w pełni niezależny.

2. Członek lub członkowie każdego organu nadzorczego podczas wypełniania swoich zadań i wykonywania swoich uprawnień zgodnie z niniejszym rozporządzeniem pozostają wolni od bezpośrednich i pośrednich wpływów zewnętrznych, nie zwracają się do nikogo o instrukcje ani ich od nikogo nie przyjmują.

3. Członek lub członkowie każdego organu nadzorczego 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. Każde państwo członkowskie zapewnia, by każdy organ nadzorczy dysponował zasobami kadrowymi, technicznymi i finansowymi, pomieszczeniami i infrastrukturą niezbędnymi do skutecznego wypełniania swoich zadań i wykonywania swoich uprawnień, w tym w zakresie wzajemnej pomocy, współpracy i uczestnictwa w pracach Europejskiej Rady Ochrony Danych.

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

6. Każde państwo członkowskie zapewnia, by każdy organ nadzorczy podlegał kontroli finansowej w sposób nienaruszający jego niezależności oraz dysponował odrębnym, publicznym budżetem rocznym, który może być częścią ogólnego budżetu państwowego lub krajowego.

Artykuł 53

Ogólne warunki dotyczące członków organu nadzorczego

1. Państwa członkowskie zapewniają, by każdy członek ich organów nadzorczych był powoływany w drodze przejrzystej procedury przez:

— ich parlament,

— ich rząd,

— ich głowę państwa, lub

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

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 może zostać odwołany ze stanowiska tylko w przypadku, gdy dopuścił się poważnego uchybienia lub przestał spełniać warunki niezbędne do pełnienia obowiązków.

Artykuł 54

Zasady ustanawiania organu nadzorczego

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

a) ustanowienie każdego z organów nadzorczych;

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

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

d) okres kadencji członka lub członków każdego z organów nadzorczych – nie krótszy niż cztery lata, z wyjątkiem pierwszej kadencji po dniu 24 maja 2016 r., która może częściowo trwać krócej, jeżeli jest to niezbędne, aby chronić niezależność organu nadzorczego w drodze procedury stopniowej wymiany członków;

e) czy członek lub członkowie każdego z organów nadzorczych mogą zostać powołani ponownie, a jeżeli tak – na ile kadencji;

f) zasady regulujące obowiązki członka lub członków oraz personelu każdego z organów nadzorczych, zakaz podejmowania działań, zajęć i czerpania korzyści – w trakcie kadencji oraz po jej zakończeniu – sprzecznych z tymi zobowiązaniami, 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 zachowania 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 zachowania tajemnicy służbowej w trakcie ich kadencji dotyczy w szczególności sytuacji, w których osoby fizyczne zgłaszają naruszenia niniejszego rozporządzenia.

Sekcja 2

Właściwość, zadania i uprawnienia

Artykuł 55

Właściwość

1. Każdy organ nadzorczy jest właściwy do wypełniania zadań i wykonywania uprawnień powierzonych mu zgodnie z niniejszym rozporządzeniem na terytorium swojego państwa członkowskiego.

2. Jeżeli przetwarzania dokonują organy publiczne lub podmioty prywatne działające na podstawie art. 6 ust. 1 lit. c) lub e), organem właściwym jest organ nadzorczy danego państwa członkowskiego. W takich przypadkach art. 56 nie ma zastosowania.

3. Organy nadzorcze nie są właściwe do nadzorowania operacji przetwarzania dokonywanych przez sądy w ramach sprawowania przez nie wymiaru sprawiedliwości.

Artykuł 56

Właściwość wiodącego organu nadzorczego

1. Bez uszczerbku dla art. 55 organ nadzorczy głównej lub pojedynczej jednostki organizacyjnej administratora lub podmiotu przetwarzającego jest właściwy do podejmowania działań jako wiodący organ nadzorczy – zgodnie z procedurą przewidzianą w art. 60 – względem transgranicznego przetwarzania dokonywanego przez tego administratora lub ten podmiot przetwarzający.

2. W drodze wyjątku od ust. 1 każdy organ nadzorczy jest właściwy do rozpatrzenia skargi, którą do niego wniesiono, lub zajęcia się ewentualnym naruszeniem niniejszego rozporządzenia, jeżeli sprawa dotyczy wyłącznie jednostki organizacyjnej w jego państwie członkowskim lub znacznie wpływa na osoby, których dane dotyczą, wyłącznie w jego państwie członkowskim.

3. W przypadkach, o których mowa w ust. 2 niniejszego artykułu, organ nadzorczy niezwłocznie informuje o danej sprawie wiodący organ nadzorczy. W terminie trzech tygodni od otrzymania informacji wiodący organ nadzorczy postanawia, czy zajmie się daną sprawą zgodnie z procedurą przewidzianą w art. 60, uwzględniając, czy w państwie członkowskim, którego organ nadzorczy przekazał mu informacje, znajduje się jednostka organizacyjna administratora lub podmiotu przetwarzającego.

4. Jeżeli wiodący organ nadzorczy postanowi zająć się daną sprawą, zastosowanie ma procedura przewidziana w art. 60. Organ nadzorczy, który przekazał informacje wiodącemu organowi nadzorczemu, może przedłożyć temu organowi projekt decyzji. Wiodący organ nadzorczy w jak największym stopniu uwzględnia ten projekt, przygotowując projekt decyzji, o którym mowa w art. 60 ust. 3.

5. Jeżeli wiodący organ nadzorczy postanowi nie zajmować się daną sprawą, sprawą zajmuje się – zgodnie z art. 61 i 62 – organ nadzorczy, który przekazał informacje wiodącemu organowi nadzorczemu.

6. Administrator lub podmiot przetwarzający komunikują się w sprawie dokonywanego przez nich transgranicznego przetwarzania jedynie z wiodącym organem nadzorczym.

Artykuł 57

Zadania

1. Bez uszczerbku dla innych zadań określonych na mocy niniejszego rozporządzenia każdy organ nadzorczy na swoim terytorium:

a) monitoruje i egzekwuje stosowanie niniejszego rozporządzenia;

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

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

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

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

f) rozpatruje skargi wniesione przez osobę, której dane dotyczą, lub przez podmiot, organizację lub zrzeszenie zgodnie z art. 80, w odpowiednim zakresie prowadzi postępowania w przedmiocie tych skarg i w rozsądnym terminie informuje skarżącego o postępach i wynikach tych postępowań, w szczególności jeżeli niezbędne jest dalsze prowadzenie postępowań lub koordynacja działań z innym organem nadzorczym;

g) współpracuje z innymi organami nadzorczymi, w tym dzieli się informacjami oraz świadczy wzajemną pomoc, w celu zapewnienia spójnego stosowania i egzekwowania niniejszego rozporządzenia;

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

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

j) przyjmuje standardowe klauzule umowne, o których mowa w art. 28 ust. 8 i art. 46 ust. 2 lit. d);

k) ustanawia i prowadzi wykaz związany z wymogiem dokonania oceny skutków dla ochrony danych na mocy art. 35 ust. 4;

l) udziela zaleceń, o których mowa w art. 36 ust. 2, dotyczących operacji przetwarzania;

m) zachęca do sporządzania kodeksów postępowania zgodnie z art. 40 ust. 1, wydaje opinie na ich temat oraz zatwierdza te kodeksy, w których znajdują się odpowiednie zabezpieczenia, na mocy art. 40 ust. 5;

n) zachęca do ustanawiania mechanizmów certyfikacji w dziedzinie ochrony danych oraz znaków jakości i oznaczeń z tej dziedziny zgodnie z art. 42 ust. 1, a także zatwierdza kryteria certyfikacji zgodnie z art. 42 ust. 5;

o) gdy ma to zastosowanie – zgodnie z art. 42 ust. 7 dokonuje okresowego przeglądu udzielonych certyfikacji;

p) opracowuje i publikuje kryteria akredytacji podmiotu monitorującego kodeksy postępowania na mocy art. 41 oraz podmiotu certyfikującego na mocy art. 43;

q) akredytuje podmiot monitorujący kodeksy postępowania na mocy art. 41 oraz podmiot certyfikujący na mocy art. 43;

r) wydaje zezwolenia na klauzule umowne i przepisy, o których mowa w art. 46 ust. 3;

s) zatwierdza wiążące reguły korporacyjne na mocy art. 47;

t) bierze udział w pracach Europejskiej Rady Ochrony Danych;

u) prowadzi wewnętrzny rejestr naruszeń niniejszego rozporządzenia i działań podjętych zgodnie z art. 58 ust. 2; oraz

v) wypełnia inne zadania związane z ochroną danych osobowych.

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 również wypełnić elektronicznie, co nie wyklucza innych sposobów komunikacji.

3. Każdy organ nadzorczy wypełnia zadania na rzecz osoby, której dane dotyczą, i – gdy ma to zastosowanie – inspektora ochrony danych bezpłatnie.

4. Jeżeli żądanie jest w sposób oczywisty nieuzasadnione lub nadmierne, w szczególności ze względu na swą powtarzalność, organ nadzorczy może pobrać opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych lub może odmówić podjęcia żądanych działań. Obowiązek wykazania, że żądanie jest w sposób oczywisty nieuzasadnione lub nadmierne, spoczywa na organie nadzorczym.

Artykuł 58

Uprawnienia

1. Każdemu organowi nadzorczemu przysługują wszystkie następujące uprawnienia w zakresie prowadzonych postępowań:

a) nakazanie administratorowi i podmiotowi przetwarzającemu, a w stosownym przypadku przedstawicielowi administratora lub podmiotu przetwarzającego, dostarczenia wszelkich informacji potrzebnych organowi nadzorczemu do realizacji swoich zadań;

b) prowadzenie postępowań w formie audytów ochrony danych;

c) dokonywanie przeglądu udzielonych certyfikacji na mocy art. 42 ust. 7;

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

e) uzyskiwanie od administratora i podmiotu przetwarzającego dostępu do wszelkich danych osobowych i wszelkich informacji niezbędnych organowi nadzorczemu do realizacji swoich zadań;

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

2. Każdemu organowi nadzorczemu przysługują wszystkie następujące uprawnienia naprawcze:

a) wydawanie ostrzeżeń administratorowi lub podmiotowi przetwarzającemu dotyczących możliwości naruszenia przepisów niniejszego rozporządzenia poprzez planowane operacje przetwarzania;

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

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

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

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

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

g) nakazanie na mocy art. 16, 17 i 18 sprostowania lub usunięcia danych osobowych lub ograniczenia ich przetwarzania oraz nakazanie na mocy art. 17 ust. 2 i art. 19 powiadomienia o tych czynnościach odbiorców, którym dane osobowe ujawniono;

h) cofnięcie certyfikacji lub nakazanie podmiotowi certyfikującemu cofnięcia certyfikacji udzielonej na mocy art. 42 lub 43, lub nakazanie podmiotowi certyfikującemu nieudzielania certyfikacji, jeżeli jej wymogi nie są spełnione lub przestały być spełniane;

i) zastosowanie, oprócz lub zamiast środków, o których mowa w niniejszym ustępie, administracyjnej kary pieniężnej na mocy art. 83, zależnie od okoliczności konkretnej sprawy;

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

3. Każdemu organowi nadzorczemu przysługują wszystkie następujące uprawnienia w zakresie wydawania zezwoleń i uprawnienia doradcze:

a) udzielanie porad administratorowi zgodnie z procedurą uprzednich konsultacji, o której mowa w art. 36;

b) wydawanie, z własnej inicjatywy lub na wniosek, opinii przeznaczonych dla parlamentu narodowego, rządu państwa członkowskiego lub – zgodnie z prawem państwa członkowskiego – innych instytucji i organów oraz ogółu społeczeństwa we wszelkich sprawach związanych z ochroną danych osobowych;

c) zezwalanie na przetwarzanie zgodnie z art. 36 ust. 5, jeżeli prawo państwa członkowskiego wymaga takiego uprzedniego zezwolenia;

d) opiniowanie i zatwierdzanie projektów kodeksów postępowania zgodnie z art. 40 ust. 5;

e) akredytowanie na mocy art. 43 podmiotów certyfikujących;

f) udzielanie certyfikacji i zatwierdzanie kryteriów certyfikacji zgodnie z art. 42 ust. 5;

g) przyjmowanie standardowych klauzul ochrony danych, o których mowa w art. 28 ust. 8 i art. 46 ust. 2 lit. d);

h) zezwalanie na klauzule umowne, o których mowa w art. 46 ust. 3 lit. a);

i) zezwalanie na uzgodnienia administracyjne, o których mowa w art. 46 ust. 3 lit. b);

j) zatwierdzanie wiążących reguł korporacyjnych na mocy art. 47.

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

5. Każde państwo członkowskie przewiduje w swoich przepisach, że jego organ nadzorczy jest uprawniony do wniesienia do organów wymiaru sprawiedliwości sprawy dotyczącej naruszenia niniejszego rozporządzenia oraz w stosownych przypadkach do wszczęcia lub do uczestniczenia w inny sposób w postępowaniu sądowym w celu wyegzekwowania stosowania przepisów niniejszego rozporządzenia.

6. Każde państwo członkowskie może przewidzieć w swoich przepisach, że jego organowi nadzorczemu przysługują poza uprawnieniami określonymi w ust. 1, 2 i 3 także inne uprawnienia. Wykonywanie tych uprawnień nie może utrudniać skutecznego stosowania przepisów rozdziału VII.

Artykuł 59

Sprawozdanie z działalności

Każdy organ nadzorczy sporządza roczne sprawozdanie ze swojej działalności, w którym może wyszczególnić rodzaje zgłoszonych mu naruszeń i rodzaje środków podjętych zgodnie z art. 58 ust. 2. Sprawozdania te są przekazywane parlamentowi narodowemu, rządowi i innym organom wskazanym prawem państwa członkowskiego. Są one udostępniane opinii publicznej, Komisji oraz Europejskiej Radzie Ochrony Danych.

ROZDZIAŁ VII

Współpraca i spójność

Sekcja 1

Współpraca

Artykuł 60

Współpraca miedzy wiodącym organem nadzorczym a innymi organami nadzorczymi, których sprawa dotyczy

1. Wiodący organ nadzorczy współpracuje z innymi organami nadzorczymi, których sprawa dotyczy, zgodnie z niniejszym artykułem w celu osiągnięcia porozumienia. Wiodący organ nadzorczy i organy nadzorcze, których sprawa dotyczy, wymieniają się wszelkimi stosownymi informacjami.

2. Wiodący organ nadzorczy może w dowolnym momencie zwrócić się do innych organów nadzorczych, których sprawa dotyczy, o wzajemną pomoc zgodnie z art. 61 i może prowadzić wspólne operacje zgodnie z art. 62, w szczególności w celu przeprowadzenia postępowania lub monitorowania wdrażania środka dotyczącego administratora lub podmiotu przetwarzającego posiadającego jednostkę organizacyjną w innym państwie członkowskim.

3. Wiodący organ nadzorczy niezwłocznie przekazuje innym organom nadzorczym, których sprawa dotyczy, stosowne informacje dotyczące danej sprawy. Niezwłocznie przedkłada innym organom, których sprawa dotyczy, nadzorczym projekt decyzji w celu uzyskania ich opinii i należytego uwzględnienia ich uwag.

4. Jeżeli w terminie czterech tygodni od otrzymania wniosku o opinię zgodnie z ust. 3 niniejszego artykułu inny organ nadzorczy, którego sprawa dotyczy, zgłosi mający znaczenie dla sprawy i uzasadniony sprzeciw wobec projektu decyzji, wiodący organ nadzorczy – jeżeli nie przychyla się do mającego znaczenie dla sprawy i uzasadnionego sprzeciwu lub sądzi, że sprzeciw nie ma znaczenia dla sprawy lub nie jest uzasadniony –przekazuje sprawę w ramach mechanizmu spójności, o którym mowa w art. 63.

5. Jeżeli wiodący organ nadzorczy zamierza przychylić się do zgłoszonego mającego znaczenie dla sprawy i uzasadnionego sprzeciwu, przedkłada innym organom nadzorczym, których sprawa dotyczy, zmieniony projekt decyzji w celu uzyskania ich opinii. Zmieniony projekt decyzji jest poddawany procedurze, o której mowa w ust. 4, w terminie dwóch tygodni.

6. Jeżeli w terminie, o którym mowa w ust. 4 i 5, żaden inny organ nadzorczy, którego sprawa dotyczy, nie zgłosi sprzeciwu wobec projektu decyzji przedłożonego przez wiodący organ nadzorczy, uznaje się, że wiodący organ nadzorczy i organy nadzorcze, których sprawa dotyczy, porozumiały się w sprawie projektu decyzji i są nią związane.

7. Wiodący organ nadzorczy przyjmuje decyzję i doręcza ją odpowiednio głównej lub pojedynczej jednostce organizacyjnej administratora lub podmiotu przetwarzającego oraz informuje o decyzji inne organy nadzorcze, których sprawa dotyczy, i Europejską Radę Ochrony Danych, dołączając streszczenie stanu faktycznego i powodów decyzji. Organ nadzorczy, do którego wniesiono skargę, informuje skarżącego o decyzji.

8. W drodze wyjątku od ust. 7, jeżeli skarga zostaje oddalona lub odrzucona, organ nadzorczy, do którego wniesiono skargę, przyjmuje decyzję i doręcza ją skarżącemu oraz informuje o niej administratora.

9. Jeżeli wiodący organ nadzorczy i organy nadzorcze, których sprawa dotyczy, porozumiały się co do oddalenia lub odrzucenia części skargi oraz co do podjęcia działań względem innych części tej skargi, dla każdej z tych części przyjmuje się odrębną decyzję. Wiodący organ nadzorczy przyjmuje decyzję w sprawie części dotyczącej działań względem administratora i doręcza ją głównej lub pojedynczej jednostce organizacyjnej administratora lub podmiotu przetwarzającego na terytorium swojego państwa członkowskiego i informuje o niej skarżącego, a organ nadzorczy skarżącego przyjmuje decyzję w sprawie części dotyczącej oddalenia lub odrzucenia tej skargi, doręcza ją skarżącemu oraz informuje o niej administratora lub podmiot przetwarzający.

10. Po doręczeniu administratorowi lub podmiotowi przetwarzającemu decyzji wiodącego organu nadzorczego zgodnie z ust. 7 i 9, podejmują oni niezbędne działania, by zastosować się do tej decyzji, jeżeli chodzi o czynności przetwarzania w ramach wszystkich swoich jednostek organizacyjnych w Unii. Administrator lub podmiot przetwarzający zawiadamiają wiodący organ nadzorczy o działaniach podjętych w celu zastosowania się do decyzji, ten zaś informuje o nich inne organy nadzorcze, których sprawa dotyczy.

11. Jeżeli w wyjątkowych okolicznościach organ nadzorczy, którego sprawa dotyczy, ma powody sądzić, że istnieje pilna potrzeba podjęcia działań w celu ochrony interesów osób, których dane dotyczą, zastosowanie ma tryb pilny, o którym mowa w art. 66.

12. Wiodący organ nadzorczy i inne organy nadzorcze, których sprawa dotyczy, dostarczają sobie nawzajem informacji wymaganych na mocy niniejszego artykułu drogą elektroniczną w standardowym formacie.

Artykuł 61

Wzajemna pomoc

1. Organy nadzorcze przekazują sobie stosowne informacje i świadczą sobie wzajemną pomoc w celu spójnego wdrażania i stosowania niniejszego rozporządzenia oraz wprowadzają środki na rzecz skutecznej wzajemnej współpracy. Wzajemna pomoc obejmuje w szczególności wnioski o udzielenie informacji oraz środki nadzorcze, takie jak wnioski o udzielenie uprzednich zezwoleń i przeprowadzenie uprzednich konsultacji oraz o przeprowadzenie kontroli i postępowań wyjaśniających.

2. Każdy organ nadzorczy podejmuje wszelkie odpowiednie środki, by odpowiedzi na wniosek innego organu nadzorczego udzielić bez zbędnej zwłoki i nie później niż w terminie miesiąca od otrzymania wniosku. Środki takie mogą obejmować w szczególności przekazanie stosownych informacji o przebiegu postępowania.

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

4. Wezwany organ nadzorczy nie może odmówić wykonania wniosku, chyba że:

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

b) wykonanie wniosku stanowiłoby naruszenie niniejszego rozporządzenia, prawa Unii lub prawa państwa członkowskiego, któremu podlega wezwany organ nadzorczy.

5. Wezwany organ nadzorczy informuje wzywający organ nadzorczy, od którego wniosek pochodzi, o rezultatach lub w stosownym przypadku o postępach lub środkach zastosowanych w związku z tym wnioskiem. Wezwany organ nadzorczy uzasadnia odmowę wykonania wniosku na mocy ust. 4.

6. Wezwane organy nadzorcze przekazują informacje żądane przez inne organy nadzorcze zasadniczo drogą elektroniczną w standardowym formacie.

7. Wezwane organy nadzorcze nie pobierają opłat za działania podejmowane w związku z wnioskiem o wzajemną pomoc. Organy nadzorcze mogą uzgodnić zasady dokonywania wzajemnego zwrotu konkretnych wydatków poniesionych w wyniku świadczenia wzajemnej pomocy w wyjątkowych okolicznościach.

8. Jeżeli organ nadzorczy nie dostarczy informacji, o których mowa w ust. 5 niniejszego artykułu, w terminie miesiąca od otrzymania wniosku innego organu nadzorczego, wzywający organ nadzorczy może zastosować środek tymczasowy na terytorium swojego państwa członkowskiego zgodnie z art. 55 ust. 1. W takiej sytuacji uznaje się, że zgodnie z art. 66 ust. 1 zachodzi pilna potrzeba działania i że zgodnie z art. 66 ust. 2 wymagana jest pilna wiążąca decyzja Europejskiej Rady Ochrony Danych.

9. Komisja może w drodze aktów wykonawczych określić formułę i procedurę wzajemnej pomocy, o której mowa w niniejszym artykule, oraz zasady wymiany informacji drogą elektroniczną między organami nadzorczymi oraz między organami nadzorczymi a Europejską Radą Ochrony Danych, w szczególności standardowy format, o którym mowa w ust. 6 niniejszego artykułu. Akty wykonawcze są przyjmowane zgodnie z procedurą sprawdzającą, o której mowa w art. 93 ust. 2.

Artykuł 62

Wspólne operacje organów nadzorczych

1. Organy nadzorcze prowadzą w stosownych przypadkach wspólne operacje, w tym wspólne postępowania i wspólne działania egzekucyjne, w których uczestniczą członkowie lub personel organów nadzorczych innych państw członkowskich.

2. Jeżeli administrator lub podmiot przetwarzający posiadają jednostki organizacyjne w kilku państwach członkowskich lub jeżeli operacje przetwarzania mogą istotnie wpłynąć na znaczną liczbę osób, których dane dotyczą, w więcej niż jednym państwie członkowskim, organ nadzorczy każdego z tych państw członkowskich ma prawo uczestniczyć we wspólnych operacjach. Organ nadzorczy, który jest właściwy zgodnie z art. 56 ust. 1 lub 4 zaprasza organ nadzorczy każdego z tych państw członkowskich do uczestnictwa w danych wspólnych operacjach i niezwłocznie odpowiada na wniosek organu nadzorczego dotyczący uczestnictwa.

3. Organ nadzorczy może zgodnie z prawem państwa członkowskiego i za zgodą organu nadzorczego oddelegowującego pracownika przyznać uprawnienia, w tym uprawnienia do prowadzenia postępowań wyjaśniających, członkom lub personelowi organu nadzorczego oddelegowującego pracownika uczestniczącym we wspólnych operacjach lub – jeżeli zezwala na to prawo państwa członkowskiego przyjmującego organu nadzorczego – zezwolić członkom lub personelowi organu nadzorczego oddelegowującego pracownika na wykonywanie ich własnych uprawnień w zakresie prowadzenia postępowań wyjaśniających zgodnie z prawem państwa członkowskiego organu nadzorczego oddelegowującego pracownika. Uprawnienia takie mogą być wykonywane wyłącznie pod kierownictwem i w obecności członków lub personelu przyjmującego organu nadzorczego. Członkowie lub personel organu nadzorczego oddelegowującego pracownika podlegają prawu państwa członkowskiego przyjmującego organu nadzorczego.

4. Jeżeli zgodnie z ust. 1 personel organu nadzorczego oddelegowującego pracownika działa w innym państwie członkowskim, państwo członkowskie przyjmującego organu nadzorczego ponosi odpowiedzialność za czynności tego personelu, w tym odpowiedzialność prawną za wszelkie szkody wyrządzone przez ten personel w trakcie operacji, zgodnie z prawem państwa członkowskiego, na którego terytorium ten personel działa.

5. Państwo członkowskie, na którego terytorium została wyrządzona szkoda, naprawia taką szkodę na warunkach mających zastosowanie do szkód wyrządzonych przez jego własny personel. Państwo członkowskie organu nadzorczego oddelegowującego pracownika, którego personel wyrządził szkodę wobec osoby na terytorium innego państwa członkowskiego, zwraca temu innemu państwu członkowskiemu całą kwotę, którą zapłaciło ono osobom uprawnionym w jego imieniu.

6. Bez uszczerbku dla możliwości dochodzenia swoich praw wobec osób trzecich i z wyjątkiem ust. 5, każde państwo członkowskie powstrzymuje się w przypadku określonym w ust. 1 od żądania odszkodowania od innego państwa członkowskiego za szkody, o których mowa w ust. 4.

7. Jeżeli planowana jest wspólna operacja, a organ nadzorczy nie wywiąże się w terminie miesiąca z obowiązku określonego w ust. 2 zdanie drugie niniejszego artykułu, pozostałe organy nadzorcze mogą przyjąć środek tymczasowy na terytorium swojego państwa członkowskiego zgodnie z art. 55. W takiej sytuacji uznaje się, że zgodnie z art. 66 ust. 1 zachodzi pilna potrzeba działania i że zgodnie z art. 66 ust. 2 wymagana jest pilna opinia lub pilna wiążąca decyzja Europejskiej Rady Ochrony Danych.

Sekcja 2

Spójność

Artykuł 63

Mechanizm spójności

Aby przyczynić się do spójnego stosowania niniejszego rozporządzenia w całej Unii, organy nadzorcze współpracują ze sobą, a w stosownym przypadku także z Komisją, stosując mechanizm spójności określony w niniejszej sekcji.

Artykuł 64

Opinia Europejskiej Rady Ochrony Danych

1. Europejska Rada Ochrony Danych wydaje opinię w przypadku, gdy właściwy organ nadzorczy zamierza przyjąć środek wymieniony poniżej. W tym celu właściwy organ nadzorczy zgłasza Europejskiej Radzie Ochrony Danych projekt decyzji dotyczącej:

a) przyjęcia na mocy art. 35 ust. 4 wykazu operacji przetwarzania podlegających wymogowi dokonania oceny skutków dla ochrony danych;

b) stwierdzenia zgodnie z art. 40 ust. 7, czy projekt kodeksu postępowania, zmiana kodeksu lub rozszerzenie jego zakresu są zgodne z niniejszym rozporządzeniem;

c) zatwierdzenia kryteriów akredytacji podmiotu na mocy art. 41 ust. 3 lub podmiotu certyfikującego na mocy art. 43 ust. 3;

d) określenia standardowych klauzul ochrony danych, o których mowa w art. 46 ust. 2 lit. d) i art. 28 ust. 8;

e) wydania zezwolenia na klauzule umowne, o których mowa w art. 46 ust. 3; lub

f) zatwierdzenia wiążących reguł korporacyjnych w rozumieniu art. 47.

2. Każdy organ nadzorczy, przewodniczący Europejskiej Rady Ochrony Danych lub Komisja mogą wystąpić o przeanalizowanie przez Europejską Radę Ochrony Danych w celu wydania opinii sprawy mającej charakter ogólny lub wywołującej skutki w więcej niż jednym państwie członkowskim, w szczególności jeżeli właściwy organ nadzorczy nie wywiązuje się z obowiązków dotyczących wzajemnej pomocy zgodnie z art. 61 lub wspólnych operacji zgodnie z art. 62.

3. W przypadkach, o których mowa w ust. 1 i 2, Europejska Rada Ochrony Danych wydaje opinię w przedłożonej jej sprawie, o ile wcześniej nie wydała już opinii w takiej samej sprawie. Europejska Rady Ochrony Danych przyjmuje tę opinię w terminie ośmiu tygodni zwykłą większością głosów swoich członków. Ze względu na złożony charakter sprawy termin ten można przedłużyć o sześć tygodni. Jeżeli chodzi o projekt decyzji, o którym mowa w ust. 1 i który został przekazany członkom Europejskiej Rady Ochrony Danych zgodnie z ust. 5, uznaje się, że członek, który w rozsądnym terminie wskazanym przez przewodniczącego nie zgłosił sprzeciwu, zgadza się z tym projektem.

4. Organy nadzorcze i Komisja przekazują bez zbędnej zwłoki Europejskiej Radzie Ochrony Danych drogą elektroniczną w standardowym formacie wszelkie stosowne informacje, w tym w odpowiednim przypadku streszczenie stanu faktycznego, projekt decyzji, powody przemawiające za koniecznością przyjęcia takiego środka oraz opinię innych organów nadzorczych, których sprawa dotyczy.

5. Przewodniczący Europejskiej Rady Ochrony Danych bez zbędnej zwłoki przekazuje drogą elektroniczną:

a) członkom Europejskiej Rady Ochrony Danych i Komisji wszelkie stosowne informacje otrzymane w standardowym formacie. W razie potrzeby sekretariat Europejskiej Rady Ochrony Danych zapewnia tłumaczenie stosownych informacji; oraz

b) organowi nadzorczemu, o którym zależnie od sytuacji mowa w ust. 1 i 2, oraz Komisji opinię, którą podaje też do wiadomości publicznej.

6. Właściwy organ nadzorczy nie przyjmuje projektu decyzji, o którym mowa w art. ust. 1 przed upływem terminu, o którym mowa w ust. 3.

7. Organ nadzorczy, o którym mowa w ust. 1, w jak największym stopniu uwzględnia opinię Europejskiej Rady Ochrony Danych i w terminie dwóch tygodni po otrzymaniu tej opinii informuje drogą elektroniczną przewodniczącego Europejskiej Rady Ochrony Danych, czy podtrzymuje projekt decyzji, czy też go zmieni, a w stosownym przypadku przekazuje mu w standardowym formacie zmieniony projekt decyzji.

8. Jeżeli w terminie, o którym mowa w ust. 7 niniejszego artykułu, organ nadzorczy, którego sprawa dotyczy, poinformuje przewodniczącego Europejskiej Rady Ochrony Danych, że nie zamierza się zastosować do całości lub części jej opinii podając odpowiednie uzasadnienie, zastosowanie ma art. 65 ust. 1.

Artykuł 65

Rozstrzyganie sporów przez Europejską Radę Ochrony Danych

1. Aby w poszczególnych sytuacjach zapewnić właściwe i spójne stosowanie niniejszego rozporządzenia, Europejska Rada Ochrony Danych przyjmuje w następujących przypadkach wiążące decyzje:

a) jeżeli w przypadku, o którym mowa w art. 60 ust. 4, organ nadzorczy, którego sprawa dotyczy, zgłosił mający znaczenie dla sprawy i uzasadniony sprzeciw wobec projektu decyzji wiodącego organu nadzorczego, a wiodący organ nadzorczy odrzucił taki sprzeciw jako niemający znaczenia dla sprawy lub nieuzasadniony. Wiążąca decyzja dotyczy wszystkich spraw, które są przedmiotem mającego znaczenie dla sprawy i uzasadnionego sprzeciwu, w szczególności dotyczy tego, czy doszło do naruszenia niniejszego rozporządzenia;

b) jeżeli panują sprzeczne opinie co do tego, który z organów nadzorczych, których sprawa dotyczy, jest właściwy względem głównej jednostki organizacyjnej;

c) jeżeli właściwy organ nadzorczy nie wystąpił o opinię do Europejskiej Rady Ochrony Danych w przypadkach, o których mowa w art. 64 ust. 1, lub nie zastosował się do opinii Europejskiej Rady Ochrony Danych wydanej zgodnie z art. 64. W takim przypadku organ nadzorczy, którego sprawa dotyczy, lub Komisja mogą zgłosić sprawę Europejskiej Radzie Ochrony Danych.

2. Decyzję, o której mowa w ust. 1, Europejska Rada Ochrony Danych przyjmuje większością dwóch trzecich głosów swoich członków w terminie miesiąca od wpłynięcia sprawy. Ze względu na złożony charakter sprawy termin ten można przedłużyć o miesiąc. Decyzja, o której mowa w ust. 1, zostaje wraz z uzasadnieniem skierowana do wiodącego organu nadzorczego i wszystkich organów nadzorczych, których sprawa dotyczy, i jest dla nich wiążąca.

3. Jeżeli Europejska Rada Ochrony Danych nie jest w stanie przyjąć decyzji w terminach, o których mowa w ust. 2, przyjmuje decyzję w terminie dwóch tygodni po upłynięciu drugiego miesiąca, o którym mowa w ust. 2, zwykłą większością głosów swoich członków. Jeżeli głosy członków Europejskiej Rady Ochrony Danych rozkładają się po równo, decyduje głos przewodniczącego.

4. Przed upływem terminów, o których mowa w ust. 2 i 3, organy nadzorcze, których sprawa dotyczy, nie przyjmują decyzji w sprawie przedłożonej Europejskiej Radzie Ochrony Danych na mocy ust. 1.

5. Przewodniczący Europejskiej Rady Ochrony Danych bez zbędnej zwłoki notyfikuje organom nadzorczym, których sprawa dotyczy, decyzję, o której mowa w ust. 1. Informuje o niej Komisję. Decyzja jest niezwłocznie publikowana na stronie internetowej Europejskiej Rady Ochrony Danych, po tym jak organ nadzorczy notyfikował ostateczną decyzję, o której mowa w ust. 6.

6. Bez zbędnej zwłoki i najpóźniej w terminie miesiąca po notyfikowaniu przez Europejską Radę Ochrony Danych swojej decyzji, wiodący organ nadzorczy lub w stosownym przypadku organ nadzorczy, do którego wniesiono skargę, przyjmuje ostateczną decyzję na podstawie decyzji, o której mowa w ust. 1 niniejszego artykułu. Wiodący organ nadzorczy lub w stosownym przypadku organ nadzorczy, do którego wniesiono skargę, informuje Europejską Radę Ochrony Danych o terminie, w którym doręczono ostateczną decyzję odpowiednio administratorowi lub podmiotowi przetwarzającemu oraz osobie, której dane dotyczą. Ostateczna decyzja organów nadzorczych, których sprawa dotyczy, zostaje przyjęta w trybie art. 60 ust. 7, 8 i 9. Ostateczna decyzja zawiera informacje o decyzji, o której mowa w ust. 1 niniejszego artykułu, i wskazuje, że decyzja, o której mowa w tym ustępie, zostanie opublikowana na stronie internetowej Europejskiej Rady Ochrony Danych zgodnie z ust. 5 niniejszego artykułu. Do ostatecznej decyzji załączona zostaje decyzja, o której mowa w ust. 1 niniejszego artykułu.

Artykuł 66

Tryb pilny

1. W wyjątkowych okolicznościach, jeżeli organ nadzorczy, którego sprawa dotyczy, uzna, że istnieje pilna potrzeba podjęcia działań w celu ochrony praw i wolności osób, których dane dotyczą, może w drodze odstępstwa od mechanizmu spójności, o którym mowa w art. 63, 64 i 65, lub od procedury, o której mowa w art. 60, niezwłocznie przyjąć środki tymczasowe mające na terytorium jego państwa członkowskiego wywołać skutki prawne przez określony okres, nieprzekraczający trzech miesięcy. Organ nadzorczy niezwłocznie informuje o tych środkach i o powodach ich przyjęcia pozostałe organy nadzorcze, których sprawa dotyczy, Europejską Radę Ochrony Danych i Komisję.

2. Jeżeli organ nadzorczy zastosował środek na mocy ust. 1 i uznaje, że należy pilnie przyjąć środki o charakterze ostatecznym, może zwrócić się z wnioskiem o pilne wydanie opinii lub wiążącej decyzji do Europejskiej Rady Ochrony Danych, uzasadniając swój wniosek o taką opinię lub decyzję.

3. Organ nadzorczy może zwrócić się do Europejskiej Rady Ochrony Danych z wnioskiem o pilne wydanie opinii lub w stosownym przypadku wiążącej decyzji, uzasadniając swój wniosek o taką opinię lub decyzję, w tym uzasadniając pilną potrzebę działań – jeżeli właściwy organ nadzorczy nie zastosował odpowiedniego środka w sytuacji, w której istnieje pilna potrzeba podjęcia działań w celu ochrony praw i wolności osób, których dane dotyczą.

4. W drodze wyjątku od art. 64 ust. 3 i art. 65 ust. 2, Europejska Rada Ochrony Danych przyjmuje opinię lub wiążącą decyzję wydawane w trybie pilnym, o których mowa w ust. 2 i 3 niniejszego artykułu, w terminie dwóch tygodni zwykłą większością głosów swoich członków.

Artykuł 67

Wymiana informacji

Komisja może przyjmować akty wykonawcze o charakterze ogólnym, w celu określenia zasad wymiany informacji drogą elektroniczną między organami nadzorczymi oraz między organami nadzorczymi a Europejską Radą Ochrony Danych, w szczególności standardowy format, o którym mowa w art. 64.

Te akty wykonawcze są przyjmowane zgodnie z procedurą sprawdzającą, o której mowa w art. 93 ust. 2.

Sekcja 3

Europejska rada ochrony danych

Artykuł 68

Europejska Rada Ochrony Danych

1. Niniejszym ustanawia się Europejską Radę Ochrony Danych jako organ Unii posiadający osobowość prawną.

2. Europejską Radę Ochrony Danych reprezentuje jej przewodniczący.

3. Do Europejskiej Rady Ochrony Danych należą: przewodniczący jednego organu nadzorczego każdego państwa członkowskiego oraz Europejski Inspektor Ochrony Danych lub ich przedstawiciele.

4. Jeżeli w państwie członkowskim za monitorowanie stosowania przepisów na mocy niniejszego rozporządzenia odpowiada więcej niż jeden organ nadzorczy, to zgodnie z prawem tego państwa członkowskiego wyznaczony zostaje wspólny przedstawiciel.

5. Komisja ma prawo do udziału w działaniach i posiedzeniach Europejskiej Rady Ochrony Danych, nie ma jednak prawa głosowania. Komisja wyznacza swojego przedstawiciela. Przewodniczący Europejskiej Rady Ochrony Danych informuje Komisję o działaniach Europejskiej Rady Ochrony Danych.

6. W kwestiach, o których mowa w art. 65, Europejski Inspektor Ochrony Danych ma prawo głosowania wyłącznie względem decyzji co do zasad i przepisów, które mają zastosowanie do instytucji, organów i jednostek organizacyjnych Unii i merytorycznie odpowiadają przepisom niniejszego rozporządzenia.

Artykuł 69

Niezależność

1. W toku wypełniania swoich zadań lub wykonywania swoich uprawnień na mocy art. 70 i 71 Europejska Rada Ochrony Danych działa w sposób niezależny.

2. Bez uszczerbku dla wniosków Komisji, o których mowa w art. 70 ust. 1 lit. b) i art. 70 ust. 2, Europejska Rada Ochrony Danych podczas wypełniania swoich zadań lub wykonywania swoich uprawnień nie zwraca się do nikogo o instrukcje ani ich od nikogo nie przyjmuje.

Artykuł 70

Zadania Europejskiej Rady Ochrony Danych

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

a) monitoruje i zapewnia właściwe stosowanie niniejszego rozporządzenia w przypadkach, o których mowa w art. 64 i 65, bez uszczerbku dla zadań krajowych organów nadzorczych;

b) doradza Komisji w sprawach związanych z ochroną danych osobowych w Unii, w tym w sprawie wszelkich proponowanych zmian do niniejszego rozporządzenia;

c) doradza Komisji w sprawie formatu i procedur wymiany informacji między administratorami, podmiotami przetwarzającymi i organami nadzorczymi do celów wiążących reguł korporacyjnych;

d) wydaje wytyczne, zalecenia oraz określa najlepsze praktyki dotyczące usuwania z ogólnodostępnych usług łączności łącz do danych osobowych, kopi tych danych lub ich replikacji, o czym mowa w art. 17 ust. 2;

e) z własnej inicjatywy lub na wniosek jednego ze swoich członków lub Komisji bada wszelkie kwestie dotyczące stosowania niniejszego rozporządzenia i wydaje wytyczne, zalecenia oraz określa najlepsze praktyki, by zachęcić do spójnego stosowania niniejszego rozporządzenia;

f) wydaje wytyczne, zalecenia i określa najlepsze praktyki zgodnie z lit. e) niniejszego ustępu, by na potrzeby art. 22 ust. 2 doprecyzować kryteria i wymogi dotyczące decyzji opartych na profilowaniu;

g) wydaje wytyczne, zalecenia i określa najlepsze praktyki zgodnie z lit. e) niniejszego ustępu dotyczące stwierdzania naruszenia ochrony danych osobowych i określenia zbędnej zwłoki w rozumieniu art. 33 ust. 1 i 2 oraz szczególnych okoliczności, w których administrator lub podmiot przetwarzający mają obowiązek zgłosić naruszenie ochrony danych osobowych;

h) wydaje wytyczne, zalecenia i określa najlepsze praktyki zgodnie z lit. e) niniejszego ustępu wskazujące, w jakich okolicznościach naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych w rozumieniu art. 34 ust. 1;

i) wydaje wytyczne, zalecenia i określa najlepsze praktyki zgodnie z lit. e) niniejszego ustępu, by doprecyzować kryteria i wymogi względem przekazywania danych osobowych, które opiera się na wiążących regułach korporacyjnych stosowanych przez administratorów i na wiążących regułach korporacyjnych stosowanych przez podmioty przetwarzające, oraz inne konieczne wymogi mające zapewnić ochronę danych osobowych osób, których dane dotyczą, zgodnie z art. 47;

j) wydaje wytyczne, zalecenia i określa najlepsze praktyki zgodnie z lit. e) niniejszego ustępu, by doprecyzować kryteria i wymogi względem przekazywania danych osobowych na podstawie art. 49 ust. 1;

k) opracowuje wytyczne dla organów nadzorczych w sprawie stosowania środków, o których mowa w art. 58 ust. 1, 2 i 3, oraz w sprawie określania wysokości administracyjnych kar pieniężnych zgodnie z art. 83;

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

m) wydaje wytyczne, zalecenia i określa najlepsze praktyki zgodnie z lit. e) niniejszego ustępu, by na potrzeby art. 54 ust. 2 określić wspólne procedury postępowania w przypadkach zgłaszania przez osoby fizyczne naruszeń niniejszego rozporządzenia;

n) zachęca do sporządzania kodeksów postępowania oraz do ustanawiania mechanizmów certyfikacji w dziedzinie ochrony danych oraz znaków jakości i oznaczeń w tej dziedzinie zgodnie z art. 40 i 42;

o) akredytuje podmioty certyfikujące i dokonuje okresowego przeglądu certyfikacji zgodnie z art. 43 oraz prowadzi publiczny rejestr podmiotów akredytowanych zgodnie z art. 43 ust. 6 i administratorów i podmiotów przetwarzających akredytowanych zgodnie z art. 42 ust. 7, mających siedzibę w państwach trzecich;

p) precyzuje wymogi, o których mowa w art. 43 ust. 3, z myślą o akredytacji podmiotów certyfikujących zgodnie z art. 42;

q) udziela Komisji opinii w sprawie wymogów certyfikacyjnych, o których mowa w art. 43 ust. 8;

r) udziela Komisji opinii w sprawie znaków graficznych, o których mowa w art. 12 ust. 7;

s) udziela Komisji opinii na potrzeby oceny, czy stopień ochrony w państwie trzecim lub organizacji międzynarodowej jest odpowiedni, w tym na potrzeby oceny, czy państwo trzecie, terytorium, określony sektor lub określone sektory w tym państwie trzecim lub organizacja międzynarodowa nie przestały zapewniać odpowiedniego stopnia ochrony. W tym celu Komisja udostępnia Europejskiej Radzie Ochrony Danych wszelką niezbędną dokumentację, w tym korespondencję z rządem państwa trzeciego w odniesieniu do tego państwa trzeciego, terytorium lub określonego sektora lub korespondencję z organizacją międzynarodową;

t) wydaje opinie w sprawie projektów decyzji zgłoszonych przez organy nadzorcze zgodnie z mechanizmem spójności, o którym mowa w art. 64 ust. 1, w sprawach przedłożonych jej zgodnie z art. 64 ust. 2 oraz wydaje wiążące decyzje zgodnie z art. 65, w tym w sprawach, o których mowa w art. 66;

u) upowszechnia współpracę oraz skuteczną dwustronną i wielostronną wymianę informacji i dobrych praktyk między organami nadzorczymi;

v) upowszechnia wspólne programy szkoleń oraz ułatwia wymianę personelu między organami nadzorczymi, a w stosownych przypadkach – z organami nadzorczymi państw trzecich lub organizacji międzynarodowych;

w) upowszechnia wymianę wiedzy i dokumentów na temat ustawodawstwa i praktyki w dziedzinie ochrony danych z organami nadzorczymi odpowiedzialnymi za ochronę danych na świecie;

x) wydaje opinie na temat kodeksów postępowania opracowywanych na szczeblu Unii zgodnie z art. 40 ust. 9; oraz

y) prowadzi publicznie dostępny elektroniczny rejestr decyzji podjętych przez organy nadzorcze i wyroków sądowych w sprawach rozpatrywanych w ramach mechanizmu spójności.

2. Jeżeli Komisja zwraca się do Europejskiej Rady Ochrony Danych o konsultację, może zależnie od pilności sprawy wskazać termin udzielenia odpowiedzi.

3. Europejska Rada Ochrony Danych przekazuje swoje opinie, wytyczne, zalecenia i najlepsze praktyki Komisji i komitetowi, o którym mowa w art. 93, oraz podaje je do wiadomości publicznej.

4. Europejska Rada Ochrony Danych konsultuje się w stosownych przypadkach ze stronami, których sprawa dotyczy, i daje im możliwość przestawienia uwag w rozsądnym terminie. Bez uszczerbku dla art. 76 Europejska Rada Ochrony Danych podaje wyniki procedury konsultacji do wiadomości publicznej.

Artykuł 71

Sprawozdania

1. Europejska Rada Ochrony Danych sporządza roczne sprawozdanie na temat ochrony osób fizycznych w związku z przetwarzaniem danych w Unii, a w stosownym przypadku w państwach trzecich i organizacjach międzynarodowych. Sprawozdanie zostaje podane do wiadomości publicznej oraz przekazane Parlamentowi Europejskiemu, Radzie i Komisji.

2. Sprawozdanie roczne obejmuje przegląd praktycznego stosowania wytycznych, zaleceń i najlepszych praktyk, o których mowa w art. 70 ust. 1 lit. l), oraz wiążących decyzji, o których mowa w art. 65.

Artykuł 72

Procedura

1. Europejska Rada Ochrony Danych podejmuje decyzje zwykłą większością głosów swoich członków, o ile niniejsze rozporządzenie nie przewiduje inaczej.

2. Europejska Rada Ochrony Danych przyjmuje swój regulamin wewnętrzny większością dwóch trzecich głosów swoich członków i określa swoje zasady działania.

Artykuł 73

Przewodniczący

1. Europejska Rada Ochrony Danych wybiera zwykłą większością głosów spośród swoich członków przewodniczącego i dwóch wiceprzewodniczących.

2. Kadencja przewodniczącego i wiceprzewodniczących trwa pięć lat i może zostać jednokrotnie powtórzona.

Artykuł 74

Zadania przewodniczącego

1. Przewodniczący ma następujące zadania:

a) zwołuje posiedzenia Europejskiej Rady Ochrony Danych i sporządza porządek obrad;

b) notyfikuje wiodącemu organowi nadzorczemu i organom nadzorczym, których sprawa dotyczy, decyzje przyjęte przez Europejską Radę Ochrony Danych na mocy art. 65;

c) zapewnia terminowe wykonanie zadań Europejskiej Rady Ochrony Danych, w szczególności w odniesieniu do mechanizmu spójności, o którym mowa w art. 63.

2. Europejska Rada Ochrony Danych określa w swoim regulaminie wewnętrznym podział zadań między przewodniczącego a wiceprzewodniczących.

Artykuł 75

Sekretariat

1. Europejski Inspektor Ochrony Danych zapewnia obsługę sekretariatu dla Europejskiej Rady Ochrony Danych.

2. Sekretariat wykonuje swoje zadania wyłącznie pod kierunkiem przewodniczącego Europejskiej Rady Ochrony Danych.

3. Personel Europejskiego Inspektora Ochrony Danych wykonujący zadania, które niniejsze rozporządzenie powierza Europejskiej Radzie Ochrony Danych, podlega oddzielnej hierarchii służbowej, innej niż personel wykonujący zadania powierzone Europejskiemu Inspektorowi Ochrony Danych.

4. W stosownych przypadkach Europejska Rada Ochrony Danych i Europejski Inspektor Ochrony Danych opracowują i publikują protokół ustaleń, który służy wykonaniu niniejszego artykułu: określa on warunki współpracy i ma zastosowanie do personelu Europejskiego Inspektora Ochrony Danych wykonującego zadania powierzone niniejszym rozporządzeniem Europejskiej Radzie Ochrony Danych.

5. Sekretariat zapewnia Europejskiej Radzie Ochrony Danych wsparcie analityczne, administracyjne i logistyczne.

6. Sekretariat odpowiada w szczególności za:

a) bieżącą działalność Europejskiej Rady Ochrony Danych;

b) komunikację między członkami Europejskiej Rady Ochrony Danych, jej przewodniczącym i Komisją;

c) komunikację z innymi instytucjami i opinią publiczną;

d) stosowanie elektronicznych środków komunikacji wewnętrznej i zewnętrznej;

e) tłumaczenie stosownych informacji;

f) przygotowywanie posiedzeń Europejskiej Rady Ochrony Danych oraz działania następcze w związku z nimi;

g) przygotowywanie, redagowanie i publikowanie opinii, decyzji w sprawie rozstrzygnięcia sporów między organami nadzorczymi oraz innych tekstów przyjmowanych przez Europejską Radę Ochrony Danych.

Artykuł 76

Poufność

1. Dyskusje Europejskiej Rady Ochrony Danych są poufne, jeżeli taką konieczność stwierdzi Rada zgodnie ze swoim regulaminem wewnętrznym.

2. Dostęp do dokumentów przedłożonych członkom Europejskiej Rady Ochrony Danych, ekspertom i przedstawicielom stron trzecich jest regulowany rozporządzeniem Parlamentu Europejskiego i Rady (WE) nr 1049/2001 ([1]).

ROZDZIAŁ VIII

Środki ochrony prawnej, odpowiedzialność i sankcje

Artykuł 77

Prawo do wniesienia skargi do organu nadzorczego

1. Bez uszczerbku dla innych administracyjnych lub środków ochrony prawnej przed sądem każda osoba, której dane dotyczą, ma prawo wnieść skargę do organu nadzorczego, w szczególności w państwie członkowskim swojego zwykłego pobytu, swojego miejsca pracy lub miejsca popełnienia domniemanego naruszenia, jeżeli sądzi, że przetwarzanie danych osobowych jej dotyczące narusza niniejsze rozporządzenie.

2. Organ nadzorczy, do którego wniesiono skargę, informuje skarżącego o postępach i efektach rozpatrywania skargi, w tym o możliwości skorzystania z sądowego środka ochrony prawnej na mocy art. 78.

Artykuł 78

Prawo do skutecznego środka ochrony prawnej przed sądem przeciwko organowi nadzorczemu

1. Bez uszczerbku dla innych administracyjnych lub pozasądowych środków ochrony prawnej każda osoba fizyczna lub prawna ma prawo do skutecznego środka ochrony prawnej przed sądem przeciwko prawnie wiążącej decyzji organu nadzorczego jej dotyczącej.

2. Bez uszczerbku dla innych administracyjnych lub pozasądowych środków ochrony prawnej każda osoba, której dane dotyczą, ma prawo do skutecznego środka ochrony prawnej przed sądem, jeżeli organ nadzorczy właściwy zgodnie z art. 55 i 56 nie rozpatrzył skargi lub nie poinformował osoby, której dane dotyczą, w terminie trzech miesięcy o postępach lub efektach rozpatrywania skargi wniesionej zgodnie z art. 77.

3. Postępowanie przeciwko organowi nadzorczemu zostaje wszczęte przed sądem państwa członkowskiego, w którym organ nadzorczy ma siedzibę.

4. Jeżeli postępowanie zostało wszczęte przeciwko decyzji organu nadzorczego, którą poprzedziła opinia lub decyzja Europejskiej Rady Ochrony Danych w ramach mechanizmu spójności, organ nadzorczy przekazuje sądowi tę opinię lub decyzję.

Artykuł 79

Prawo do skutecznego środka ochrony prawnej przed sądem przeciwko administratorowi lub podmiotowi przetwarzającemu

1. Bez uszczerbku dla dostępnych administracyjnych lub pozasądowych środków ochrony prawnej, w tym prawa do wniesienia skargi do organu nadzorczego zgodnie z art. 77, każda osoba, której dane dotyczą, ma prawo do skutecznego środka ochrony prawnej przed sądem, jeżeli uzna ona, że prawa przysługujące jej na mocy niniejszego rozporządzenia zostały naruszone w wyniku przetwarzania jego danych osobowych z naruszeniem niniejszego rozporządzenia.

2. Postępowanie przeciwko administratorowi lub podmiotowi przetwarzającemu wszczyna się przed sądem państwa członkowskiego, w którym administrator lub podmiot przetwarzający posiadają jednostkę organizacyjną. Ewentualnie postępowanie takie może zostać wszczęte przed sądem państwa członkowskiego, w którym osoba, której dane dotyczą, ma miejsce zwykłego pobytu, chyba że administrator lub podmiot przetwarzający są organami publicznymi państwa członkowskiego wykonującymi swoje uprawnienia publiczne.

([1]) Rozporządzenie (WE) nr 1049/2001 Parlamentu Europejskiego i Rady z dnia 30 maja 2001 r. w sprawie publicznego dostępu do dokumentów Parlamentu Europejskiego, Rady i Komisji (Dz.U. L 145 z 31.5.2001, s. 43).

Artykuł 80

Reprezentowanie osób, których dane dotyczą

1. Osoba, której dane dotyczą, ma prawo umocować podmiot, organizację lub zrzeszenie – które nie mają charakteru zarobkowego, zostały należycie ustanowione zgodnie z prawem państwa członkowskiego, mają cele statutowe leżące w interesie publicznym i działają w dziedzinie ochrony praw i wolności osoób, których dane dotyczą, w związku z ochroną ich danych osobowych – do wniesienia w jej imieniu skargi oraz wykonywania w jej imieniu praw, o których mowa w art. 77, 78 i 79, oraz żądania w jej imieniu odszkodowania, o którym mowa w art. 82, jeżeli przewiduje to prawo państwa członkowskiego.

2. Państwa członkowskie mogą przewidzieć, że podmiot, organizacja lub zrzeszenie, o których mowa w ust. 1 niniejszego artykułu, mają – niezależnie od upoważnienia otrzymanego od osoby, której dane dotyczą – prawo wnieść w tym państwie członkowskim skargę do organu nadzorczego właściwego zgodnie z art. 77 oraz wykonać prawa, o których mowa w art. 78 i 79, jeżeli uznają, że w wyniku przetwarzania naruszone zostały prawa osoby, której dane dotyczą, wynikające z niniejszego rozporządzenia.

Artykuł 81

Zawieszenie postępowania

1. Jeżeli właściwy sąd państwa członkowskiego posiada informację, że przed sądem w innym państwie członkowskim toczy się postępowanie w tej samej sprawie w odniesieniu do przetwarzania przez tego samego administratora lub ten sam podmiot przetwarzający, kontaktuje się z tym sądem w innym państwie członkowskim, aby potwierdzić istnienie takiego postępowania.

2. Jeżeli przed sądem w innym państwie członkowskim toczy się postępowanie w tej samej sprawie w odniesieniu do przetwarzania przez tego samego administratora lub ten sam podmiot przetwarzający, właściwy sąd inny niż sąd, przed którym jako pierwszym wszczęto postępowanie, może zawiesić swoje postępowanie.

3. Jeżeli postępowania te toczą się w pierwszej instancji, sąd inny niż sąd, przed którym jako pierwszym wszczęto postępowanie, może także – na wniosek jednej ze stron – stwierdzić brak swojej jurysdykcji, jeżeli sąd, przed którym jako pierwszym wszczęto postępowanie, ma jurysdykcję względem przedmiotowych spraw, a jego prawo dopuszcza ich połączenie.

Artykuł 82

Prawo do odszkodowania i odpowiedzialność

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

2. Każdy administrator uczestniczący w przetwarzaniu odpowiada za szkody spowodowane przetwarzaniem naruszającym niniejsze rozporządzenie. Podmiot przetwarzający odpowiada za szkody spowodowane przetwarzaniem wyłącznie, gdy nie dopełnił obowiązków, które niniejsze rozporządzenie nakłada bezpośrednio na podmioty przetwarzające, lub gdy działał poza zgodnymi z prawem instrukcjami administratora lub wbrew tym instrukcjom.

3. Administrator lub podmiot przetwarzający zostają zwolnieni z odpowiedzialności wynikającej z ust. 2, jeżeli udowodnią, że w żaden sposób nie ponoszą winy za zdarzenie, które doprowadziło do powstania szkody.

4. Jeżeli w tym samym przetwarzaniu uczestniczy więcej niż jeden administrator lub podmiot przetwarzający lub uczestniczy w nim zarówno administrator jak i podmiot przetwarzający i zgodnie z ust. 2 i 3 odpowiadają za szkodę spowodowaną przetwarzaniem, ponoszą oni odpowiedzialność solidarną za całą szkodę, tak by zapewnić osobie, której dane dotyczą, rzeczywiste uzyskanie odszkodowania.

5. Administrator lub podmiot przetwarzający, który zgodnie z ust. 4 zapłacił odszkodowanie za całą wyrządzoną szkodę, ma prawo żądania od pozostałych administratorów lub podmiotów przetwarzających, którzy uczestniczyli w tym samym przetwarzaniu, zwrotu części odszkodowania odpowiadającej części szkody, za którą ponoszą odpowiedzialność, zgodnie z warunkami określonymi w ust. 2.

6. Postępowanie sądowe dotyczące odszkodowania jest wszczynane przed sądem właściwym na mocy prawa państwa członkowskiego, o którym mowa w art. 79 ust. 2.

Artykuł 83

Ogólne warunki nakładania administracyjnych kar pieniężnych

1. Każdy organ nadzorczy zapewnia, by stosowane na mocy niniejszego artykułu za naruszenia niniejszego rozporządzenia administracyjne kary pieniężne, o których mowa w ust. 4, 5 i 6, były w każdym indywidualnym przypadku skuteczne, proporcjonalne i odstraszające.

2. Administracyjne kary pieniężne nakłada się, zależnie od okoliczności każdego indywidualnego przypadku, oprócz lub zamiast środków, o których mowa w art. 58 ust. 2 lit. a)–h) oraz j). Decydując, czy nałożyć administracyjną karę pieniężną, oraz ustalając jej wysokość, zwraca się w każdym indywidualnym przypadku należytą uwagę na:

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

b) umyślny lub nieumyślny charakter naruszenia;

c) działania podjęte przez administratora lub podmiot przetwarzający w celu zminimalizowania szkody poniesionej przez osoby, których dane dotyczą;

d) stopień odpowiedzialności administratora lub podmiotu przetwarzającego z uwzględnieniem środków technicznych i organizacyjnych wdrożonych przez nich na mocy art. 25 i 32;

e) wszelkie stosowne wcześniejsze naruszenia ze strony administratora lub podmiotu przetwarzającego;

f) stopień współpracy z organem nadzorczym w celu usunięcia naruszenia oraz złagodzenia jego ewentualnych negatywnych skutków;

g) kategorie danych osobowych, których dotyczyło naruszenie;

h) sposób, w jaki organ nadzorczy dowiedział się o naruszeniu, w szczególności, czy i w jakim zakresie administrator lub podmiot przetwarzający zgłosili naruszenie;

i) jeżeli wobec administratora lub podmiotu przetwarzającego, których sprawa dotyczy, zostały wcześniej zastosowane w tej samej sprawie środki, o których mowa w art. 58 ust. 2 – przestrzeganie tych środków;

j) stosowanie zatwierdzonych kodeksów postępowania na mocy art. 40 lub zatwierdzonych mechanizmów certyfikacji na mocy art. 42; oraz

k) wszelkie inne obciążające lub łagodzące czynniki mające zastosowanie do okoliczności sprawy, takie jak osiągnięte bezpośrednio lub pośrednio w związku z naruszeniem korzyści finansowe lub uniknięte straty.

3. Jeżeli administrator lub podmiot przetwarzający narusza umyślnie lub nieumyślnie w ramach tych samych lub powiązanych operacji przetwarzania kilka przepisów niniejszego rozporządzenia, całkowita wysokość administracyjnej kary pieniężnej nie przekracza wysokości kary za najpoważniejsze naruszenie.

4. Naruszenia przepisów dotyczących następujących kwesti podlegają zgodnie z ust. 2 administracyjnej karze pieniężnej w wysokości do 10 000 000 EUR, a w przypadku przedsiębiorstwa – w wysokości do 2 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa:

a) obowiązków administratora i podmiotu przetwarzającego, o których mowa w art. 8, 11, 25 –39 oraz 42 i 43;

b) obowiązków podmiotu certyfikującego, o których mowa w art. 42 oraz 43;

c) obowiązków podmiotu monitorującego, o których mowa w art. 41 ust. 4;

5. Naruszenia przepisów dotyczących następujących kwestii podlegają zgodnie z ust. 2 administracyjnej karze pieniężnej w wysokości do 20 000 000 EUR, a w przypadku przedsiębiorstwa – w wysokości do 4 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa:

a) podstawowych zasad przetwarzania, w tym warunków zgody, o których to zasadach i warunkach mowa w art. 5, 6, 7 oraz 9;

b) praw osób, których dane dotyczą, o których mowa w art. 12–22;

c) przekazywania danych osobowych odbiorcy w państwie trzecim lub organizacji międzynarodowej, o którym to przekazywaniu mowa w art. 44–49;

d) wszelkich obowiązków wynikających z prawa państwa członkowskiego przyjętego na podstawie rozdziału IX;

e) nieprzestrzegania nakazu, tymczasowego lub ostatecznego ograniczenia przetwarzania lub zawieszenia przepływu danych orzeczonego przez organ nadzorczy na podstawie art. 58 ust. 2 lub niezapewnienia dostępu skutkującego naruszeniem art. 58 ust. 1.

6. Nieprzestrzeganie nakazu orzeczonego przez organ nadzorczy na podstawie art. 58 ust. 2 podlega na mocy ust. 2 niniejszego artykułu administracyjnej karze pieniężnej w wysokości do 20 000 000 EUR, a w przypadku przedsiębiorstwa – w wysokości do 4 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa.

7. Bez uszczerbku dla uprawnień naprawczych organu nadzorczego, o których mowa w ust. 58 ust. 2, każde państwo członkowskie może określić, czy i w jakim zakresie administracyjne kary pieniężne można nakładać na organy i podmioty publiczne ustanowione w tym państwie członkowskim.

8. Wykonywanie przez organ nadzorczy uprawnień powierzonych mu na mocy niniejszego artykułu podlega odpowiednim zabezpieczeniom proceduralnym zgodnie z prawem Unii i prawem państwa członkowskiego, obejmującym prawo do skutecznego sądowego środka ochrony prawnej i rzetelnego procesu.

9. Jeżeli ustrój prawny państwa członkowskiego nie przewiduje administracyjnych kar pieniężnych, niniejszy artykuł można stosować w ten sposób, że o zastosowanie kary pieniężnej wnosi właściwy organ nadzorczy, a nakłada ją właściwy sąd krajowy, o ile zapewniona zostaje skuteczność tych rozwiązań prawnych i równoważność ich skutku względem administracyjnej kary pieniężnej nakładanej przez organ nadzorczy. Nakładane kary pieniężne muszą być w każdym przypadku skuteczne, proporcjonalne i odstraszające. W terminie określonym w art. 91 ust. 2 takie państwa członkowskie zawiadamiają Komisję o przepisach swojego prawa, które przyjęły zgodnie z niniejszym ustępem do dnia 25 maja 2018 r., a następnie niezwłocznie o wszelkich późniejszych aktach zmieniających lub zmianach mających wpływ na te przepisy.

Artykuł 84

Sankcje

1. Państwa członkowskie przyjmują przepisy określające inne sankcje za naruszenia niniejszego rozporządzenia, w szczególności za naruszenia niepodlegające administracyjnym karom pieniężnym na mocy art. 83, oraz podejmują wszelkie środki niezbędne do ich wykonania. Sankcje te muszą być skuteczne, proporcjonalne i odstraszające.

2. Do dnia 25 maja 2018 r. każde państwo członkowskie zawiadamia Komisję o swoich przepisach przyjętych zgodnie z ust. 1, a następnie niezwłocznie o każdej późniejszej ich zmianie.

ROZDZIAŁ IX

Przepisy dotyczące szczególnych sytuacji związanych z przetwarzaniem

Artykuł 85

Przetwarzanie a wolność wypowiedzi i informacji

1. Państwa członkowskie przyjmują przepisy pozwalające pogodzić prawo do ochrony danych osobowych na mocy niniejszego rozporządzenia z wolnością wypowiedzi i informacji, w tym do przetwarzania dla potrzeb dziennikarskich oraz do celów wypowiedzi akademickiej, artystycznej lub literackiej.

2. Dla przetwarzania do celów dziennikarskich lub do celów wypowiedzi akademickiej, artystycznej lub literackiej państwa członkowskie określają odstępstwa lub wyjątki od rozdziału II (Zasady), rozdziału III (Prawa osoby, której dane dotyczą), rozdziału IV (Administrator i podmiot przetwarzający), rozdziału V (Przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych), rozdziału VI (Niezależne organy nadzorcze), rozdziału VII (Współpraca i spójność) oraz rozdziału IX (Szczególne sytuacje związane z przetwarzaniem danych), jeżeli są one niezbędne, by pogodzić prawo do ochrony danych osobowych z wolnością wypowiedzi i informacji.

3. Każde państwo członkowskie zawiadamia Komisję o przepisach, które przyjęło zgodnie z ust. 2, a następnie niezwłocznie o wszelkich późniejszych aktach zmieniających lub zmianach ich dotyczących.

Artykuł 86

Przetwarzanie a publiczny dostęp do dokumentów urzędowych

Dane osobowe zawarte w dokumentach urzędowych, które posiada organ lub podmiot publiczny lub podmiot 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 na mocy niniejszego rozporządzenia.

Artykuł 87

Przetwarzanie krajowego numeru identyfikacyjnego

Państwa członkowskie mogą określić szczególne warunki przetwarzania krajowego numeru identyfikacyjnego lub innego identyfikatora o zasięgu ogólnym. W takim przypadku krajowego numeru identyfikacyjnego lub innego identyfikatora o zasięgu ogólnym używa się wyłącznie z zachowaniem odpowiednich zabezpieczeń praw i wolności osoby, której dane dotyczą, które przewiduje niniejsze rozporządzenie.

Artykuł 88

Przetwarzanie w kontekście zatrudnienia

1. Państwa członkowskie mogą zawrzeć w swoich przepisach lub w porozumieniach zbiorowych bardziej szczegółowe przepisy mające zapewnić ochronę praw i wolności w przypadku przetwarzania danych osobowych pracowników w związku z zatrudnieniem, w szczególności do celów rekrutacji, wykonania umowy o pracę, w tym wykonania obowiązków określonych przepisami lub porozumieniami zbiorowymi, zarządzania, planowania i organizacji pracy, równości i różnorodności w miejscu pracy, bezpieczeństwa i higieny pracy, ochrony własności pracodawcy lub klienta oraz do celów indywidualnego lub zbiorowego wykonywania praw i korzystania ze świadczeń związanych z zatrudnieniem, a także do celów zakończenia stosunku pracy.

2. Przepisy te muszą obejmować odpowiednie i szczegółowe środki zapewniające osobie, której dane dotyczą, poszanowanie jej godności, prawnie uzasadnionych interesów i praw podstawowych, w szczególności pod względem przejrzystości przetwarzania, przekazywania danych osobowych w ramach grupy przedsiębiorstw lub grupy przedsiębiorców prowadzących wspólną działalność gospodarczą oraz systemów monitorujących w miejscu pracy.

3. Do dnia 25 maja 2018 r. każde państwo członkowskie zawiadamia Komisję o swoich przepisach przyjętych na mocy ust. 1, a następnie niezwłocznie o każdej dotyczącej ich późniejszej zmianie.

Artykuł 89

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

1. Przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych podlega odpowiednim zabezpieczeniom dla praw i wolności osoby, której dane dotyczą, zgodnie z niniejszym rozporządzeniem. Zabezpieczenia te polegają na wdrożeniu środków technicznych i organizacyjnych zapewniających poszanowanie zasady minimalizacji danych. Środki te mogą też obejmować pseudonimizację

danych, o ile pozwala ona realizować powyższe cele. Jeżeli cele te można zrealizować w drodze dalszego przetwarzania danych, które nie pozwalają albo przestały pozwalać na zidentyfikować osoby, której dane dotyczą, cele należy realizować w ten sposób.

2. W przypadku przetwarzania danych osobowych do celów badań naukowych lub historycznych lub do celów statystycznych prawo Unii lub prawo państwa członkowskiego mogą przewidzieć wyjątki od praw, o których mowa w art. 15, 16, 18 i 21, z zastrzeżeniem warunków i zabezpieczeń, o których mowa w ust. 1 niniejszego artykułu, jeżeli jest prawdopodobne, że prawa te uniemożliwią lub poważnie utrudnią realizację wspomnianych konkretnych celów, i jeżeli wyjątki takie są konieczne do realizacji tych celów.

3. W przypadku przetwarzania danych osobowych do celów archiwalnych w interesie publicznym prawo Unii lub prawo państwa członkowskiego mogą przewidzieć wyjątki od praw, o których mowa w art. 15, 16, 18, 19, 20 i 21, z zastrzeżeniem warunków i zabezpieczeń, o których mowa w ust. 1 niniejszego artykułu, jeżeli jest prawdopodobne, że prawa te uniemożliwią lub poważnie utrudnią realizację wspomnianych konkretnych celów, i jeżeli wyjątki takie są konieczne do realizacji tych celów.

4. Jeżeli przetwarzanie, o którym mowa w ust. 2 i 3, służy równocześnie innemu celowi, wspomniane wyjątki mają zastosowanie wyłącznie do przetwarzania w celach, o których mowa w tych ustępach.

Artykuł 90

Obowiązek zachowania tajemnicy

1. Państwa członkowskie mogą przyjąć przepisy szczególne określające uprawnienia organów nadzorczych ustanowione w art. 58 ust. 1 lit. e) i f) wobec administratorów lub podmiotów przetwarzających, którzy podlegają – na mocy prawa Unii lub prawa państwa członkowskiego lub przepisów ustanowionych przez właściwe organy krajowe – obowiązkowi zachowania tajemnicy zawodowej lub innym równoważnym obowiązkom zachowania tajemnicy, jeżeli jest to niezbędne i proporcjonalne w celu pogodzenia prawa do ochrony danych osobowych z obowiązkiem zachowania tajemnicy. Przepisy te mają zastosowanie wyłącznie do danych osobowych, które administrator lub podmiot przetwarzający otrzymali lub pozyskali w wyniku lub w ramach działania objętego tym obowiązkiem zachowania tajemnicy.

2. Do dnia 25 maja 2018 r. każde państwo członkowskie zawiadamia Komisję o swoich przepisach uchwalonych na mocy ust. 1, a następnie niezwłocznie o każdej dotyczącej ich późniejszej zmianie.

Artykuł 91

Istniejące zasady ochrony danych obowiązujące kościoły i związki wyznaniowe

1. Jeżeli w państwie członkowskim w momencie wejścia niniejszego rozporządzenia w życie kościoły i związki lub wspólnoty wyznaniowe stosują szczegółowe zasady ochrony osób fizycznych w związku z przetwarzaniem, zasady takie mogą być nadal stosowane, pod warunkiem że zostaną dostosowane do niniejszego rozporządzenia.

2. Kościoły i związki wyznaniowe, które stosują szczegółowe zasady zgodnie z ust. 1 niniejszego artykułu, podlegają nadzorowi niezależnego organu nadzorczego, który może być organem odrębnym, z zastrzeżeniem że spełnia warunki określone w rozdziale VI niniejszego rozporządzenia.

ROZDZIAŁ X

Akty delegowane i akty wykonawcze

Artykuł 92

Wykonywanie przekazanych uprawnień

1. Powierzenie Komisji uprawnień do przyjęcia aktów delegowanych podlega warunkom określonym w niniejszym artykule.

2. Uprawnienia do przyjmowania aktów delegowanych, o których mowa w art. 12 ust. 8 i art. 43 ust. 8, powierza się Komisji na czas nieokreślony od dnia 24 maja 2016 r.

3. Przekazanie uprawnień, o którym mowa w art. 12. ust. 8 i art. 43 ust. 8, może zostać w dowolnym momencie odwołane przez Parlament Europejski lub przez Radę. Decyzja o odwołaniu kończy przekazanie określonych w niej uprawnień. Decyzja o odwołaniu staje się skuteczna od następnego dnia po jej opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej* lub w określonym w tej decyzji późniejszym terminie. Nie wpływa ona na ważność jakichkolwiek już obowiązujących aktów delegowanych.

4. Niezwłocznie po przyjęciu aktu delegowanego Komisja przekazuje go równocześnie Parlamentowi Europejskiemu i Radzie.

5. Akt delegowany przyjęty na podstawie art. 12 ust. 8 i art. 43 ust. 8 wchodzi w życie tylko wówczas, gdy ani Parlament Europejski, ani Rada nie wyraziły sprzeciwu w terminie trzech miesięcy od przekazania tego aktu Parlamentowi Europejskiemu i Radzie, lub gdy, przed upływem tego terminu, zarówno Parlament Europejski, jak i Rada poinformowały Komisję, że nie wniosą sprzeciwu. Termin ten przedłuża się o trzy miesiące z inicjatywy Parlamentu Europejskiego lub Rady..

Artykuł 93

Procedura komitetowa

1. Komisję wspomaga komitet. Komitet ten jest komitetem w rozumieniu rozporządzenia (UE) nr 182/2011.

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

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

ROZDZIAŁ XI

Przepisy końcowe

Artykuł 94

Uchylenie dyrektywy 95/46/WE

1. Dyrektywa 95/46/WE zostaje uchylona ze skutkiem od dnia 25 maja 2018 r.

2. Odesłania do uchylonej dyrektywy należy traktować jako odesłania do niniejszego rozporządzenia. Odesłania do Grupy Roboczej ds. Ochrony Osób Fizycznych w zakresie Przetwarzania Danych Osobowych, ustanowionej w art. 29 dyrektywy 95/46/WE, należy traktować jako odesłania do Europejskiej Rady Ochrony Danych, ustanowionej niniejszym rozporządzeniem.

Artykuł 95

Stosunek do dyrektywy 2002/58/WE

Niniejsze rozporządzenie nie nakłada dodatkowych obowiązków na osoby fizyczne ani prawne co do przetwarzania w związku ze świadczeniem ogólnodostępnych usług łączności elektronicznej w publicznych sieciach łączności w Unii w sprawach, w których podmioty te podlegają szczegółowym obowiązkom mającym ten sam cel określonym w dyrektywie 2002/58/WE.

Artykuł 96

Stosunek do uprzednio zawartych umów

Umowy międzynarodowe, które przewidują przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych i które zostały zawarte przez państwa członkowskie przed dniem 24 maja 2016 r., i które są zgodne z prawem Unii mającym zastosowanie przed tym dniem, pozostają w mocy do czasu ich zmiany, zastąpienia lub uchylenia.

Artykuł 97

Sprawozdania Komisji

1. Do dnia 25 maja 2020 r., a następie co cztery lata Komisja przedkłada Parlamentowi Europejskiemu i Radzie sprawozdania z oceny i przeglądu niniejszego rozporządzenia. Sprawozdania te są podawane do wiadomości publicznej.

2. W ramach tych ocen Komisja analizuje i dokonuje przeglądu, o którym mowa w ust. 1, w szczególności stosowania i funkcjonowania przepisów:

a) rozdziału V dotyczącego przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych ze szczególnym uwzględnieniem decyzji przyjętych na mocy art. 45 ust. 3 niniejszego rozporządzenia oraz decyzji przyjętych na podstawie art. 25 ust. 6 dyrektywy 95/46/WE;

b) rozdziału VII dotyczącego współpracy i spójności.

3. Na potrzeby ust. 1, 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 innych stosownych podmiotów lub źródeł.

5. W razie potrzeby Komisja przedkłada odpowiednie wnioski przewidujące zmianę niniejszego rozporządzenia, uwzględniając w szczególności rozwój technologii informacyjnych oraz postęp w społeczeństwie informacyjnym.

Artykuł 98

Przegląd innych aktów prawnych Unii dotyczących ochrony danych

Komisja przedkłada w stosownym przypadku wnioski ustawodawcze dotyczące zmiany innych aktów prawnych Unii dotyczących ochrony danych osobowych, aby zapewnić jednolitą i spójną ochronę osób fizycznych w związku z przetwarzaniem. Dotyczy to w szczególności przepisów o ochronie osób fizycznych w związku z przetwarzaniem przez instytucje, organy i jednostki organizacyjne Unii oraz o swobodnym przepływie danych osobowych.

Artykuł 99

Wejście w życie i stosowanie

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

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

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

Sporządzono w Brukseli dnia 27 kwietnia 2016 r.

W imieniu Parlamentu Europejskiego	*W imieniu Rady*
M. SCHULZ	J.A. HENNIS-PLASSCHAERT
Przewodniczący	*Przewodniczący*