ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2018/1725

z dnia 23 października 2018 r.

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

(Tekst mający znaczenie dla EOG)

PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ,

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

uwzględniając wniosek Komisji Europejskiej,

po przekazaniu projektu aktu ustawodawczego parlamentom narodowym,

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

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą ([2]),

a także mając na uwadze, co następuje:

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

(2) W rozporządzeniu (WE) nr 45/2001 Parlamentu Europejskiego i Rady ([3]) zapewnia się osobom fizycznym prawnie egzekwowalne prawa, określa się zobowiązania administratorów w instytucjach i organach wspólnotowych odnoszące się do przetwarzania danych osobowych oraz tworzy się niezależny organ nadzorczy, Europejskiego Inspektora Ochrony Danych, odpowiedzialny za monitorowanie przetwarzania danych osobowych przez instytucje i organy Unii. Rozporządzenie to nie ma jednak zastosowania do przetwarzania danych osobowych w toku prowadzenia przez instytucje i organy Unii działalności nieobjętej zakresem stosowania prawa Unii.

(3) W dniu 27 kwietnia 2016 r. przyjęto rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 ([4]) i dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/680 ([5]). W wyżej wymienionym rozporządzeniu określa się przepisy ogólne dotyczące ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i zapewnienia swobodnego przepływu danych osobowych w Unii, natomiast we wspomnianej dyrektywie określa się przepisy szczegółowe dotyczące ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i zapewnienia swobodnego przepływu danych osobowych w Unii w dziedzinach współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej.

(4) W rozporządzeniu (UE) 2016/679 dokonano dostosowania rozporządzenia (WE) nr 45/2001 w celu zapewnienia solidnych i spójnych ram ochrony danych w Unii oraz umożliwienia ich stosowania równocześnie z rozporządzeniem (UE) 2016/679.

(5) Z myślą o spójnym podejściu do ochrony danych osobowych w całej Unii oraz swobodnego przepływu danych osobowych na terytorium Unii należy w miarę możliwości dostosować przepisy o ochronie danych dotyczące instytucji, organów i jednostek organizacyjnych Unii z przepisami o ochronie danych przyjętymi w odniesieniu do sektora publicznego w państwach członkowskich. Zgodnie z orzecznictwem Trybunału Sprawiedliwości Unii Europejskiej (zwanego dalej „Trybunałem Sprawiedliwości"), w każdym przypadku, w którym przepisy niniejszego

([1]) Dz.U. C 288 z 31.8.2017, s. 107.

([2]) Stanowisko Parlamentu Europejskiego z dnia 13 września 2018 r. (dotychczas nieopublikowane w Dzienniku Urzędowym) oraz decyzja Rady z dnia 11 października 2018 r.

([3]) 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.

([4]) 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) (Dz.U. L 119 z 4.5.2016, s. 1).

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

rozporządzenia opierają się na tych samych założeniach, co przepisy rozporządzenia (UE) 2016/679, przepisy obu aktów należy interpretować tak samo, w szczególności ze względu na fakt, że systematyka niniejszego rozporządzenia powinna być uznawana za tożsamą z systematyką rozporządzenia (UE) 2016/679.

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

(7) Aby zapobiec poważnemu ryzyku obchodzenia prawa, ochrona osób fizycznych powinna być neutralna pod względem technicznym i nie powinna zależeć od stosowanych technik.

(8) Niniejsze rozporządzenie powinno mieć zastosowanie do przetwarzania danych osobowych przez wszystkie instytucje, organy i jednostki organizacyjne Unii. Niniejsze rozporządzenie powinno mieć zastosowanie do przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany oraz do przetwarzania w sposób inny niż zautomatyzowany danych osobowych stanowiących lub mających stanowić część zbioru danych. Zbiory lub zestawy zbiorów oraz ich strony tytułowe, które nie są uporządkowane według określonych kryteriów, nie powinny być objęte zakresem niniejszego rozporządzenia.

(9) W deklaracji nr 21 w sprawie ochrony danych osobowych w dziedzinie współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej – załączonej do Aktu końcowego konferencji międzyrządowej, która przyjęła Traktat z Lizbony – konferencja uznała, że ze względu na szczególny charakter współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej konieczne może okazać się przyjęcie, na podstawie art. 16 TFUE, szczególnych przepisów o ochronie danych osobowych i swobodnym przepływie danych osobowych w tych dziedzinach. Osobny rozdział niniejszego rozporządzenia zawierający przepisy ogólne powinien mieć zatem zastosowanie do przetwarzania operacyjnych danych osobowych, takich jak dane osobowe przetwarzane na potrzeby postępowań prowadzonych przez organy lub jednostki organizacyjne Unii wykonujące czynności w dziedzinie współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej.

(10) Dyrektywa (UE) 2016/680 określa zharmonizowane zasady ochrony i swobodnego przepływu danych osobowych przetwarzanych do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania lub ścigania czynów zabronionych, lub wykonywania kar, w tym do celów ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom. Aby zapewnić identyczny stopień ochrony osób fizycznych w całej Unii za pomocą prawnie wykonalnych praw oraz zapobiegać rozbieżnościom utrudniającym wymianę danych osobowych między organami i jednostkami organizacyjnymi Unii, gdy wykonują one czynności wchodzące w zakres stosowania części trzeciej tytuł V rozdział 4 lub rozdział 5 TFUE, a właściwymi organami, przepisy dotyczące ochrony i swobodnego przepływu operacyjnych danych osobowych przetwarzanych przez tego rodzaju organy i jednostki organizacyjne Unii powinny być spójne z dyrektywą (UE) 2016/680.

(11) Przepisy ogólne odrębnego rozdziału niniejszego rozporządzenia dotyczące przetwarzania operacyjnych danych osobowych powinny mieć zastosowanie z zastrzeżeniem przepisów szczegółowych mających zastosowanie do przetwarzania operacyjnych danych osobowych przez organy i jednostki organizacyjne Unii podczas wykonywania przez nie czynności wchodzących w zakres części trzeciej tytuł V rozdział 4 lub rozdział 5 TFUE. Te przepisy szczegółowe należy postrzegać jako *lex specialis* w stosunku do przepisów zawartych w osobnym rozdziale niniejszego rozporządzenia dotyczących przetwarzania operacyjnych danych osobowych (*lex specialis derogat legi generali*). Aby zmniejszyć fragmentaryzację przepisów, szczegółowe przepisy dotyczące ochrony danych mające zastosowanie do przetwarzania operacyjnych danych osobowych przez organy i jednostki organizacyjne Unii przy wykonywaniu przez nie czynności wchodzących w zakres części trzeciej tytuł V rozdział 4 lub rozdział 5 TFUE powinny być spójne z zasadami leżącymi u podstaw rozdziału niniejszego rozporządzenia dotyczącego przetwarzania operacyjnych danych osobowych, a także z przepisami niniejszego rozporządzenia odnoszącymi się do niezależnego nadzoru, środków ochrony prawnej, odpowiedzialności i sankcji.

(12) Rozdział niniejszego rozporządzenia dotyczący przetwarzania operacyjnych danych osobowych powinien mieć zastosowanie do organów i jednostek organizacyjnych Unii przy wykonywaniu przez nie czynności wchodzących w zakres części trzeciej tytuł V rozdział 4 lub rozdział 5 TFUE – niezależnie od tego, czy wykonują one te czynności w ramach zadań głównych czy dodatkowych – do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania lub ścigania przestępstw. Nie powinien mieć on jednak zastosowania do Europolu oraz Prokuratury Europejskiej do chwili, gdy akty prawne ustanawiające Europol i Prokuraturę Europejską zostaną zmienione w celu objęcia ich dostosowanym rozdziałem niniejszego rozporządzenia dotyczącym przetwarzania operacyjnych danych osobowych.

(13) Komisja powinna dokonać przeglądu niniejszego rozporządzenia, w szczególności jego rozdziału dotyczącego przetwarzania operacyjnych danych osobowych. Komisja powinna również dokonać przeglądu innych aktów prawnych przyjętych w oparciu o Traktaty, które to akty regulują przetwarzanie operacyjnych danych osobowych

przez organy i jednostki organizacyjne Unii podczas wykonywania przez nie czynności wchodzących w zakres części trzeciej tytuł V rozdział 4 lub rozdział 5 TFUE. Aby zapewnić jednolitą i spójną ochronę osób fizycznych w odniesieniu do przetwarzania danych osobowych, po przeprowadzeniu wspomnianego przeglądu, Komisja powinna mieć możliwość przedstawienia odnośnych wniosków ustawodawczych, w tym niezbędnych dostosowań rozdziału niniejszego rozporządzenia dotyczącego operacyjnych danych osobowych, z myślą o zastosowaniu tego rozdziału do Europolu i Prokuratury Europejskiej. Dostosowania te powinny uwzględniać przepisy odnoszące się do niezależnego nadzoru, środków ochrony prawnej, odpowiedzialności i sankcji.

(14) Przetwarzanie administracyjnych danych osobowych, takich jak dane pracowników organów i jednostek organizacyjnych Unii przy wykonywaniu przez nie czynności wchodzących w zakres części trzeciej tytuł V rozdział 4 i rozdział 5 TFUE, powinno być objęte zakresem niniejszego rozporządzenia.

(15) Niniejsze rozporządzenie powinno mieć zastosowanie do przetwarzania danych osobowych przez instytucje, organy lub jednostki organizacyjne Unii przy wykonywaniu przez nie czynności wchodzących w zakres tytułu V rozdział 2 Traktatu o Unii Europejskiej (TUE). Niniejsze rozporządzenie nie powinno mieć zastosowania do przetwarzania danych osobowych przez misje, o których mowa w art. 42 ust. 1, art. 43 i 44 TUE, służące realizacji wspólnej polityki bezpieczeństwa i obrony. W stosownych przypadkach należy przedstawić odpowiednie wnioski w celu dalszego uregulowania przetwarzania danych osobowych w dziedzinie wspólnej polityki bezpieczeństwa i obrony.

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

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

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

(19) Zgoda powinna być wyrażona w drodze jednoznacznej, potwierdzającej czynności, która wyraża odnoszące się do określonej sytuacji dobrowolne, świadome i jednoznaczne przyzwolenie osoby, której dane dotyczą, na przetwarzanie dotyczących jej danych osobowych i która ma na przykład formę pisemnego (w tym elektronicznego) lub ustnego oświadczenia. Może to polegać na zaznaczeniu okienka wyboru podczas przeglądania strony internetowej, na wyborze ustawień technicznych do korzystania z usług społeczeństwa informacyjnego lub też na innym oświadczeniu, lub 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 zapytanie elektroniczne, zapytanie takie musi być jasne, zwięzłe i nie może niepotrzebnie zakłócać korzystania z usługi, której dotyczy. Jednocześnie osoba, której dane dotyczą, powinna mieć prawo do wycofania zgody w dowolnym momencie, co nie powinno mieć wpływu na legalność przetwarzania danych, które odbyło się na podstawie zgody przed jej wycofaniem. 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, i dlatego jest mało prawdopodobne, by w tej konkretnej sytuacji zgodę wyrażono dobrowolnie we wszystkich przypadkach. 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.

(20) Wszelkie przetwarzanie danych osobowych powinno być zgodne z prawem i rzetelne. Dla osób fizycznych powinno być jasne, że dotyczące ich dane osobowe są zbierane, wykorzystywane, przeglądane lub w inny sposób przetwarzane oraz w jakim stopniu te dane osobowe są lub będą przetwarzane. Zasada przejrzystości wymaga, by wszelkie informacje i wszelkie komunikaty związane z przetwarzaniem tych danych osobowych były łatwo dostępne i zrozumiałe oraz sformułowane jasnym i prostym językiem. Zasada ta dotyczy w szczególności informowania osób, których dane dotyczą, o tożsamości administratora i celach przetwarzania oraz innych informacji mających zapewnić rzetelność i przejrzystość przetwarzania w stosunku do osób fizycznych, których sprawa dotyczy, a także prawa tych osób do uzyskania potwierdzenia i informacji o przetwarzanych danych osobowych ich dotyczących. Osobom fizycznym należy uświadomić ryzyko, zasady, zabezpieczenia i prawa związane z przetwarzaniem danych osobowych oraz sposoby wykonywania praw przysługujących im w związku z przetwarzaniem tych danych. 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 jest niezbędne do celów, dla których są one przetwarzane. Wymaga to w szczególności zapewnienia ograniczenia do ścisłego minimum okresu przechowywania danych. 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 lub do sprzętu służącego ich przetwarzaniu, przed nieuprawnionym korzystaniem z tych danych lub z tego sprzętu oraz ochronę przed ich nieuprawnionym ujawnieniem w trakcie ich przekazywania.

(21) Zgodnie z zasadą rozliczalności, jeżeli instytucje i organy Unii przekazują dane osobowe w obrębie danej instytucji lub danego organu Unii, a odbiorca nie należy do struktur administratora, lub do innych instytucji lub organów Unii, powinny one sprawdzić, czy tego rodzaju dane osobowe są niezbędne do zgodnego z prawem wykonywania zadań należących do kompetencji odbiorcy. W szczególności po otrzymaniu od odbiorcy wniosku o przekazanie danych osobowych administrator powinien sprawdzić, czy istnieje odpowiednia podstawa do zgodnego z prawem przetwarzania danych osobowych, których dotyczy wniosek, oraz powinien sprawdzić kompetencje odbiorcy. Powinien również dokonać wstępnej oceny konieczności przekazania danych. Jeżeli pojawią się wątpliwości co do tej konieczności, administrator powinien zażądać dalszych informacji od odbiorcy. Odbiorca powinien zapewnić możliwość zweryfikowania konieczności przekazania danych po jego dokonaniu.

(22) Aby przetwarzanie danych osobowych było zgodne z prawem, musi być ono podyktowane koniecznością wykonania zadania realizowanego w interesie publicznym przez instytucje i organy Unii lub w ramach sprawowania przez nie władzy publicznej, koniecznością poszanowania obowiązku prawnego, któremu podlega administrator, lub inną uzasadnioną podstawą na mocy niniejszego rozporządzenia, w tym zgodą osoby, której dane dotyczą, lub koniecznością poszanowania umowy, której stroną jest osoba, której dane dotyczą, lub w celu podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy. Przetwarzanie danych osobowych w celu przeprowadzenia czynności wykonywanych w interesie ogólnym przez instytucje i organy Unii obejmuje przetwarzanie danych osobowych niezbędnych do zarządzania tymi instytucjami i organami oraz ich funkcjonowania. Przetwarzanie danych osobowych należy uznać za zgodne z prawem również w przypadkach, gdy jest niezbędne do ochrony interesu, który ma istotne znaczenie dla życia osoby, której dane dotyczą, lub innej osoby fizycznej. Żywotny interes innej osoby fizycznej powinien zasadniczo być podstawą przetwarzania danych osobowych wyłącznie w przypadkach, gdy przetwarzania tego nie da się w sposób ewidentny 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.

(23) Prawo Unii, o którym mowa w niniejszym rozporządzeniu, powinno być jasne i precyzyjne, a jego zastosowanie przewidywalne dla osób mu podlegających zgodnie z wymogami Karty i Konwencji o ochronie praw człowieka i podstawowych wolności.

(24) Przepisy wewnętrzne, o których mowa w niniejszym rozporządzeniu, powinny być jasne i określać akty o charakterze ogólnym mające na celu wywołanie skutków prawnych wobec osób, których dane dotyczą. Powinny one być przyjęte na najwyższym szczeblu kierownictwa instytucji i organów Unii, w ramach ich kompetencji i w sprawach dotyczących ich funkcjonowania. Powinny one być publikowane w *Dzienniku Urzędowym Unii Europejskiej*. Zastosowanie tych przepisów powinno być przewidywalne dla osób, których przepisy te dotyczą, zgodnie z wymogami Karty oraz Konwencji o ochronie praw człowieka i podstawowych wolności. Przepisy wewnętrzne mogą mieć formę decyzji, w szczególności gdy zostały przyjęte przez instytucje unijne.

(25) 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 inna podstawa prawna niż ta, na podstawie której możliwe było zebranie danych osobowych. Jeżeli przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi, prawo Unii może określać i precyzować zadania i cele, dla których dalsze przetwarzanie powinno być uznawane za zgodne z prawem i z pierwotnymi celami. Dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych, lub do celów statystycznych powinno być uznawane za operacje przetwarzania zgodne z prawem i z pierwotnymi celami. Podstawa prawna przetwarzania danych osobowych w prawie Unii może być również podstawą prawną dalszego przetwarzania. Aby ustalić, czy cel dalszego przetwarzania danych osobowych jest zgodny z celem, w którym dane te zostały pierwotnie zebrane, administrator – po spełnieniu wszystkich wymogów warunkujących zgodność pierwotnego przetwarzania z prawem – powinien uwzględnić między innymi: wszelkie powiązania pomiędzy tymi celami a celami zamierzonego dalszego przetwarzania; kontekst, w którym zostały zebrane dane osobowe, w szczególności rozsądne oczekiwania osób, których dane dotyczą, co do dalszego wykorzystania tych 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.

(26) 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, lub nie może odmówić ani wycofać zgody bez niekorzystnych konsekwencji.

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

(28) Jeżeli odbiorcy mający siedzibę w Unii, inni niż instytucje i organy Unii, chcą, aby instytucje i organy Unii przekazywały im dane osobowe, powinni oni wykazać, że dane te są im potrzebne do wykonania ich zadań prowadzonych w interesie publicznym lub w ramach sprawowania powierzonej im władzy publicznej. Ewentualnie odbiorcy ci powinni dowieść, że przekazanie danych jest niezbędne dla określonego celu w interesie publicznym, a administrator powinien ustalić, czy istnieje jakikolwiek powód, by przypuszczać, że może zostać naruszony uzasadniony interes osoby, której dane dotyczą. W takim przypadku administrator powinien wyraźnie wyważyć różne przeciwstawne interesy, aby dokonać oceny proporcjonalności wnioskowanego przekazania danych

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

osobowych. Taki określony cel w interesie publicznym może dotyczyć przejrzystości instytucji i organów Unii. Ponadto instytucje i organy Unii powinny wykazać taką konieczność, jeżeli same inicjują przekazywanie, zgodnie z zasadą przejrzystości i dobrej administracji. Wymogi określone w niniejszym rozporządzeniu dotyczące przekazywania danych do odbiorców mających siedzibę w Unii, innych niż instytucje i organy Unii, powinny być rozumiane jako uzupełniające w stosunku do warunków zgodnego z prawem przetwarzania.

(29) 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 zagrożenie dla podstawowych praw i wolności. Takie dane osobowe nie powinny być przetwarzane, jeżeli nie zostaną spełnione szczególne warunki określone w niniejszym rozporządzeniu. Do takich danych osobowych powinny zaliczać się dane osobowe ujawniające pochodzenie rasowe lub etniczne, przy czym użycie w niniejszym rozporządzeniu terminu „pochodzenie rasowe" nie oznacza, że Unia akceptuje teorie sugerujące istnienie odrębnych ras ludzkich. Przetwarzanie fotografii nie powinno zawsze stanowić przetwarzania szczególnych kategorii danych osobowych, gdyż fotografie są objęte definicją „danych biometrycznych" tylko w przypadkach, gdy są przetwarzane specjalnymi metodami technicznymi, umożliwiającymi jednoznaczną identyfikację osoby fizycznej lub potwierdzenie jej tożsamości. Oprócz wymogów szczegółowych mających zastosowanie do przetwarzania danych objętych szczególną ochroną 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.

(30) Szczególne kategorie danych osobowych zasługujące na większą ochronę powinny być przetwarzane do celów zdrowotnych wyłącznie wtedy, gdy jest to konieczne do realizacji tych celów z korzyścią dla osób fizycznych i ogółu społeczeństwa, zwłaszcza w kontekście zarządzania usługami i systemami opieki zdrowotnej i zabezpieczenia społecznego. Niniejsze rozporządzenie powinno zatem przewidywać zharmonizowane warunki przetwarzania szczególnych kategorii danych osobowych dotyczących zdrowia ze względu na szczególne potrzeby, zwłaszcza gdy takie dane są przetwarzane w określonych celach zdrowotnych przez osoby podlegające prawnemu obowiązkowi zachowania tajemnicy zawodowej. W prawie Unii powinno się uwzględnić konkretne i odpowiednie środki, aby chronić prawa podstawowe i dane osobowe osób fizycznych.

(31) Przetwarzanie szczególnych kategorii danych osobowych bez zgody osoby, której dane dotyczą, może być niezbędne z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego. 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 usług 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.

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

(33) 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

([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).

celów badań naukowych lub historycznych, lub do celów statystycznych można prowadzić, jeżeli administrator ocenił możliwość realizacji tych celów w drodze przetwarzania danych, 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). Instytucje i organy Unii powinny ustanowić odpowiednie zabezpieczenia w odniesieniu do przetwarzania danych osobowych do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych, lub do celów statystycznych przewidzianych w prawie Unii, które mogą obejmować przepisy wewnętrzne przyjęte przez instytucje i organy Unii w sprawach dotyczących ich funkcjonowania.

(34) Należy przewidzieć procedury ułatwiające osobie, której dane dotyczą, wykonywanie praw przysługujących jej na mocy niniejszego rozporządzenia, w tym mechanizmy żądania i, w stosownych przypadkach, uzyskiwania nieodpłatnie 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, a najpóźniej w terminie miesiąca, zaś jeżeli nie zamierza spełnić takiego żądania – podać tego przyczyny.

(35) 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 danych 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 ogólny zarys zamierzonego przetwarzania. Jeżeli znaki te są przedstawione elektronicznie, powinny nadawać się do odczytu maszynowego.

(36) Informacje o przetwarzaniu danych osobowych odnoszące się do 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, przy ujawnieniu danych temu odbiorcy po raz pierwszy. Jeżeli administrator planuje przetwarzać dane osobowe w celu innym niż cel, w którym dane osobowe zostały zebrane, powinien on przed dalszym przetwarzaniem poinformować osobę, której dane dotyczą, o innym celu przetwarzania oraz dostarczyć jej inne niezbędne informacje. Jeżeli osobie, której dane dotyczą, nie można podać pochodzenia danych osobowych, ponieważ korzystano z różnych źródeł, informacje należy przedstawić w sposób ogólny.

(37) 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 zgodności z prawem 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 zawartych w odnoszącej się do nich dokumentacji medycznej zawierającej takie informacje, jak diagnozy, 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 na temat celów, w jakich dane osobowe są przetwarzane, w miarę możliwości okresu, przez jaki dane osobowe są przetwarzane, odbiorców danych osobowych, założeń ewentualnego zautomatyzowanego przetwarzania danych osobowych oraz, przynajmniej w przypadku profilowania, konsekwencji takiego przetwarzania. Prawo to nie powinno negatywnie wpływać na prawa lub wolności innych osób, w tym tajemnice handlowe lub własność intelektualną, w szczególności na prawa autorskie chroniące oprogramowanie. Względy te nie powinny jednak skutkować odmową udzielenia osobie, której dane dotyczą, jakichkolwiek informacji. Jeżeli administrator przetwarza duże ilości informacji o osobie, której dane dotyczą, powinien on mieć możliwość zażądania przed podaniem informacji, by osoba, której dane dotyczą, sprecyzowała informacje lub czynności przetwarzania, których dotyczy jej żądanie.

(38) Każda osoba fizyczna powinna mieć prawo do sprostowania dotyczących jej danych osobowych oraz prawo do „bycia zapomnianym”, jeżeli zatrzymywanie takich danych narusza niniejsze rozporządzenie lub prawo Unii, któremu podlega administrator. Osoba, której dane dotyczą, powinna mieć prawo do tego, by jej dane osobowe zostały usunięte i przestały być przetwarzane, jeżeli dane te nie są już niezbędne do celów, w których były zbierane lub w inny sposób przetwarzane, jeżeli osoba, której dane dotyczą, cofnęła zgodę lub jeżeli wniosła sprzeciw wobec przetwarzania danych osobowych jej dotyczących, lub jeżeli przetwarzanie jej danych osobowych nie jest z innego powodu zgodne z niniejszym rozporządzeniem. Prawo to ma znaczenie w przypadkach, gdy osoba, której dane

dotyczą, wyraziła zgodę jako dziecko, gdy nie była w pełni świadoma ryzyka związanego z przetwarzaniem, a w późniejszym czasie chce usunąć takie dane osobowe, w szczególności z internetu. Osoba, której dane dotyczą, powinna móc wykonywać to prawo, mimo że już nie jest dzieckiem. Dalsze zatrzymywanie danych osobowych powinno być jednak uznane za zgodne z prawem, jeżeli jest niezbędne do korzystania z wolności wypowiedzi i informacji, do wywiązania się z obowiązku prawnego, do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi, z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego, do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych, lub do celów statystycznych lub do ustalenia, dochodzenia lub obrony roszczeń.

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

(40) 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 za pomocą środków technicznych 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.

(41) 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, które 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 formatów interoperacyjnych, które umożliwiają przenoszenie danych. Prawo to powinno mieć zastosowanie w przypadkach, gdy osoba, której dane dotyczą, przekazała dane osobowe na podstawie własnej zgody lub gdy przetwarzanie jest niezbędne do wykonania umowy. Dlatego nie powinno ono mieć zastosowania w przypadkach, gdy przetwarzanie danych osobowych jest niezbędne do wywiązania się z obowiązku prawnego, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym, lub w ramach sprawowania władzy publicznej powierzonej administratorowi. Przysługujące osobie, której dane dotyczą, prawo do przesłania lub otrzymania swoich danych osobowych nie powinno nakładać na administratorów obowiązku wprowadzenia lub prowadzenia kompatybilnych technicznie systemów przetwarzania. Jeżeli określony zestaw danych osobowych odnosi się do więcej niż jednej osoby, której dane dotyczą, prawo do otrzymania danych osobowych powinno obowiązywać z zastrzeżeniem praw i wolności innych osób, których dane dotyczą, wynikających z niniejszego rozporządzenia. Prawo to powinno ponadto obowiązywać z zastrzeżeniem prawa osoby, której dane dotyczą, do spowodowania, by dane osobowe zostały usunięte oraz z zastrzeżeniem ograniczeń tego prawa określonych w niniejszym rozporządzeniu i nie powinno w szczególności skutkować usunięciem danych osobowych dotyczących osoby, której dane dotyczą, przekazanych przez tę osobę do celów wykonania umowy, o ile te dane osobowe są niezbędne do wykonania tej umowy i w zakresie, w jakim są do tego niezbędne. O ile jest to technicznie możliwe, osoba, której dane dotyczą, powinna mieć prawo do spowodowania, by dane osobowe zostały przekazane przez jednego administratora bezpośrednio innemu administratorowi.

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

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

odnoszące się do efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się osoby, której dane dotyczą, wywołujące skutki prawne względem tej osoby lub w podobny sposób znacząco na nią wpływające.

Niemniej podejmowanie decyzji na podstawie takiego przetwarzania, w tym profilowania, powinno być dozwolone wówczas, gdy jest to wyraźnie dopuszczone prawem Unii. Przetwarzanie takie powinno zawsze podlegać odpowiednim zabezpieczeniom, obejmującym przekazywanie konkretnych informacji osobie, której dane dotyczą, oraz prawo do uzyskania interwencji człowieka, prawo do wyrażenia własnego stanowiska, prawo do uzyskania wyjaśnienia co do decyzji wynikłej z takiej oceny oraz prawo do zakwestionowania takiej decyzji. Takie przetwarzanie nie powinno dotyczyć dzieci. Aby zapewnić rzetelność i przejrzystość przetwarzania wobec osoby, której dane dotyczą, mając na uwadze konkretne okoliczności i kontekst przetwarzania danych osobowych, administrator powinien stosować odpowiednie matematyczne lub statystyczne procedury profilowania, wdrożyć środki techniczne i organizacyjne zapewniające w szczególności korektę czynników powodujących nieprawidłowości w danych osobowych i maksymalne zmniejszenie ryzyka błędów, zabezpieczyć dane osobowe w sposób uwzględniający potencjalne ryzyko dla interesów i praw osoby, której dane dotyczą, oraz zapobiec 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 lub orientację seksualną, lub przetwarzaniu wyników skutkującemu środkami mającymi taki efekt. Zautomatyzowane podejmowanie decyzji i profilowanie oparte na szczególnych kategoriach danych osobowych powinny być dozwolone wyłącznie przy zachowaniu szczególnych warunków.

(44) W aktach prawnych przyjętych na podstawie Traktatów lub w przepisach wewnętrznych przyjętych przez instytucje i organy Unii w sprawach dotyczących ich funkcjonowania można przewidzieć ograniczenia dotyczące określonych zasad oraz prawa do informacji, dostępu do danych osobowych i ich sprostowania lub usuwania, prawa do przenoszenia danych, poufności danych pochodzących z łączności elektronicznej, zawiadamiania osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych oraz ograniczenia dotyczące określonych powiązanych obowiązków administratorów, o ile jest to niezbędne i proporcjonalne w społeczeństwie demokratycznym, dla zapewnienia bezpieczeństwa publicznego, zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, ścigania przestępstw lub wykonywania kar. Obejmuje to ochronę przed zagrożeniami dla bezpieczeństwa publicznego, w tym ochronę życia ludzkiego – w szczególności w odpowiedzi na klęski żywiołowe lub katastrofy spowodowane przez człowieka – i zapobieganie takim zagrożeniom, bezpieczeństwo wewnętrzne instytucji i organów Unii, ochronę innych ważnych celów leżących w ogólnym interesie publicznym Unii lub państwa członkowskiego, w szczególności celów wspólnej polityki zagranicznej i bezpieczeństwa lub ważnego interesu gospodarczego lub finansowego Unii, lub państwa członkowskiego, oraz prowadzenie rejestrów publicznych z uwagi na względy ogólnego interesu publicznego, ochronę osoby, której dane dotyczą, lub praw i wolności innych osób, w tym na rzecz celów w dziedzinie ochrony socjalnej, zdrowia publicznego i celów humanitarnych.

(45) 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.

(46) Ryzyko naruszenia praw lub wolności osób fizycznych, 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 skutkować dyskryminacją, kradzieżą tożsamości lub oszustwem dotyczącym tożsamości, stratą finansową, naruszeniem dobrego imienia, naruszeniem poufności danych osobowych chronionych tajemnicą zawodową, nieuprawnionym odwróceniem pseudonimizacji lub jakąkolwiek inną poważną 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 nimi środków bezpieczeństwa; jeżeli oceniane są czynniki osobowe, w szczególności analizowanie lub prognozowanie aspektów dotyczących efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się, w celu tworzenia lub wykorzystywania profili osobistych; jeżeli przetwarzane są dane osobowe osób wymagających szczególnej opieki, w szczególności dzieci lub jeżeli przetwarzanie dotyczy dużej ilości danych osobowych i wpływa na dużą liczbę osób, których dane dotyczą.

(47) 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.

(48) 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 strategie wewnętrzne i wdrożyć środki, które są zgodne w szczególności z zasadą uwzględniania ochrony danych w fazie projektowania oraz z zasadą domyślnej ochrony danych. Takie środki mogą polegać m.in. na minimalizacji przetwarzania danych osobowych, jak najszybszej pseudonimizacji danych osobowych, przejrzystości co do funkcji i przetwarzania danych osobowych, umożliwieniu osobie, której dane dotyczą, monitorowania przetwarzania danych, umożliwieniu administratorowi tworzenia i doskonalenia zabezpieczeń. Zasadę uwzględniania ochrony danych w fazie projektowania i zasadę domyślnej ochrony danych należy też brać pod uwagę w przetargach publicznych.

(49) Rozporządzenie (UE) 2016/679 przewiduje wykazywanie przestrzegania prawa przez administratorów danych poprzez stosowanie zatwierdzonych mechanizmów certyfikacji. Również instytucje i organy Unii powinny być w stanie wykazać zgodność z wymogami niniejszego rozporządzenia dzięki uzyskaniu certyfikacji zgodnie z art. 42 rozporządzenia (UE) 2016/679.

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

(51) 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 wyłącznie z usług podmiotów przetwarzających, które zapewniają wystarczające gwarancje – w szczególności jeżeli chodzi o wiedzę fachową, wiarygodność i zasoby – wdrożenia środków technicznych i organizacyjnych odpowiadających wymogom niniejszego rozporządzenia, w tym wymogom bezpieczeństwa przetwarzania. Stosowanie zatwierdzonego kodeksu postępowania lub zatwierdzonego mechanizmu certyfikacji przez podmioty przetwarzające inne niż instytucje i organy Unii może posłużyć za element wykazujący wywiązywanie się z obowiązków administratora. Przetwarzanie przez podmiot przetwarzający inny niż instytucja lub organ Unii powinno być regulowane umową lub, w przypadku gdy podmiotem przetwarzającym są instytucje i organy Unii, umową lub innym instrumentem prawnym, które podlegają prawu Unii, 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 uwzględniają konkretne zadania i obowiązki podmiotu przetwarzającego w kontekście planowanego przetwarzania oraz ryzyko naruszenia praw lub wolności osoby, której dane dotyczą. Administrator i podmiot przetwarzający powinni mieć możliwość podjęcia decyzji o skorzystaniu z umowy indywidualnej lub ze standardowych klauzul umownych, które zostały przyjęte albo bezpośrednio przez Komisję, albo przez Europejskiego Inspektora Ochrony Danych, a następnie przyjęte przez Komisję. Po zakończeniu przetwarzania w imieniu administratora podmiot przetwarzający powinien – zgodnie z decyzją administratora – zwrócić lub usunąć dane osobowe, chyba że prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający, nakładają obowiązek przechowywania tych danych osobowych.

(52) Dla zachowania zgodności z niniejszym rozporządzeniem administratorzy powinni prowadzić rejestry czynności przetwarzania, za które są odpowiedzialni, a podmioty przetwarzające – rejestry kategorii czynności przetwarzania, za które są odpowiedzialne. Instytucje i organy Unii powinny być zobowiązane do współpracy z Europejskim Inspektorem Ochrony Danych i na jego żądanie powinny udostępniać mu swoje rejestry w celu monitorowania wspomnianych operacji przetwarzania. Instytucje i organy Unii powinny mieć możliwość ustanowienia centralnego rejestru prowadzonych przez nie czynności przetwarzania, chyba że nie jest to właściwe z uwagi na rozmiar instytucji lub organu Unii. Ze względu na przejrzystość powinny mieć również możliwość publicznego udostępnienia takiego rejestru.

(53) W celu zachowania bezpieczeństwa i zapobiegania przetwarzaniu niezgodnemu z niniejszym rozporządzeniem administrator lub podmiot przetwarzający powinni oszacować ryzyko związane z przetwarzaniem 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 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, które może w szczególności prowadzić do uszczerbku fizycznego, szkód majątkowych lub niemajątkowych.

(54) Instytucje i organy Unii powinny zapewniać poufność łączności elektronicznej zgodnie z art. 7 Karty. Instytucje i organy Unii powinny w szczególności zapewniać bezpieczeństwo swoich sieci łączności elektronicznej. Powinny one chronić informacje mające związek z końcowymi urządzeniami telekomunikacyjnymi użytkowników łączącymi się z dostępnymi publicznie stronami internetowymi i aplikacjami mobilnymi tych instytucji i organów, zgodnie z dyrektywą Parlamentu Europejskiego i Rady 2002/58/WE ([1]). Powinny ponadto chronić dane osobowe przechowywane w spisach użytkowników.

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

(56) 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, aby umożliwić tej osobie podjęcie niezbędnych działań zapobiegawczych. Informacja taka powinna zawierać opis charakteru naruszenia ochrony danych osobowych oraz zalecenia dla danej osoby fizycznej co do minimalizacji potencjalnych niekorzystnych skutków. Informacje należy przekazywać osobom, których dane dotyczą, tak szybko, jak jest to rozsądnie możliwe, w ścisłej współpracy z Europejskim Inspektorem Ochrony Danych, z poszanowaniem wskazówek przekazanych przez ten organ lub inne odpowiednie organy, takie jak organy ścigania.

(57) W rozporządzeniu (WE) nr 45/2001 przewidziano ogólny obowiązek administratora zgłaszania przetwarzania danych osobowych inspektorowi ochrony danych. Inspektor ochrony danych prowadzi rejestr zgłaszanych operacji przetwarzania, chyba że nie jest to właściwe z uwagi na rozmiar instytucji lub organu Unii. Poza tym ogólnym obowiązkiem należy wprowadzić skuteczne procedury i mechanizmy monitorowania operacji przetwarzania, które ze względu na swój charakter, zakres, kontekst i cele mogą powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych. Takie procedury muszą istnieć w szczególności tych w przypadkach, gdy rodzaje operacji przetwarzania wiążą się z użyciem nowych technologii lub są one 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. 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.

(58) 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 Europejskim Inspektorem Ochrony Danych. Takie wysokie ryzyko mogą powodować pewne rodzaje przetwarzania oraz zakres i częstotliwość przetwarzania, które mogą skutkować także szkodą lub ingerencją w prawa i wolności osoby fizycznej. Europejski Inspektor Ochrony Danych powinien odpowiedzieć na wniosek o konsultacje w określonym terminie. Jednak brak reakcji ze strony Europejskiego

([1]) Dyrektywą 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).

Inspektora Ochrony Danych w tym terminie nie powinien wykluczać interwencji Europejskiego Inspektora Ochrony Danych zgodnie z jego zadaniami i uprawnieniami określonymi w niniejszym rozporządzeniu, w tym uprawnieniami do zakazania operacji przetwarzania. W ramach konsultacji powinna istnieć możliwość przedłożenia Europejskiemu Inspektorowi Ochrony Danych wyników oceny skutków dla ochrony danych dokonanej w odniesieniu do danego przetwarzania, a w szczególności środków planowanych w celu zminimalizowania ryzyka naruszenia praw lub wolności osób fizycznych.

(59) Europejski Inspektor Ochrony Danych powinien być informowany o środkach administracyjnych i proszony o opinię na temat przepisów wewnętrznych przyjmowanych przez instytucje i organy Unii w kwestiach dotyczących ich funkcjonowania, w których przewidziały one przetwarzanie danych osobowych, określiły warunki ograniczeń praw osób, których dane dotyczą, lub zapewniły odpowiednie zabezpieczenia praw osób, których dane dotyczą, aby zagwarantować zgodność zamierzonego przetwarzania z niniejszym rozporządzeniem, a w szczególności w zakresie zminimalizowania ryzyka dla osoby, której dane dotyczą.

(60) Rozporządzeniem (UE) 2016/679 ustanowiono Europejską Radę Ochrony Danych jako niezależny organ Unii posiadający osobowość prawną. Europejska Rada Ochrony Danych powinna przyczyniać się do spójnego stosowania przepisów rozporządzenia (UE) 2016/679 i dyrektywy (UE) 2016/680 w całej Unii, m.in. poprzez doradzanie Komisji. Jednocześnie Europejski Inspektor Ochrony Danych powinien w dalszym ciągu wykonywać swoje funkcje nadzorcze i doradcze w odniesieniu do wszystkich instytucji i organów Unii, z inicjatywy własnej lub na wniosek. Aby zapewnić zgodność przepisów o ochronie danych w całej Unii, Komisja powinna dążyć do konsultacji z Europejskim Inspektorem Ochrony Danych podczas opracowywania wniosków lub zaleceń. Komisja powinna mieć obowiązek przeprowadzania konsultacji po przyjęciu aktów ustawodawczych lub podczas opracowywania aktów delegowanych i aktów wykonawczych, o których mowa w art. 289, 290 i 291 TFUE, oraz po przyjęciu zaleceń i wniosków odnoszących się do umów z państwami trzecimi i organizacjami międzynarodowymi, o których mowa w art. 218 TFUE i które mają wpływ na prawo do ochrony danych osobowych. W takich przypadkach Komisja powinna mieć obowiązek skonsultowania się z Europejskim Inspektorem Ochrony Danych, z wyjątkiem przypadków, w odniesieniu do których w rozporządzeniu (UE) 2016/679 przewidziano obowiązek konsultacji z Europejską Radą Ochrony Danych, na przykład w przypadku decyzji stwierdzających odpowiedni stopień ochrony lub aktów delegowanych w sprawie standardowych znaków graficznych i wymogów dotyczących mechanizmów certyfikacji. Ponadto, jeżeli dany akt ma szczególne znaczenie dla ochrony praw i wolności osób fizycznych w zakresie przetwarzania danych osobowych, Komisja powinna mieć możliwość skonsultowania się z Europejską Radą Ochrony Danych. W takich przypadkach Europejski Inspektor Ochrony Danych, jako członek Europejskiej Rady Ochrony Danych, powinien skoordynować swoje prace z pracami rady w celu wydania wspólnej opinii. Europejski Inspektor Ochrony Danych i w stosownych przypadkach Europejska Rada Ochrony Danych powinni przedstawić swoje pisemne zalecenie w terminie ośmiu tygodni. W przypadkach niecierpiącego zwłoki lub w innym uzasadnionym przypadku, na przykład gdy Komisja jest w trakcie prac nad aktami delegowanymi i wykonawczymi, powyższe ramy czasowe należy skrócić.

(61) Zgodnie z art. 75 rozporządzenia (UE) 2016/679 Europejski Inspektor Ochrony Danych zapewnia obsługę sekretariatu Europejskiej Rady Ochrony Danych.

(62) We wszystkich instytucjach i organach Unii inspektor ochrony danych powinien zapewniać stosowanie przepisów niniejszego rozporządzenia oraz doradzać administratorom i podmiotom przetwarzającym w kwestii wypełniania ich zobowiązań. Inspektor powinien być osobą posiadającą wiedzę fachową w zakresie przepisów i praktyk ochrony danych, której poziom należy ustalić w szczególności w świetle prowadzonych przez administratora lub podmiot przetwarzający operacji przetwarzania danych oraz ochrony, której wymagają przetwarzane dane osobowe. Tacy inspektorzy ochrony danych powinni być w stanie wykonywać swoje obowiązki i zadania w sposób niezależny.

(63) Przekazując dane osobowe z instytucji i organów Unii administratorom, podmiotom przetwarzającym lub innym odbiorcom w państwach trzecich lub organizacjom międzynarodowym, należy zagwarantować stopień ochrony osób fizycznych zapewniany w Unii niniejszym rozporządzeniem. Takie same gwarancje powinny mieć zastosowanie 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 odbywać się wyłącznie przy zachowaniu pełnej zgody z niniejszym rozporządzeniem oraz przy poszanowaniu podstawowych praw i wolności zapisanych w Karcie. 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.

(64) Zgodnie z art. 45 rozporządzenia (UE) 2016/679 lub art. 36 dyrektywy (UE) 2016/680 Komisja może uznać, że państwo trzecie, terytorium lub określony sektor w państwie trzecim, lub organizacja międzynarodowa zapewnia odpowiedni stopień ochrony danych. W takich przypadkach przekazywanie danych osobowych do tego państwa trzeciego lub tej organizacji międzynarodowej przez instytucję lub organ Unii może się odbywać bez potrzeby uzyskania dodatkowego zezwolenia.

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

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

(67) Niektóre państwa trzecie przyjmują ustawy, rozporządzenia i inne akty prawne mające bezpośrednio regulować czynności przetwarzania podejmowane przez instytucje i organy Unii. Może to obejmować wyroki sądów lub trybunałów czy decyzje organów administracyjnych państw trzecich nakazujące administratorowi lub podmiotowi przetwarzającemu przekazać lub ujawnić dane osobowe, które nie mają za podstawę umowy międzynarodowej obowiązującej między wzywającym państwem trzecim a Unią. Transgraniczne stosowanie tych ustaw, rozporządzeń i innych aktów prawnych może naruszać prawo międzynarodowe i uniemożliwiać zapewnienie osobom fizycznym ochrony ustanowionej niniejszym rozporządzeniem na terytorium Unii. Przekazywanie danych powinno być dopuszczalne wyłącznie w przypadkach, gdy spełnione są warunki przekazywania do państw trzecich ustanowione w niniejszym rozporządzeniu. Tak może być m.in. w przypadkach, gdy ujawnienie jest niezbędne ze względu na ważny interes publiczny uznany w prawie Unii.

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

(69) Wyjątki te powinny mieć w szczególności zastosowanie do przekazywania danych wymaganego i niezbędnego z uwagi na ważne względy interesu publicznego, na przykład do międzynarodowej wymiany danych między instytucjami i organami Unii a organami ds. konkurencji, organami podatkowymi lub celnymi, organami nadzoru finansowego, służbami odpowiedzialnymi za sprawy zabezpieczenia społecznego lub za zdrowie publiczne, na przykład w przypadku ustalania kontaktów zakaźnych w razie chorób zakaźnych lub w celu zmniejszenia lub wyeliminowania dopingu w sporcie. Przekazywanie danych osobowych należy uznać za zgodne z prawem również

w przypadkach, gdy jest niezbędne w celu ochrony interesu, który ma istotne znaczenie dla żywotnych interesów osoby, której dane dotyczą, lub innej osoby, w tym integralności fizycznej lub życia, jeżeli osoba, której dane dotyczą, nie jest w stanie wyrazić zgody. W razie braku stwierdzenia odpowiedniego stopnia ochrony prawo Unii może z uwagi na ważne względy interesu publicznego wyraźnie nakładać ograniczenia na przekazywanie konkretnych kategorii danych do państwa trzeciego lub organizacji międzynarodowej. Każde przekazanie danych osobowych osoby, której dane dotyczą, fizycznie lub prawnie niezdolnej do wyrażenia zgody, do międzynarodowej organizacji humanitarnej, aby mogła wykonać zadanie nałożone na nią konwencjami genewskimi lub by mogła spełnić wymogi międzynarodowego prawa humanitarnego mającego zastosowanie w konfliktach zbrojnych, można uznać za niezbędne z uwagi na ważny wzgląd interesu publicznego lub za leżące w żywotnym interesie osoby, której dane dotyczą.

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

(71) 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 krajowe organy nadzorcze, jak i Europejski Inspektor Ochrony Danych, mogą nie być w stanie rozpatrzyć skargi lub przeprowadzić postępowania w sprawie działalności, która ma miejsce poza granicami ich jurysdykcji. Ich starania na rzecz współpracy w kontekście transgranicznym mogą także zostać zakłócone przez niewystarczające uprawnienia prewencyjne lub zaradcze, niespójne systemy prawne oraz przeszkody praktyczne, takie jak ograniczone środki. Należy więc upowszechniać ściślejszą współpracę między Europejskim Inspektorem Ochrony Danych a krajowymi organami nadzorującymi ochronę danych, by pomóc im prowadzić wymianę informacji i postępowania z ich odpowiednikami międzynarodowymi.

(72) Utworzenie na mocy rozporządzenia (WE) nr 45/2001 urzędu Europejskiego Inspektora Ochrony Danych, który jest uprawniony do wypełniania swoich zadań i wykonywania swoich uprawnień w sposób całkowicie niezależny, stanowi zasadniczy element ochrony osób fizycznych w związku z przetwarzaniem danych osobowych. Niniejsze rozporządzenie powinno jeszcze bardziej wzmocnić i wyjaśnić rolę i niezależność tego urzędu. Europejski Inspektor Ochrony Danych powinien być osobą, której niezależność jest niekwestionowana i o której wiadomo, że posiada doświadczenie i umiejętności wymagane do pełnienia obowiązków Europejskiego Inspektora Ochrony Danych, ponieważ na przykład należy lub należała do organów nadzorczych ustanowionych na mocy art. 51 rozporządzenia (UE) 2016/679.

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

(74) Aby chronić niezawisłość Trybunału w wykonywaniu zadań sądowych, w tym w procesie decyzyjnym, uprawnienia nadzorcze Europejskiego Inspektora Ochrony Danych nie powinny obejmować przetwarzania danych osobowych przez Trybunał Sprawiedliwości działający jako organ sądowniczy. W przypadku takich operacji przetwarzania Trybunał powinien ustanowić niezależną kontrolę zgodnie z art. 8 ust. 3 Karty, na przykład w formie mechanizmu wewnętrznego.

(75) Decyzje Europejskiego Inspektora Ochrony Danych dotyczące wyjątków, gwarancji, upoważnienia i warunków dotyczących operacji przetwarzania danych zgodnie z definicją niniejszego rozporządzenia powinny być publikowane w sprawozdaniu z działalności. Niezależnie od publikacji rocznego sprawozdania z działalności Europejski Inspektor Ochrony Danych może publikować sprawozdania na konkretne tematy.

(76) Europejski Inspektor Ochrony Danych powinien działać zgodnie z przepisami rozporządzenia (WE) nr 1049/2001 Parlamentu Europejskiego i Rady ([1]).

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

(78) W niektórych przypadkach prawo Unii przewiduje model skoordynowanego nadzoru sprawowanego wspólnie przez Europejskiego Inspektora Ochrony Danych i krajowe organy nadzorcze. Ponadto Europejski Inspektor Ochrony Danych pełni również rolę organu nadzorczego względem Europolu i w tym celu ustanowiono również szczególny model współpracy z krajowymi organami nadzorczymi, który funkcjonuje za pośrednictwem rady współpracy pełniącej funkcje doradcze. Aby poprawić skuteczny nadzór i egzekwowanie przepisów prawa materialnego o ochronie danych, należy wprowadzić w Unii jednolity, spójny model skoordynowanego nadzoru. W związku z tym w stosownych przypadkach Komisja powinna przedłożyć wnioski ustawodawcze w celu zmiany unijnych aktów prawnych, w których przewidziano model skoordynowanego nadzoru, aby dostosować je do skoordynowanego modelu nadzoru przewidzianego w niniejszym rozporządzeniu. Europejska Rada Ochrony Danych powinna funkcjonować jako jednolite forum, aby zapewnić skuteczny i skoordynowany nadzór we wszystkich dziedzinach.

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

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

(81) Aby wzmocnić rolę nadzorczą Europejskiego Inspektora Ochrony Danych i skuteczne wdrażanie przepisów niniejszego rozporządzenia, Europejski Inspektor Ochrony Danych powinien mieć prawo do nakładania administracyjnych kar pieniężnych jako ostatecznej sankcji. Celem kar pieniężnych powinno być ukaranie za nieprzestrzeganie przepisów niniejszego rozporządzenia nie tyle poszczególnych osób, co instytucji lub organów Unii, aby powstrzymać przed kolejnymi naruszeniami niniejszego rozporządzenia i upowszechniać kulturę ochrony danych osobowych wewnątrz instytucji i organów Unii. W niniejszym rozporządzeniu należy wymienić rodzaje naruszeń zagrożonych administracyjnymi karami pieniężnymi oraz wskazać górne granice i kryteria ustalania związanych z nimi kar pieniężnych. Europejski Inspektor Ochrony Danych powinien określać wysokość kar pieniężnych indywidualnie dla każdego przypadku z uwzględnieniem wszystkich stosownych okoliczności danej sytuacji, charakteru, wagi, czasu trwania naruszenia i jego konsekwencji, a także środków podjętych w celu wywiązania się z obowiązków wynikających z niniejszego rozporządzenia oraz w celu zapobieżenia konsekwencjom naruszenia lub ich złagodzenia. Nakładając administracyjną karę pieniężną na instytucję lub organ Unii, Europejski Inspektor Ochrony Danych powinien wziąć pod uwagę proporcjonalność wysokości kary pieniężnej. Procedura administracyjna nakładania kar pieniężnych na instytucje i organy Unii powinna być zgodna z ogólnymi przepisami prawa Unii, w myśl wykładni ustalonej przez Trybunał Sprawiedliwości.

(82) Jeżeli osoba, której dane dotyczą, uzna, że naruszane są jej prawa wynikające z niniejszego rozporządzenia, powinna mieć ona prawo zlecić podmiotowi, organizacji lub zrzeszeniu, które nie mają charakteru zarobkowego, zostały ustanowione zgodnie z prawem Unii lub z prawem państwa członkowskiego, mają statutowo na celu interes publiczny i działają w dziedzinie ochrony danych osobowych, wniesienie skargi w jej imieniu do Europejskiego

([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).

Inspektora Ochrony Danych. Taki organ, organizacja lub zrzeszenie powinny mieć również możliwość wykonywania prawa do środka ochrony prawnej w imieniu osób, których dane dotyczą, lub wykonywania prawa do odszkodowania w imieniu osób, których dane dotyczą.

(83) Urzędnik lub inny pracownik Unii, który nie dopełni zobowiązań wynikających z niniejszego rozporządzenia, podlega karze dyscyplinarnej lub innej zgodnie z regułami i procedurami ustanowionymi w regulaminie pracowniczym urzędników Unii Europejskiej i w warunkach zatrudnienia innych pracowników Unii Europejskiej, ustanowionych w rozporządzeniu Rady (EWG, Euratom, EWWiS) nr 259/68 ([1]) („regulamin pracowniczy").

(84) Aby zapewnić jednolite warunki wdrażania niniejszego rozporządzenia, należy powierzyć Komisji uprawnienia wykonawcze. Uprawnienia te powinny być wykonywane zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 182/2011 ([2]). W przypadku przyjmowania standardowych klauzul umownych między administratorami a podmiotami przetwarzającymi oraz między podmiotami przetwarzającymi, przyjmowania wykazu operacji przetwarzania, jeżeli wymagane są uprzednie konsultacje administratorów dokonujących przetwarzania danych osobowych z Europejskim Inspektorem Ochrony Danych na potrzeby wykonania zadania realizowanego w interesie publicznym, oraz przyjmowania standardowych klauzul umownych zapewniających stosowne gwarancje dla międzynarodowego przekazywania danych należy stosować procedurę sprawdzającą.

(85) Należy chronić informacje poufne, które organy statystyczne Unii i państw członkowskich gromadzą do celów opracowywania oficjalnych statystyk europejskich i krajowych. Statystyki europejskie należy opracowywać, tworzyć i rozpowszechniać zgodnie z zasadami statystycznymi przewidzianymi w art. 338 ust. 2 TFUE. Dalsze szczegółowe informacje o zasadzie poufności odnoszącej się do statystyki europejskiej zawiera rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 223/2009 ([3]).

(86) Należy uchylić rozporządzenie (WE) nr 45/2001 i decyzji nr 1247/2002/WE Parlamentu Europejskiego, Rady i Komisji ([4]). Odesłania do uchylonego rozporządzenia oraz uchylonej decyzji należy rozumieć jako odesłania do niniejszego rozporządzenia.

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

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

(89) Zgodnie z art. 28 ust. 2 rozporządzenia (WE) nr 45/2001 skonsultowano się z Europejskim Inspektorem Ochrony Danych, który wydał opinię w dniu 15 marca 2017 r. ([5]),

---

([1]) Dz.U. L 56 z 4.3.1968, s. 1.

([2]) 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).

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

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

([5]) Dz.U. C 164 z 24.5.2017, s. 2.

PRZYJMUJĄ NINIEJSZE ROZPORZĄDZENIE:

ROZDZIAŁ I

PRZEPISY OGÓLNE

Artykuł 1

Przedmiot i cele

1. W niniejszym rozporządzeniu ustanawia się przepisy o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy Unii oraz przepisy o swobodnym przepływie danych osobowych między nimi lub do odbiorców mających siedzibę w Unii.

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

3. Europejski Inspektor Ochrony Danych monitoruje stosowanie przepisów niniejszego rozporządzenia w odniesieniu do wszystkich operacji przetwarzania przeprowadzanych przez instytucję lub organ Unii.

Artykuł 2

Zakres stosowania

1. Niniejsze rozporządzenie stosuje się do przetwarzania danych osobowych przez wszystkie instytucje i organy Unii.

2. Do przetwarzania operacyjnych danych osobowych przez organy i jednostki organizacyjne Unii przy wykonywaniu przez nie czynności wchodzących w zakres części trzeciej tytuł V rozdział 4 lub 5 TFUE zastosowanie ma wyłącznie art. 3 oraz rozdział IX niniejszego rozporządzenia.

3. Niniejsze rozporządzenie nie ma zastosowania do przetwarzania operacyjnych danych osobowych przez Europol i Prokuraturę Europejską do czasu dostosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/794 ([1]) oraz rozporządzenia Rady (UE) 2017/1939 ([2]) zgodnie z art. 98 niniejszego rozporządzenia.

4. Niniejsze rozporządzenie nie ma zastosowania do przetwarzania danych osobowych przez misje, o których mowa w art. 42 ust. 1, art. 43 i 44 TUE.

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

Artykuł 3

Definicje

Do celów niniejszego rozporządzenia stosuje się następujące definicje:

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) „operacyjne dane osobowe" oznaczają dane osobowe przetwarzane przez organy lub jednostki organizacyjne Unii przy wykonywaniu czynności, które wchodzą w zakres stosowania części trzeciej tytuł V rozdział 4 lub rozdział 5 TFUE, z myślą o osiągnięciu celów i realizacji zadań określonych w aktach prawnych ustanawiających te organy lub jednostki organizacyjne;

([1]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/794 z dnia 11 maja 2016 r. w sprawie Agencji Unii Europejskiej ds. Współpracy Organów Ścigania (Europol), zastępujące i uchylające decyzje Rady 2009/371/WSiSW, 2009/934/WSiSW, 2009/935/WSiSW, 2009/936/WSiSW i 2009/968/WSiSW (Dz.U. L 135 z 24.5.2016. s. 53).

([2]) Rozporządzenie Rady (UE) 2017/1939 z dnia 12 października 2017 r. wdrażające wzmocnioną współpracę w zakresie ustanowienia Prokuratury Europejskiej (Dz.U. L 283 z 31.10.2017, s. 1).

3) „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;

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

5) „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;

6) „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;

7) „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;

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

9) „administratorzy inni, niż instytucje i organy Unii” oznaczają administratorów w rozumieniu art. 4 pkt 7 rozporządzenia (UE) 2016/679 oraz administratorów w rozumieniu art. 3 pkt 8 dyrektywy (UE) 2016/680;

10) „instytucje i organy Unii” oznaczają instytucje, organy i jednostki organizacyjne Unii ustanowione TUE, TFUE lub Traktatem Euratom, lub na ich podstawie;

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

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

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

14) „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;

15) „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;

16) „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;

17) „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;

18) „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;

19) „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;

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

21) „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;

22) „krajowy organ nadzorczy" oznacza niezależny organ publiczny ustanowiony przez państwo członkowskie zgodnie z art. 51 rozporządzenia (UE) 2016/679 lub zgodnie z art. 41 dyrektywy (UE) 2016/680;

23) „użytkownik" oznacza osobę fizyczną korzystającą z sieci lub z końcowego urządzenia telekomunikacyjnego, działających pod kontrolą instytucji lub organu Unii;

24) „spis" oznacza dostępny publicznie spis użytkowników lub wewnętrzny spis użytkowników dostępny w instytucji lub organie Unii, lub wspólny dla instytucji i organów Unii, zarówno w formie drukowanej, jak i elektronicznej.

25) „sieć łączności elektronicznej" oznacza system transmisyjny mogący opierać się na stałej infrastrukturze lub mechanizmie scentralizowanej administracji, a także, w stosownych przypadkach, urządzenia przełączające lub routingowe oraz inne zasoby, w tym nieaktywne elementy sieci, które umożliwiają przekazywanie sygnałów przewodowo, za pomocą radia, środków optycznych lub innych środków elektromagnetycznych, w tym sieci satelitarnych, stacjonarnych (komutowanych i pakietowych, w tym internetu) i naziemnych sieci przenośnych, elektrycznych systemów kablowych, w zakresie, w jakim są one wykorzystywane do przekazywania sygnałów, w sieciach nadawania radiowego i telewizyjnego oraz sieciach telewizji kablowej, niezależnie od rodzaju przekazywanej informacji;

26) „końcowe urządzenie" oznacza końcowe urządzenie określone w art. 1 pkt 1 dyrektywy Komisji 2008/63/WE ([2]).

ROZDZIAŁ II

ZASADY OGÓLNE

Artykuł 4

Zasady dotyczące przetwarzania danych osobowych

1. Dane osobowe muszą być:

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

b) zbierane w konkretnych, wyraźnych i 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. 13 za niezgodne z pierwotnymi celami („ograniczenie celu");

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

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

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

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. 13, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą („ograniczenie przechowywania”);

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

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

Artykuł 5

Zgodność przetwarzania z prawem

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

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

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

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

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

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

2. Podstawa przetwarzania, o którym mowa w ust. 1 lit. a) i b), musi być określona w prawie Unii.

Artykuł 6

Przetwarzanie w innym zgodnym celu

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

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

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

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

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

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

Artykuł 7

Warunki wyrażenia zgody

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

2. Jeżeli osoba, której dane dotyczą, wyraża 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, która stanowi 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 między innymi, czy wykonanie umowy, w tym świadczenie usługi, jest uzależnione od zgody na przetwarzanie danych osobowych, które nie jest niezbędne do wykonania tej umowy.

Artykuł 8

Warunki wyrażenia zgody przez dzieci w przypadku usług społeczeństwa informacyjnego

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

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

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

Artykuł 9

Przekazywanie danych osobowych odbiorcom mającym siedzibę w Unii, innym niż instytucje i organy Unii

1. Bez uszczerbku dla art. 4–6 i 10 dane osobowe przekazuje się odbiorcom mającym siedzibę w Unii innym niż instytucje i organy Unii, wyłącznie jeżeli odbiorca stwierdzi, że:

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

b) przekazanie danych jest niezbędne w określonym celu w interesie publicznym, zaś administrator, w przypadku gdy istnieje jakikolwiek powód, by uznać, że uzasadniony interes osoby, której dane dotyczą, może zostać zagrożony, ustali po wyraźnym dokonaniu oceny różnych przeciwstawnych interesów, że przekazanie danych osobowych w tym określonym celu jest proporcjonalne.

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

3. Instytucje i organy Unii muszą godzić prawo do ochrony danych osobowych z prawem dostępu do dokumentów, zgodnie z prawem Unii.

Artykuł 10

Przetwarzanie szczególnych kategorii danych osobowych

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

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

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

b) przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie zatrudnienia, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem Unii przewidującym 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, 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 podmiot nienastawiony na zysk, który stanowi zintegrowaną jednostkę w ramach instytucji lub organu Unii oraz posiada cele polityczne, światopoglądowe, religijne lub związkowe, pod warunkiem że przetwarzanie dotyczy wyłącznie członków lub byłych członków tego podmiotu lub osób utrzymujących z nim stałe kontakty w związku z jego celami oraz że dane nie są ujawniane poza tym podmiotem bez zgody osób, których dane dotyczą;

e) przetwarzanie dotyczy danych 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 Trybunał Sprawiedliwości;

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

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

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

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

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.

Artykuł 11

Przetwarzanie danych osobowych dotyczących wyroków skazujących i czynów zabronionych

Przetwarzanie danych osobowych dotyczących wyroków skazujących oraz czynów zabronionych lub powiązanych środków bezpieczeństwa na podstawie art. 5 ust. 1 odbywa się wyłącznie pod nadzorem władz publicznych lub jeżeli przetwarzanie jest dozwolone na mocy prawa Unii przewidującego odpowiednie zabezpieczenia praw i wolności osób, których dane dotyczą.

Artykuł 12

Przetwarzanie niewymagające identyfikacji

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

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

Artykuł 13

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

Przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych, lub do celów statystycznych podlega odpowiednim zabezpieczeniom praw i wolności osoby, której dane dotyczą, zgodnie z niniejszym rozporządzeniem. Zabezpieczenia te polegają na wdrożeniu środków technicznych i organizacyjnych, w szczególności aby zapewnić 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 umożliwiają albo przestały umożliwiać zidentyfikować osoby, której dane dotyczą, cele należy realizować w ten sposób.

ROZDZIAŁ III

PRAWA OSOBY, KTÓREJ DANE DOTYCZĄ

SEKCJA 1

przejrzystość oraz tryb korzystania z praw

Artykuł 14

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

1. Administrator podejmuje odpowiednie środki, aby w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem – w szczególności gdy informacje są kierowane do dziecka – udzielić osobie, której dane dotyczą, wszelkich informacji dotyczących przetwarzania, o których mowa w art. 15 i 16, oraz przekazać jej wszelkie komunikaty na ten temat na mocy art. 17–24 i 35. Informacji udziela się na piśmie lub w inny sposób, w tym w stosownych przypadkach – elektronicznie. Jeżeli osoba, której dane dotyczą, tego zażąda, informacji można udzielić ustnie, o ile innymi sposobami potwierdzi się tożsamość osoby, której dane dotyczą.

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

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

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

5. Informacje podawane na mocy art. 15 i 16 oraz wszelkie komunikaty i działania podejmowane na mocy art. 17–24 i 35 są wolne od opłat. Jeżeli żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na ich ustawiczny charakter, administrator może odmówić podjęcia działań w związku z żądaniem. Obowiązek wykazania, że żądanie ma ewidentnie nieuzasadniony lub nadmierny charakter, spoczywa na administratorze.

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

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

8. Jeżeli Komisja przyjmuje akty delegowane zgodnie z art. 12 ust. 8 rozporządzenia (UE) 2016/679, które określają informacje mające zostać przedstawione za pomocą znaków graficznych i procedury ustanowienia standardowych znaków graficznych, instytucje i organy Unii w stosownych przypadkach przekazują informacje zgodnie z art. 15 i 16 niniejszego rozporządzenia w połączeniu z takimi standardowymi znakami graficznymi.

SEKCJA 2

informacje i dostęp do danych osobowych

Artykuł 15

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

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

a) tożsamość i dane kontaktowe administratora;

b) dane kontaktowe inspektora ochrony danych;

c) cele przetwarzania danych osobowych oraz podstawę prawną przetwarzania;

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

e) w stosownych przypadkach informacje o zamiarze przekazania przez administratora danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu przez Komisję odpowiedniego stopnia ochrony lub braku odpowiedniego stopnia ochrony, lub w przypadku przekazania, o którym mowa w art. 48, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii tych zabezpieczeń lub o miejscu ich udostępnienia.

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

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

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

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

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

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

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

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

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

Artykuł 16

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

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

a) tożsamość i dane kontaktowe administratora;

b) dane kontaktowe inspektora ochrony danych;

c) cele przetwarzania danych osobowych oraz podstawę prawną przetwarzania;

d) kategorie odnośnych danych osobowych;

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

f) w stosownych przypadkach – informacje o zamiarze przekazania danych osobowych odbiorcy w państwie trzecim lub organizacji międzynarodowej oraz o stwierdzeniu przez Komisję odpowiedniego stopnia ochrony lub braku odpowiedniego stopnia ochrony, lub w przypadku przekazania, o którym mowa w art. 48, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

c) pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem Unii 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, w tym ustawowym obowiązkiem zachowania tajemnicy.

6. W przypadkach, o których mowa w ust. 5 lit. b), administrator podejmuje odpowiednie środki, by chronić prawa i wolności oraz prawnie uzasadniony interes osoby, której dane dotyczą, w tym przy publicznym udostępnianiu informacji.

Artykuł 17

Prawo dostępu przysługujące osobie, której dane dotyczą

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

a) cele przetwarzania;

b) kategorie odnośnych danych osobowych;

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

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

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

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

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

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

2. Jeżeli dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej, osoba, której dane dotyczą, ma prawo zostać poinformowana o odpowiednich zabezpieczeniach, o których mowa w art. 48, związanych z przekazaniem.

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

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

SEKCJA 3

sprostowanie i usuwanie danych

Artykuł 18

Prawo do sprostowania danych

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

Artykuł 19

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

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

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

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

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

d) dane osobowe były przetwarzane niezgodnie z prawem;

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

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

2. Jeżeli administrator upublicznił dane osobowe, a na mocy ust. 1 ma obowiązek usunąć te dane osobowe, to – biorąc pod uwagę dostępną technologię i koszt realizacji – podejmuje rozsądne działania, w tym środki techniczne, by poinformować administratorów lub administratorów innych, niż instytucje i organy Unii 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. Ustępy 1 i 2 nie mają zastosowania, w zakresie w jakim przetwarzanie jest niezbędne:

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

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

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

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

e) do ustalenia, dochodzenia lub obrony roszczeń.

Artykuł 20

Prawo do ograniczenia przetwarzania

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

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

b) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się 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. 23 ust. 1 wobec przetwarzania – do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie administratora są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.

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

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

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

Artykuł 21

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

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

Artykuł 22

Prawo do przenoszenia danych

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

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

b) przetwarzanie odbywa się w sposób zautomatyzowany.

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

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

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

SEKCJA 4

prawo do sprzeciwu oraz zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach

Artykuł 23

Prawo do sprzeciwu

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

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

3. Bez uszczerbku dla art. 36 i 37 oraz w związku z korzystaniem z usług społeczeństwa informacyjnego, osoba, której dane dotyczą, może wykonać prawo do sprzeciwu za pośrednictwem zautomatyzowanych środków wykorzystujących specyfikacje techniczne.

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

Artykuł 24

Zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach, w tym profilowanie

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

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

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

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

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

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

SEKCJA 5

ograniczenia

Artykuł 25

Ograniczenia

1. Akty prawne przyjęte na podstawie Traktatów lub, w sprawach odnoszących się do działalności instytucji i organów Unii, przepisy wewnętrzne przyjęte przez te instytucje i organy mogą ograniczyć zastosowanie art. 14–22, 35 i 36, a także art. 4 – o ile ich przepisy odpowiadają prawom i obowiązkom przewidzianym w art. 14–22 – jeżeli ograniczenie takie nie narusza istoty podstawowych praw i wolności oraz jest w demokratycznym społeczeństwie środkiem niezbędnym i proporcjonalnym, służącym:

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

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

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

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

e) ochronie niezależności sądów i postępowania sądowego;

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

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

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

i) egzekucji roszczeń cywilnoprawnych.

2. W szczególności wszelkie akty prawne lub przepisy wewnętrzne, o których mowa w ust. 1, zawierają w stosownych przypadkach szczegółowe postanowienia dotyczące:

a) celów lub kategorii przetwarzania;

b) kategorii danych osobowych;

c) zakresu wprowadzonych ograniczeń;

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

e) określenia administratora lub kategorii administratorów;

f) okresów przechowywania oraz mających zastosowanie zabezpieczeń z uwzględnieniem charakteru, zakresu i celów lub kategorii przetwarzania oraz

g) ryzyka naruszenia praw lub wolności osób, których dane dotyczą.

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

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

5. Przepisy wewnętrzne, o których mowa w ust. 1, 3 i 4, powinny mieć formę jasnych i precyzyjnych aktów o zasięgu ogólnym, których celem jest wywarcie skutków prawnych wobec osób, których dane dotyczą, przyjętych na najwyższym szczeblu kierownictwa instytucji i organów Unii i powinny być publikowane w Dzienniku Urzędowym Unii Europejskiej.

6. Jeżeli nałożono ograniczenie zgodnie z ust. 1, osoba, której dane dotyczą, zostaje poinformowana zgodnie z prawem Unii o podstawowych powodach zastosowania ograniczenia oraz przysługującym jej prawie do wniesienia skargi do Europejskiego Inspektora Ochrony Danych.

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

8. Można wstrzymać przekazanie informacji, o których mowa w ust. 6 i 7 niniejszego artykułu oraz w art. 45 ust. 2, pominąć je lub go odmówić, gdyby mogło ono unieważnić skutek ograniczenia nałożonego zgodnie z ust. 1 niniejszego artykułu.

ROZDZIAŁ IV

ADMINISTRATOR I PODMIOT PRZETWARZAJĄCY

SEKCJA 1

obowiązki ogólne

Artykuł 26

Obowiązki administratora

1. Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze, 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 strategii ochrony danych.

3. Wywiązywanie się przez administratora z ciążących na nim obowiązków można wykazać w drodze stosowania zatwierdzonych mechanizmów certyfikacji, o których mowa w art. 42 rozporządzenia (UE) 2016/679.

Artykuł 27

Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych

1. Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz wynikające z przetwarzania ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze, 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 włączenia do procesu przetwarzania 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, można wykazać za pomocą zatwierdzonego mechanizmu certyfikacji określonego w art. 42 rozporządzenia (UE) 2016/679.

Artykuł 28

Współadministratorzy

1. Jeżeli co najmniej dwóch administratorów albo jeden lub większa liczba administratorów wraz z jednym lub większą liczbą administratorów innych, niż instytucje i organy Unii, wspólnie ustalają cele i sposoby przetwarzania, są oni współadministratorami. W drodze wspólnych uzgodnień współadministratorzy w sposób przejrzysty 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 obowiązków administratorów w odniesieniu do podawania informacji, o których mowa w art. 15 i 16, o ile – i w zakresie, w jakim – przypadające im wspólnie obowiązki określa prawo Unii lub prawo państwa członkowskiego, któremu ci współadministratorzy podlegają. W uzgodnieniach można wskazać punkt kontaktowy dla osób, których dane dotyczą.

2. Uzgodnienia, o których mowa w ust. 1, 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 29

Podmiot przetwarzający

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

2. Podmiot przetwarzający nie korzysta z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej zgody pisemnej administratora. W przypadku ogólnej zgody pisemnej 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 aktu 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 akt prawny stanowią w szczególności, że podmiot przetwarzający:

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

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

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

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

e) biorąc pod uwagę charakter przetwarzania, w miarę możliwości pomaga administratorowi przy pomocy odpowiednich środków technicznych i organizacyjnych wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania przysługujących jej praw określonych w rozdziale III;

f) uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga administratorowi wywiązać się z obowiązków określonych w art. 33–41;

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

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

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

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

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

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

7. Komisja może określić standardowe klauzule umowne dotyczące kwestii, o których mowa w ust. 3 i 4 niniejszego artykułu, zgodnie z procedurą sprawdzającą, o której mowa w art. 96 ust. 2.

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

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

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

Artykuł 30

Przetwarzanie z upoważnienia administratora 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 31

Rejestrowanie czynności przetwarzania

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

a) imię i nazwisko lub nazwę oraz dane kontaktowe administratora, inspektora ochrony danych, a także w stosownych przypadkach – podmiotu przetwarzającego i współadministratora;

b) cele przetwarzania;

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

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

e) w stosownych przypadkach – przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej oraz dokumentacja odpowiednich zabezpieczeń;

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

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

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

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

b) kategorie czynności przetwarzania dokonywanych w imieniu każdego z administratorów;

c) w stosownych przypadkach – przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej oraz dokumentacja odpowiednich zabezpieczeń;

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

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

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

5. Instytucja i organ Unii przechowuje swój rejestr czynności przetwarzania w rejestrze centralnym, chyba że nie jest to właściwe z uwagi na rozmiar instytucji lub organu Unii. Udostępniają one rejestr publicznie.

Artykuł 32

Współpraca z Europejskim Inspektorem Ochrony Danych

Na żądanie Europejskiego Inspektora Ochrony Danych instytucje i organy Unii współpracują z nim w zakresie wykonywania jego zadań.

SEKCJA 2

bezpieczeństwo danych osobowych

Artykuł 33

Bezpieczeństwo przetwarzania

1. Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania, a także ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze, 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. Administrator oraz podmiot przetwarzający podejmują działania w celu zapewnienia, że każda osoba fizyczna działająca z upoważnienia administratora lub podmiotu przetwarzającego, która ma dostęp do danych osobowych, nie będzie ich przetwarzała bez polecenia administratora, chyba że wymaga tego od niej prawo Unii.

4. Wywiązywanie się z obowiązków, o których mowa w ust. 1, można wykazać za pomocą zatwierdzonego mechanizmu certyfikacji określonego w art. 42 rozporządzenia (UE) 2016/679.

Artykuł 34

Zgłaszanie naruszenia ochrony danych osobowych Europejskiemu Inspektorowi Ochrony Danych

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

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

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

a) opis charakteru naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazanie kategorii i przybliżonej liczby osób, których dane dotyczą, oraz kategorii i przybliżonej liczby wpisów danych osobowych, których dotyczy naruszenie;

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

c) opis możliwych konsekwencji naruszenia ochrony danych osobowych;

d) opis środków zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środków mających na celu zminimalizowania jego ewentualnych negatywnych skutków.

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

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

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

Artykuł 35

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. 34 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 wystąpienia wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w ust. 1;

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

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

SEKCJA 3

poufność łączności elektronicznej

Artykuł 36

Poufność łączności elektronicznej

Instytucje i organy Unii zapewniają poufność łączności elektronicznej, w szczególności poprzez zabezpieczenie swoich sieci łączności elektronicznej.

Artykuł 37

Ochrona informacji przesyłanych do, przechowywanych w, związanych z, przetwarzanych przez i pobieranych z końcowego urządzenia użytkowników

Instytucje i organy Unii chronią informacje przesyłane do, przechowywane w, związane z, przetwarzane przez i pobierane z końcowych urządzeń użytkowników łączących łączącego się z dostępnymi publicznie stronami internetowymi i aplikacjami mobilnymi tych instytucji i organów zgodnie z art. 5 ust. 3 dyrektywy 2002/58/WE.

Artykuł 38

Spisy użytkowników

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

2. Instytucje i organy Unii podejmują wszelkie niezbędne działania, aby zapobiec wykorzystywaniu danych osobowych zawartych w tych spisach do celów marketingu bezpośredniego, niezależnie od tego, czy dane te są ogólnodostępne czy też nie.

SEKCJA 4

ocena skutków dla ochrony danych i uprzednie konsultacje

Artykuł 39

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.

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

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

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

c) systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.

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

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

6. Przed przyjęciem wykazów, o których mowa w ust. 4 i 5 niniejszego artykułu, Europejski Inspektor Ochrony Danych zwraca się do Europejskiej Rady Ochrony Danych utworzonej na mocy art. 68 rozporządzenia (UE) 2016/679 o zbadanie takich wykazów zgodnie z art. 70 ust. 1 lit. e) tego rozporządzenia, jeżeli takie wykazy odnoszą się do operacji przetwarzania danych przez administratora działającego wspólnie z co najmniej jednym administratorem innym, niż instytucje i organy Unii.

7. Ocena zawiera co najmniej:

a) systematyczny opis planowanych operacji przetwarzania i celów przetwarzania;

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

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

d) przewidziane środki służące zaradzeniu zagrożeniom, w tym zabezpieczenia oraz środki bezpieczeństwa i mechanizmy zapewniające ochronę danych osobowych i potwierdzające zgodność z przepisami niniejszego rozporządzenia, z uwzględnieniem praw i uzasadnionych interesów osób, których dane dotyczą, i innych odnośnych osób.

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

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

10. Jeżeli przetwarzanie na podstawie art. 5 ust. 1 lit. a) lub b) ma podstawę prawną w akcie prawnym przyjętym na podstawie Traktatów, który reguluje daną operację przetwarzania lub zestaw operacji, a ocenę skutków dla ochrony danych sporządzono już w ramach ogólnej oceny skutków regulacji, którą przeprowadzono przed przyjęciem tego aktu prawnego, ust. 1–6 niniejszego artykułu nie mają zastosowania, chyba że ten akt prawny stanowi inaczej.

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 40

Uprzednie konsultacje

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

2. Jeżeli Europejski Inspektor Ochrony Danych jest zdania, że zamierzone przetwarzanie, o którym mowa w ust. 1, stanowiłoby naruszenie niniejszego rozporządzenia – w szczególności gdy administrator niedostatecznie zidentyfikował lub zminimalizował ryzyko – Europejski Inspektor Ochrony Danych w terminie do ośmiu tygodni od wpłynięcia wniosku o konsultacje udziela administratorowi, a w stosownych przypadkach także podmiotowi przetwarzającemu, pisemnej porady 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. Europejski Inspektor Ochrony Danych informuje administratora, a w stosownych przypadkach także podmiot przetwarzający, o takim przedłużeniu w terminie miesiąca od wpłynięcia wniosku o konsultacje, z podaniem przyczyn tego opóźnienia. Bieg tych terminów można zawiesić, do czasu aż Europejski Inspektor Ochrony Danych uzyska wszelkie informacje, których zażądał do celów konsultacji.

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

a) w stosownych przypadkach – odpowiednie obowiązki administratora, współadministratorów oraz podmiotów przetwarzających uczestniczących w przetwarzaniu;

b) cele i sposoby zamierzonego przetwarzania;

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

d) dane kontaktowe inspektora ochrony danych;

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

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

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

SEKCJA 5

informacje i konsultacje w sprawie aktów ustawodawczych

Artykuł 41

Informacje i konsultacje

1. Przy sporządzaniu środków administracyjnych i wewnętrznych przepisów odnoszących się do przetwarzania danych osobowych, w których bierze udział instytucja lub organ Unii, samodzielnie lub wspólnie z innymi, instytucje i organy Unii informują o tym Europejskiego Inspektora Ochrony Danych.

2. Instytucje i organy Unii konsultują się z Europejskim Inspektorem Ochrony Danych podczas sporządzania przepisów wewnętrznych, o których mowa w art. 25.

Artykuł 42

Konsultacje w sprawie aktów ustawodawczych

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

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

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

4. Niniejszy artykuł nie ma zastosowania w przypadku, gdy zgodnie z rozporządzeniem (UE) 2016/679 Komisja ma obowiązek skonsultowania się z Europejską Radą Ochrony Danych.

SEKCJA 6

inspektor ochrony danych

Artykuł 43

Wyznaczenie inspektora ochrony danych

1. Każda instytucja lub organ Unii wyznacza inspektora ochrony danych.

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

3. Inspektor ochrony danych jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełniania zadań, o których mowa w art. 45.

4. Inspektor ochrony danych musi być pracownikiem instytucji lub organu Unii. Biorąc pod uwagę rozmiar instytucji i organów Unii i jeśli nie skorzystano z możliwości, o której mowa w ust. 2, instytucje i organy Unii mogą wyznaczyć inspektora ochrony danych, który wypełnia swoje zadania na podstawie umowy o świadczenie usług.

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

Artykuł 44

Status inspektora ochrony danych

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

2. Instytucje i organy Unii wspierają inspektora ochrony danych w wypełnianiu przez niego zadań, o których mowa w art. 45, zapewniając mu zasoby niezbędne do wykonywania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej.

3. Instytucje i organy Unii 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 podlega bezpośrednio najwyższemu kierownictwu administratora lub podmiotu przetwarzającego.

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

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

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

7. Z inspektorem ochrony danych mogą konsultować się administrator i podmiot przetwarzający, odpowiedni komitet personelu i dowolne osoby w każdej sprawie dotyczącej interpretacji lub stosowania niniejszego rozporządzenia, bez korzystania z kanałów oficjalnych. Nikt nie może doznać uszczerbku z powodu tego, że zwrócił uwagę odpowiedniego inspektora ochrony danych na fakt zarzucanego naruszenia przepisów niniejszego rozporządzenia.

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

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

Artykuł 45

Zadania inspektora ochrony danych

1. Inspektor ochrony danych ma następujące zadania:

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

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

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

d) udzielanie na żądanie porad co do konieczności zgłoszenia lub zawiadomienia o naruszeniu ochrony danych osobowych na podstawie przepisów art. 34 i 35;

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

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

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

h) zapewnianie, by operacje przetwarzania nie wpływały negatywnie na prawa i wolności osób, których dane dotyczą.

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

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

ROZDZIAŁ V

PRZEKAZYWANIE DANYCH OSOBOWYCH DO PAŃSTW TRZECICH LUB ORGANIZACJI MIĘDZYNARODOWYCH

Artykuł 46

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, że nie zostanie naruszony stopień ochrony osób fizycznych zagwarantowany w niniejszym rozporządzeniu.

Artykuł 47

Przekazywanie na podstawie decyzji stwierdzającej odpowiedni stopień ochrony

1. Przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej może nastąpić, gdy Komisja stwierdzi na podstawie art. 45 ust. 3 rozporządzenia (UE) 2016/679 lub art. 36 ust. 3 dyrektywy (UE) 2016/680, że to państwo trzecie, terytorium lub określony sektor lub określone sektory w tym państwie trzecim, lub dana organizacja międzynarodowa zapewniają odpowiedni stopień ochrony, i gdy dane osobowe są przekazywane jedynie po to, aby umożliwić wykonywanie zadań wchodzących w zakres kompetencji administratora.

2. Instytucje i organy Unii informują Komisję i Europejskiego Inspektora Ochrony Danych o przypadkach, kiedy uważają, że dane państwo trzecie, terytorium lub określony sektor lub określone sektory w tym państwie trzecim lub dana organizacja międzynarodowa nie zapewniają odpowiedniego stopnia ochrony w rozumieniu ust. 1.

3. Instytucje i organy Unii podejmują niezbędne środki na potrzeby zapewnienia zgodności z decyzjami wydanymi przez Komisję stwierdzającymi, czy zgodnie z art. 45 ust. 3 lub 5 rozporządzenia (UE) 2016/679 lub art. 36 ust. 3 lub 5 dyrektywy (UE) 2016/680 państwo trzecie, terytorium lub określony sektor lub określone sektory w tym państwie trzecim lub organizacja międzynarodowa zapewnia odpowiedni stopień ochrony lub czy już go nie zapewnia.

Artykuł 48

Przekazywanie z zastrzeżeniem odpowiednich zabezpieczeń

1. W razie braku decyzji na podstawie art. 45 ust. 3 rozporządzenia (UE) 2016/679 lub art. 36 ust. 3 dyrektywy (UE) 2016/680 administrator lub podmiot przetwarzający mogą przekazać dane osobowe do państwa trzeciego lub organizacji międzynarodowej wyłącznie, gdy zapewnią odpowiednie zabezpieczenia, i pod warunkiem że obowiązują egzekwowalne prawa osób, których dane dotyczą, i skuteczne środki ochrony prawnej.

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

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

b) standardowych klauzul ochrony danych przyjętych przez Komisję zgodnie z procedurą sprawdzającą, o której mowa w art. 96 ust. 2;

c) standardowych klauzul ochrony danych przyjętych przez Europejskiego Inspektora Ochrony Danych i zatwierdzonych przez Komisję zgodnie z procedurą sprawdzającą, o której mowa w art. 96 ust. 2;

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

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

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

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

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

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

Artykuł 49

Przekazywanie lub ujawnianie niedozwolone na mocy prawa Unii

Wyrok sądu lub trybunału oraz decyzja organu administracji państwa trzeciego wymagająca od administratora lub podmiotu przetwarzającego przekazania lub ujawnienia danych osobowych może zostać uznana lub być egzekwowalna wyłącznie, gdy opiera się na umowie międzynarodowej, takiej jak umowa o wzajemnej pomocy prawnej, obowiązującej między wzywającym państwem trzecim a Unią, z zastrzeżeniem innych podstaw przekazania na mocy niniejszego rozdziału.

Artykuł 50

Wyjątki w szczególnych sytuacjach

1. W razie braku decyzji stwierdzającej odpowiedni stopień ochrony określonej w art. 45 ust. 3 rozporządzenia (UE) 2016/679 lub art. 36 ust. 3 dyrektywy (UE) 2016/680, lub braku odpowiednich zabezpieczeń określonych w art. 48 niniejszego rozporządzenia, jednorazowe lub wielokrotne przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej następuje wyłącznie pod warunkiem że:

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

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

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

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

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

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

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

2. Ustęp 1 lit. a), b) i c) nie mają zastosowania do działalności prowadzonej przez instytucje i organy Unii w ramach wykonywania przysługujących im uprawnień publicznych.

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

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

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

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

Artykuł 51

Międzynarodowa współpraca na rzecz ochrony danych osobowych

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

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

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

c) włączenia odnośnych podmiotów w dyskusję i działania mające na celu upowszechnianie współpracy międzynarodowej w dziedzinie egzekwowania przepisów o ochronie danych osobowych;

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

ROZDZIAŁ VI

EUROPEJSKI INSPEKTOR OCHRONY DANYCH

Artykuł 52

Europejski Inspektor Ochrony Danych

1. Niniejszym ustanawia się urząd Europejskiego Inspektora Ochrony Danych.

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

3. Europejski Inspektor Ochrony Danych jest odpowiedzialny za monitorowanie i zapewnienie stosowania przepisów niniejszego rozporządzenia i każdego innego aktu Unii odnoszącego się do podstawowych praw i wolności osób fizycznych w odniesieniu do przetwarzania danych osobowych przez instytucje i organy Unii oraz za doradzanie instytucjom i organom Unii i osobom, których dane dotyczą, we wszystkich kwestiach związanych z przetwarzaniem danych osobowych. W tym celu Europejski Inspektor Ochrony Danych realizuje zadania przewidziane w art. 57 i korzysta z uprawnień nadanych w art. 58.

4. Rozporządzenie (WE) nr 1049/2001 ma zastosowanie do dokumentów znajdujących się w posiadaniu Europejskiego Inspektora Ochrony Danych. Europejski Inspektor Ochrony Danych przyjmuje szczegółowe zasady stosowania rozporządzenia (WE) nr 1049/2001 w odniesieniu do tych dokumentów.

Artykuł 53

Powoływanie Europejskiego Inspektora Ochrony Danych

1. Parlament Europejski i Rada powołują Europejskiego Inspektora Ochrony Danych w drodze wspólnego porozumienia na okres pięciu lat na podstawie listy ustalonej przez Komisję po ogłoszeniu publicznego naboru dla kandydatów. Nabór kandydatów umożliwia złożenie wniosków zainteresowanym osobom w całej Unii. Lista kandydatów ustalona przez Komisję jest publikowana i figuruje na niej co najmniej trzech kandydatów. Na podstawie listy ustalonej przez Komisję właściwa komisja Parlamentu Europejskiego może podjąć decyzję o przeprowadzeniu przesłuchania, aby móc wyrazić swe preferencje.

2. Na liście kandydatów, o której mowa w ust. 1, znajdują się osoby, których niezależność jest niekwestionowana i o których wiadomo, że mają wiedzę fachową w dziedzinie ochrony danych, a także doświadczenie i umiejętności wymagane do pełnienia obowiązków Europejskiego Inspektora Ochrony Danych.

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

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

a) jeżeli Europejski Inspektor Ochrony Danych zostaje zastąpiony;

b) jeżeli Europejski Inspektor Ochrony Danych zrezygnuje z urzędu;

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

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

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

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

Artykuł 54

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

1. Europejskiego Inspektora Ochrony Danych traktuje się na równi z sędzią Trybunału Sprawiedliwości w odniesieniu do ustalania wysokości wynagrodzenia, dodatków, świadczenia emerytalnego i innych świadczeń w miejsce wynagrodzenia.

2. Władza budżetowa zapewnia, aby Europejski Inspektor Ochrony Danych otrzymał zasoby ludzkie i finansowe konieczne do wykonania jego zadań.

3. Budżet Europejskiego Inspektora Ochrony Danych uwzględnia się w odrębnej pozycji budżetu w sekcji regulującej wydatki administracyjne budżetu ogólnego Unii.

4. Europejskiego Inspektora Ochrony Danych wspomaga sekretariat. Urzędników i innych pracowników sekretariatu powołuje Europejski Inspektor Ochrony Danych, który jest ich przełożonym. Działają oni pod jego wyłącznym kierownictwem. Ich liczba jest ustalana każdego roku w ramach procedury budżetowej. Artykuł 75 ust. 2 rozporządzenia (UE) 2016/679 stosuje się do personelu Europejskiego Inspektora Ochrony Danych uczestniczącego w wykonywaniu zadań, które na mocy prawa Unii powierza się Europejskiej Radzie Ochrony Danych.

5. Urzędnicy i inny pracownicy sekretariatu Europejskiego Inspektora Ochrony Danych podlegają zasadom i przepisom mającym zastosowanie do urzędników i innych pracowników Unii.

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

Artykuł 55

Niezależność

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

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

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

4. Po zakończeniu swojej kadencji Europejski Inspektor Ochrony Danych jest zobowiązany do postępowania godnie i rozważnie w odniesieniu do przyjmowania stanowisk i korzyści.

Artykuł 56

Tajemnica zawodowa

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

Artykuł 57

Zadania

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

a) monitoruje i egzekwuje stosowanie przepisów niniejszego rozporządzenia przez instytucje lub organy Unii, z wyjątkiem przetwarzania danych osobowych przez Trybunał Sprawiedliwości działający jako władza sądownicza;

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

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

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

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

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

g) doradza, z własnej inicjatywy lub na wniosek, wszystkim instytucjom i organom Unii w sprawie prawnych i administracyjnych środków ochrony praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych;

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

i) przyjmuje standardowe klauzule umowne, o których mowa w art. 29 ust. 8 i w art. 48 ust. 2 lit. c);

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

k) uczestniczy w działaniach Europejskiej Rady Ochrony Danych;

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

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

n) zatwierdza klauzule umowne i przepisy, o których mowa w art. 48 ust. 3;

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

p) wypełnia inne zadania związane z ochroną danych osobowych oraz

q) uchwala swój regulamin wewnętrzny.

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

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

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

Artykuł 58

Uprawnienia

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

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

b) prowadzenie postępowań w formie audytów ochrony danych;

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

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

e) uzyskiwanie dostępu do wszystkich pomieszczeń administratora i podmiotu przetwarzającego, w tym do sprzętu i środków służących do przetwarzania danych, zgodnie z prawem unijnym.

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

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

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

c) przekazanie sprawy do administratora lub podmiotu przetwarzającego i w razie konieczności do Parlamentu Europejskiego, Rady i Komisji;

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

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

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

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

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

i) zastosowanie administracyjnej kary pieniężnej na mocy art. 66 w razie niewykonania przez instytucję lub organ Unii co najmniej jednego ze środków, o których mowa w lit. d)–h) i j), zależnie od okoliczności konkretnej sprawy;

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

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

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

b) udzielanie porad administratorowi zgodnie z procedurą uprzednich konsultacji, o której mowa w art. 40, oraz zgodnie z art. 41 ust. 2;

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

d) przyjmowanie standardowych klauzul ochrony danych, o których mowa w art. 29 ust. 8 i art. 48 ust. 2 lit. c);

e) zatwierdzanie klauzul umownych, o których mowa w art. 48 ust. 3 lit. a);

f) zatwierdzanie uzgodnień administracyjnych, o których mowa w art. 48 ust. 3 lit. b);

g) zezwalanie zgodnie z aktami wykonawczymi przyjętymi na podstawie art. 40 ust. 4.

4. Europejski Inspektor Ochrony Danych ma prawo przekazać sprawę do Trybunału Sprawiedliwości zgodnie z warunkami przewidzianymi w Traktach oraz interweniować w sprawach wniesionych do Trybunału Sprawiedliwości.

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

Artykuł 59

Obowiązek administratorów i podmiotów przetwarzających reagowania na skargi

Jeżeli Europejski Inspektor Ochrony Danych wykonuje uprawnienia przewidziane w art. 58 ust. 2 lit. a), b) i c), administrator lub podmiot przetwarzający informuje Europejskiego Inspektora Ochrony Danych o swojej opinii w odpowiednim czasie określonym przez Europejskiego Inspektora Ochrony Danych, uwzględniając okoliczności każdej sprawy. Odpowiedź powinna zawierać opis podjętych środków, jeżeli takie zostały podjęte, w odpowiedzi na uwagi Europejskiego Inspektora Ochrony Danych.

Artykuł 60

Sprawozdanie z działalności

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

2. Europejski Inspektor Ochrony Danych przekazuje sprawozdanie, o którym mowa w ust. 1, innym instytucjom i organom Unii, które mogą dołączyć komentarze, mając na względzie możliwe badanie sprawozdania w Parlamencie Europejskim.

ROZDZIAŁ VII

WSPÓŁPRACA I SPÓJNOŚĆ

Artykuł 61

Współpraca między Europejskim Inspektorem Ochrony Danych a krajowymi organami nadzorczymi

Europejski Inspektor Ochrony Danych współpracuje z krajowymi organami nadzorczymi, a także ze wspólnym organem nadzorczym utworzonym na mocy art. 25 decyzji Rady 2009/917/WSiSW ([1]) w zakresie niezbędnym do wykonywania odnośnych obowiązków tych organów, w szczególności poprzez wzajemne przekazywanie istotnych informacji, wzajemne wezwania do wykonywania ich uprawnień i odpowiadanie na wzajemne wezwania.

Artykuł 62

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

1. Jeżeli w danym akcie Unii zamieszczono odwołanie do niniejszego artykułu, Europejski Inspektor Ochrony Danych i krajowe organy nadzorcze, każdy w zakresie swoich kompetencji, czynnie współpracują w ramach swoich obowiązków, aby zapewnić skuteczny nadzór nad wielkoskalowymi systemami informatycznymi oraz organami i jednostkami organizacyjnymi Unii.

2. W zależności od potrzeb, działając w zakresie swoich odnośnych kompetencji i w ramach swoich obowiązków, prowadzą one wymianę odnośnych informacji, pomagają sobie wzajemnie w przeprowadzaniu audytów i inspekcji, badają trudności w interpretacji lub stosowaniu niniejszego rozporządzenia i innych mających zastosowanie aktów Unii, analizują problemy związane z prowadzeniem niezależnego nadzoru lub korzystaniem z praw przez osoby, których dane dotyczą, sporządzają zharmonizowane wnioski dotyczące rozwiązań wszelkich problemów oraz propagują wiedzę na temat praw do ochrony danych.

3. Do celów określonych w ust. 2 Europejski Inspektor Ochrony Danych i krajowe organy nadzorcze spotykają się co najmniej dwa razy w roku w ramach Europejskiej Rady Ochrony Danych. Do tych celów Europejska Rada Ochrony Danych może w zależności od potrzeb opracować dalsze metody pracy.

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

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

ROZDZIAŁ VIII

ŚRODKI OCHRONY PRAWNEJ, ODPOWIEDZIALNOŚĆ I SANKCJE

Artykuł 63

Prawo do wniesienia skargi do Europejskiego Inspektora Ochrony Danych

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

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

3. Jeżeli Europejski Inspektor Ochrony Danych nie rozpatrzy skargi lub w ciągu trzech miesięcy nie poinformuje osoby, której dane dotyczą, o postępach i efektach rozpatrywania skargi, przyjmuje się, że Europejski Inspektor Ochrony Danych wydał decyzję odmowną.

Artykuł 64

Prawo do skutecznego środka ochrony prawnej

1. Trybunał Sprawiedliwości jest właściwy do rozstrzygania sporów odnoszących się do przepisów niniejszego rozporządzenia, w tym dotyczących roszczeń odszkodowawczych.

2. Odwołania od decyzji Europejskiego Inspektora Ochrony Danych, w tym decyzji, o których mowa w art. 63 ust. 3, wnosi się do Trybunału Sprawiedliwości.

3. Trybunał Sprawiedliwości ma nieograniczoną jurysdykcję w zakresie kontroli administracyjnych kar pieniężnych, o których mowa w art. 66. Trybunał Sprawiedliwości może obniżyć lub podwyższyć wysokość tych kar w granicach określonych w art. 66 bądź je uchylić.

Artykuł 65

Prawo do odszkodowania

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

Artykuł 66

Administracyjne kary pieniężne

1. Europejski Inspektor Ochrony Danych może nakładać administracyjne kary pieniężne na instytucje i organy Unii – w zależności od okoliczności w poszczególnych przypadkach – w sytuacji gdy instytucja lub organ Unii nie zastosują się do poleceń Europejskiego Inspektora Ochrony Danych na podstawie art. 58 ust. 2 lit. d)–h) i j). W czasie podejmowania decyzji o nałożeniu administracyjnej kary pieniężnej oraz ustalania jej wysokości w każdym indywidualnym przypadku szczególną uwagę zwraca się na:

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

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

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

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

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

f) kategorie danych osobowych, których dotyczyło naruszenie;

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

h) przestrzeganie środków, o których mowa w art. 58, zastosowanych wcześniej w tej samej sprawie wobec instytucji lub organu Unii, których sprawa dotyczy. Procedurę, która prowadzi do nałożenia tych kar pieniężnych, przeprowadza się w rozsądnych ramach czasowych po uwzględnieniu okoliczności sprawy i właściwych czynności i procedur, o których mowa w art. 69.

2. Zgodnie z ust. 1 niniejszego artykułu naruszenia obowiązków instytucji lub organu Unii, o których to obowiązkach mowa w art. 8, 12, 27–35, 39, 40, 43, 44 i 45, podlegają administracyjnym karom pieniężnym w wysokości do 25 000 EUR za jedno naruszenie i do wysokości łącznej kwoty 250 000 EUR rocznie.

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

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

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

c) przekazywania danych osobowych odbiorcy w państwie trzecim lub organizacji międzynarodowej, o którym to przekazywaniu mowa w art. 46–50.

4. Jeżeli instytucja lub organ Unii wielokrotnie naruszają w ramach tych samych, powiązanych lub stałych operacji przetwarzania kilka przepisów lub ten sam przepis niniejszego rozporządzenia, całkowita wysokość administracyjnej kary pieniężnej nie przekracza wysokości kary za najpoważniejsze naruszenie.

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

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

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

Artykuł 67

Reprezentowanie osób, których dane dotyczą

Osoba, której dane dotyczą, ma prawo umocować podmiot, organizację lub zrzeszenie – które nie mają charakteru zarobkowego, zostały ustanowione zgodnie z prawem Unii lub prawem państwa członkowskiego, mają cele statutowe leżące w interesie publicznym i działają w dziedzinie ochrony praw i wolności osób, których dane dotyczą, w związku z ochroną ich danych osobowych – do wniesienia w jej imieniu skargi do Europejskiego Inspektora Ochrony Danych oraz wykonywania w jej imieniu praw, o których mowa w art. 63 i 64, oraz żądania w jej imieniu odszkodowania, o którym mowa w art. 65.

Artykuł 68

Skargi pracowników Unii

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

Artykuł 69

Kary

W przypadku, gdy urzędnik lub inny pracownik Unii nie dopełnieni obowiązków określonych w niniejszym rozporządzeniu, umyślne czy nieumyślne, ten urzędnik lub inny pracownik, podlega karze dyscyplinarnej lub innej karze zgodnie z przepisami i procedurami ustanowionymi w regulaminie pracowniczym.

ROZDZIAŁ IX

PRZETWARZANIE OPERACYJNYCH DANYCH OSOBOWYCH PRZEZ ORGANY IJEDNOSTKI ORGANIZACYJNE UNII PODCZAS WYKONYWANIA PRZEZ NIE CZYNNOŚCI WCHODZĄCYCH W ZAKRES CZĘŚCI TRZECIEJ TYTUŁ V ROZDZIAŁ 4 LUB ROZDZIAŁ 5 TFUE

Artykuł 70

Zakres rozdziału

Niniejszy rozdział stosuje się jedynie do przetwarzania operacyjnych danych osobowych przez organy i jednostki organizacyjne Unii prowadzące działania, które wchodzą w zakres stosowania części trzeciej tytuł V rozdział 4 lub rozdział 5 TFUE, z zastrzeżeniem szczegółowych przepisów dotyczących ochrony danych mających zastosowanie do takich organów lub jednostek organizacyjnych Unii.

Artykuł 71

Zasady dotyczące przetwarzania operacyjnych danych osobowych

1. Operacyjne dane osobowe są:

a) przetwarzane zgodnie z prawem i rzetelnie („zgodność z prawem i rzetelność”);

b) gromadzone w konkretnych, wyraźnych i uzasadnionych celach i nieprzetwarzane w sposób niezgodny z tymi celami („zasada celowości”);

c) adekwatne, stosowne i nienadmierne w stosunku do celów, w których są przetwarzane („minimalizacja danych”);

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

e) przechowywane w postaci umożliwiającej identyfikację osób, których dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których operacyjne dane osobowe są przetwarzane („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. Przetwarzanie przez tego samego lub innego administratora w jednym z celów określonych w akcie prawnym ustanawiającym organ lub jednostkę organizacyjną Unii innym niż cel, dla którego operacyjne dane osobowe zostały zebrane, jest dozwolone, o ile:

a) administrator jest uprawniony do przetwarzania takich operacyjnych danych osobowych w takim celu na mocy prawa Unii; oraz

b) przetwarzanie jest niezbędne i proporcjonalne do tego innego celu na mocy prawa Unii.

3. Przetwarzanie przez tego samego lub innego administratora może obejmować archiwizację w interesie publicznym, wykorzystanie do celów naukowych, statystycznych lub historycznych, o których mowa w akcie prawnym ustanawiającym organ lub jednostkę organizacyjną Unii, o ile podlega ono odpowiednim zabezpieczeniom praw i wolności osób, których dane dotyczą.

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

Artykuł 72

Zgodność z prawem przetwarzania operacyjnych danych osobowych

1. Przetwarzanie operacyjnych danych osobowych jest zgodne z prawem wyłącznie wówczas i w zakresie, w jakim takie przetwarzanie jest niezbędne do wykonania zadań realizowanych przez organy i jednostki organizacyjne Unii wykonujące czynności, które wchodzą w zakres stosowania części trzeciej tytuł V rozdział 4 lub rozdział 5 TFUE, i opiera się na prawie Unii.

2. Szczególne akty prawne Unii regulujące przetwarzanie w zakresie stosowania tego rozdziału określają co najmniej cele przetwarzania, operacyjne dane osobowe mające podlegać przetwarzaniu, powody przetwarzania oraz okresy przechowywania operacyjnych danych osobowych lub okresowego przeglądu potrzeby dalszego przechowywania operacyjnych danych osobowych.

Artykuł 73

Rozróżnianie poszczególnych kategorii osób, których dane dotyczą

Administrator – w stosownym przypadku i w miarę możliwości – wyraźnie rozróżnia operacyjne dane osobowe poszczególnych kategorii osób, których dane dotyczą, takie jak kategorie wymienione w aktach prawnych ustanawiających organy i jednostki organizacyjne Unii.

Artykuł 74

Rozróżnianie poszczególnych rodzajów operacyjnych danych osobowych i weryfikacja jakości operacyjnych danych osobowych

1. Administrator dokonuje, w miarę możliwości, rozróżnienia pomiędzy operacyjnymi danymi osobowymi opartymi na faktach a operacyjnymi danymi osobowymi opartymi na indywidualnych ocenach.

2. Administrator podejmuje wszelkie rozsądne działania w celu zapewnienia, by nieprawidłowe, niekompletne lub nieaktualne operacyjne dane osobowe nie były przesyłane ani udostępniane. W tym celu – w miarę możliwości i w stosownych przypadkach – administrator sprawdza jakość operacyjnych danych osobowych przed ich przesłaniem lub udostępnieniem, na przykład konsultując się z właściwym organem, z którego dane pochodzą. W miarę możliwości, we wszystkich przypadkach przesyłania operacyjnych danych osobowych administrator dodaje niezbędne informacje pozwalające odbiorcy ocenić stopień prawidłowości, kompletności i wiarygodności operacyjnych danych osobowych oraz stopień ich aktualności.

3. Jeżeli okaże się, że przesłano nieprawidłowe operacyjne dane osobowe lub że operacyjne dane osobowe przesłano niezgodnie z prawem, należy o tym niezwłocznie powiadomić odbiorcę. W takim przypadku odnośne operacyjne dane osobowe należy sprostować lub usunąć, lub ograniczyć ich przetwarzanie zgodnie z art. 82.

Artykuł 75

Szczególne warunki przetwarzania

1. Jeżeli unijne prawo mające zastosowanie do administratora przesyłającego dane przewiduje szczególne warunki przetwarzania danych, administrator informuje odbiorcę takich operacyjnych danych osobowych o tych warunkach i o obowiązku ich przestrzegania.

2. Administrator spełnia szczególne warunki przetwarzania przewidziane przez właściwy przesyłający organ zgodnie z art. 9 ust. 3 i 4 dyrektywy (UE) 2016/680.

Artykuł 76

Przetwarzanie szczególnych kategorii operacyjnych danych osobowych

1. Przetwarzanie operacyjnych danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, lub przynależność do związków zawodowych oraz przetwarzanie danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej, operacyjnych danych osobowych dotyczących zdrowia lub dotyczących seksualności bądź orientacji seksualnej osoby fizycznej jest dozwolone wyłącznie wtedy, jeżeli jest bezwzględnie niezbędne do celów operacyjnych i wchodzi w zakres mandatu danego organu lub jednostki organizacyjnej Unii i podlega odpowiednim zabezpieczeniom praw i wolności osoby, której dane dotyczą. Zabrania się dyskryminacji osób fizycznych na podstawie takich danych osobowych.

2. Inspektor ochrony danych jest informowany bez zbędnej zwłoki o zastosowaniu niniejszego artykułu.

Artykuł 77

Zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach, w tym profilowanie

1. Decyzje opierające się wyłącznie na zautomatyzowanym przetwarzaniu, w tym również na profilowaniu, i mające niekorzystne skutki prawne dla osoby, której dane dotyczą, lub poważnie na nią wpływające są zakazane, chyba że dopuszcza je prawo Unii, któremu podlega administrator i które przewiduje odpowiednie zabezpieczenia praw i wolności osoby, której dane dotyczą, przynajmniej prawo do uzyskania interwencji ludzkiej ze strony administratora.

2. Decyzje, o których mowa w ust. 1 niniejszego artykułu, nie mogą opierać się na szczególnych kategoriach danych osobowych, o których mowa w art. 76, chyba że istnieją właściwe środki ochrony praw, wolności i uzasadnionych interesów osoby, której dane dotyczą.

3. Profilowanie skutkujące dyskryminacją osób fizycznych na podstawie szczególnych kategorii danych osobowych, o których mowa w art. 76, jest zabronione zgodnie z prawem Unii.

Artykuł 78

Komunikacja oraz metody wykonywania praw osób, których dane dotyczą

1. Administrator podejmuje rozsądne działania, aby udzielić osobie, której dane dotyczą, wszelkich informacji, o których mowa w art. 79, oraz prowadzi z nią wszelką komunikację, o której mowa w art. 80–84 i 92 w sprawie przetwarzania w zwięzłej, zrozumiałej i łatwo dostępnej formie, przy użyciu jasnego i prostego języka. Informacji udziela się wszelkimi stosownymi sposobami, w tym elektronicznie. Co do zasady administrator udziela informacji w takiej samej formie, w jakiej wniesiono żądanie.

2. Administrator ułatwia osobie, której dane dotyczą, wykonanie praw przysługujących jej na mocy art. 79–84.

3. Administrator bez zbędnej zwłoki, a w każdym razie nie później niż w terminie trzech miesięcy od otrzymania żądania od osoby, której dane dotyczą, informuje pisemnie tę osobę o działaniach podjętych w związku z tym żądaniem.

4. Administrator zapewnia, aby informacje przekazywane na mocy art. 79 oraz wszelka komunikacja i wszelkie działania podjęte na mocy art. 80–84 i 92 były wolne od opłat. Jeżeli żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, administrator może odmówić podjęcia działań w związku z żądaniem. Obowiązek wykazania, że żądanie ma ewidentnie nieuzasadniony lub nadmierny charakter, spoczywa na administratorze.

5. Jeżeli administrator ma uzasadnione wątpliwości co do tożsamości osoby fizycznej składającej wniosek, o którym mowa w art. 80 lub 82, może zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby, której dane dotyczą.

Artykuł 79

Informacje udostępniane lub przekazywane osobie, której dane dotyczą

1. Administrator udostępnia osobie, której dane dotyczą, przynajmniej następujące informacje:

a) nazwę i dane kontaktowe organu lub jednostki organizacyjnej Unii;

b) dane kontaktowe inspektora ochrony danych;

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

d) informacje o prawie do wniesienia skargi do Europejskiego Inspektora Ochrony Danych i jego dane kontaktowe;

e) informacje o prawie do występowania do administratora z wnioskiem o dostęp do operacyjnych danych osobowych osoby, której dane dotyczą, ich sprostowania lub usunięcia, lub ograniczenia ich przetwarzania.

2. Oprócz informacji, o których mowa w ust. 1, w konkretnych przypadkach przewidzianych w prawie unijnym administrator przekazuje osobie, której dane dotyczą, następujące dalsze informacje umożliwiające korzystanie z przysługujących jej praw:

a) podstawa prawna przetwarzania;

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

c) w stosownych przypadkach kategorie odbiorców operacyjnych danych osobowych, w tym odbiorców w państwach trzecich lub organizacjach międzynarodowych;

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

3. Administrator może opóźnić, ograniczyć lub pominąć przekazywanie osobie, której dane dotyczą, informacji przewidzianych w ust. 2, w takim zakresie i przez taki okres, w jakim odnośny środek jest działaniem koniecznym i proporcjonalnym w społeczeństwie demokratycznym – przy uwzględnieniu praw podstawowych i uzasadnionych interesów danej osoby fizycznej – aby:

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

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

c) chronić bezpieczeństwo publiczne państw członkowskich;

d) chronić bezpieczeństwo narodowe państw członkowskich;

e) chronić prawa i wolności innych osób, takich jak ofiary i świadkowie.

Artykuł 80

Prawo dostępu przysługujące osobie, której dane dotyczą

Osoba, której dane dotyczą, jest uprawniona do uzyskania od administratora potwierdzenia, czy przetwarzane są operacyjne dane osobowe jej dotyczące, a jeżeli ma to miejsce – do uzyskania dostępu do operacyjnych danych osobowych oraz do następujących informacji:

a) cele i podstawa prawna przetwarzania;

b) kategorie odnośnych operacyjnych danych osobowych;

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

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

e) informacje o prawie do złożenia do administratora wniosku o sprostowanie lub usunięcie operacyjnych danych osobowych lub ograniczenie przetwarzania operacyjnych danych osobowych dotyczących tej osoby;

f) informacje o prawie do wniesienia skargi do Europejskiego Inspektora Ochrony Danych i jego dane kontaktowe;

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

Artykuł 81

Ograniczenia prawa dostępu

1. Administrator może ograniczyć w całości lub w części prawo dostępu osoby, której dane dotyczą, w takim zakresie i przez taki okres, w jakim takie częściowe lub całkowite ograniczenie jest działaniem niezbędnym i proporcjonalnym w społeczeństwie demokratycznym – przy uwzględnieniu praw podstawowych i uzasadnionych interesów danej osoby fizycznej – aby:

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

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

c) chronić bezpieczeństwo publiczne państw członkowskich;

d) chronić bezpieczeństwo narodowe państw członkowskich;

e) chronić prawa i wolności innych osób, takich jak ofiary i świadkowie.

2. W przypadkach, o których mowa w ust. 1, administrator bez zbędnej zwłoki informuje na piśmie osobę, której dane dotyczą, o każdej odmowie lub o każdym ograniczeniu dostępu i o przyczynach tej odmowy lub tego ograniczenia. Informacje takie można pominąć, jeżeli ich udzielenie godziłoby w którykolwiek z celów, o których mowa w ust. 1. Administrator informuje osobę, której dane dotyczą, o możliwości wniesienia skargi do Europejskiego Inspektora Ochrony Danych lub środka ochrony prawnej do Trybunału Sprawiedliwości. Administrator dokumentuje faktyczne lub prawne podstawy decyzji. Informacje te są udostępniane Europejskiemu Inspektorowi Ochrony Danych na jego wniosek.

Artykuł 82

Prawo do sprostowania lub usunięcia operacyjnych danych osobowych oraz ograniczenia ich przetwarzania

1. Osoba, której dane dotyczą, ma prawo uzyskać od administratora bez zbędnej zwłoki sprostowanie jej operacyjnych danych osobowych, jeżeli są nieprawidłowe. Z uwzględnieniem celów przetwarzania, osoba, której dane dotyczą, ma prawo uzyskania uzupełnienia niekompletnych operacyjnych danych osobowych, w tym w drodze przedstawienia dodatkowego oświadczenia.

2. Administrator bez zbędnej zwłoki usuwa operacyjne dane osobowe, a osoba, której dane dotyczą, ma prawo uzyskać od administratora usunięcie bez zbędnej zwłoki jej operacyjnych danych osobowych, w przypadku gdy ich przetwarzanie stanowi naruszenie art. 71, art. 72 ust. 1 lub art. 76 lub gdy operacyjne dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego, któremu podlega administrator.

3. Zamiast usunięcia, administrator ogranicza przetwarzanie, jeżeli:

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

b) dane osobowe muszą zostać zachowane do celów dowodowych.

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

Dane, do których dostęp ograniczono, można przetwarzać wyłącznie w celu, ze względu na który ich usunięcie nie było możliwe.

4. Administrator informuje na piśmie osobę, której dane dotyczą, o każdej odmowie sprostowania lub usunięcia danych osobowych lub ograniczenia przetwarzania danych oraz o przyczynach tej odmowy. Administrator może w całości lub w części ograniczyć udzielanie takich informacji, jeżeli takie ograniczenie jest działaniem niezbędnym i proporcjonalnym w społeczeństwie demokratycznym – przy uwzględnieniu praw podstawowych i uzasadnionych interesów danej osoby fizycznej – aby:

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

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

c) chronić bezpieczeństwo publiczne państw członkowskich;

d) chronić bezpieczeństwo narodowe państw członkowskich;

e) chronić prawa i wolności innych osób, takich jak ofiary i świadkowie.

Administrator informuje osobę, której dane dotyczą, o możliwości wniesienia skargi do Europejskiego Inspektora Ochrony Danych lub środka ochrony prawnej do Trybunału Sprawiedliwości.

5. Administrator informuje o sprostowaniu nieprawidłowych operacyjnych danych osobowych właściwy organ, od którego pochodzą nieprawidłowe operacyjne dane osobowe.

6. W przypadkach sprostowania lub usunięcia operacyjnych danych osobowych lub ograniczenia ich przetwarzania na podstawie ust. 1, 2 lub 3 administrator powiadamia o tym odbiorców i informuje ich, że muszą dokonać sprostowania lub usunięcia operacyjnych danych osobowych, lub ograniczyć przetwarzanie operacyjnych danych osobowych, za które odpowiadają.

Artykuł 83

Prawo dostępu w postępowaniach przygotowawczych i postępowaniach karnych

Jeżeli operacyjne dane osobowe pochodzą od właściwego organu" organy i jednostki organizacyjnej Unii – przed podjęciem decyzji o prawie dostępu osoby, której dane dotyczą – sprawdzają wraz z zainteresowanym właściwym organem, czy takie dane osobowe są ujęte w orzeczeniu sądowym, protokole lub akcie sprawy przetwarzanym w toku postępowania przygotowawczego lub postępowania karnego w państwie członkowskim tego właściwego organu. W takim przypadku decyzja w sprawie prawa dostępu jest podejmowana w porozumieniu i w ścisłej współpracy z zainteresowanym właściwym organem.

Artykuł 84

Wykonywanie praw osoby, której dane dotyczą, i weryfikacja przez Europejskiego Inspektora Ochrony Danych

1. W przypadkach, o których mowa w art. 79 ust. 3, art. 81 i art. 82 ust. 4, osoba, której dane dotyczą, może wykonywać swoje prawa także za pośrednictwem Europejskiego Inspektora Ochrony Danych.

2. Administrator informuje osobę, której dane dotyczą, o możliwości wykonywania przysługujących jej praw za pośrednictwem Europejskiego Inspektora Ochrony Danych na mocy ust. 1.

3. W przypadku wykonywania prawa, o którym mowa w ust. 1, Europejski Inspektor Ochrony Danych informuje osobę, której dane dotyczą, przynajmniej o fakcie przeprowadzenia wszelkich niezbędnych weryfikacji lub przeglądu. Europejski Inspektor Ochrony Danych informuje także osobę, której dane dotyczą, o przysługującym jej prawie do wniesienia środka ochrony prawnej do Trybunału Sprawiedliwości.

Artykuł 85

Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych

1. Uwzględniając stan wiedzy technicznej, koszt wdrożenia oraz charakter, zakres, kontekst i cele przetwarzania, a także wynikające z przetwarzania ryzyko (o różnym prawdopodobieństwie i wadze) naruszenia praw i wolności osób fizycznych, zarówno w czasie określania sposobów przetwarzania, jak i w czasie samego przetwarzania, administrator wdraża odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, które zostały zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, skutecznie oraz w celu zapewnienia niezbędnych zabezpieczeń przy przetwarzaniu, tak by spełnić wymogi niniejszego rozporządzenia i aktu prawnego ustanawiającego tego administratora oraz chronić prawa osób, których dane dotyczą.

2. Administrator wdraża odpowiednie środki techniczne i organizacyjne w celu zapewnienia, że domyślnie przetwarzane będą wyłącznie te operacyjne dane osobowe, które są adekwatne, stosowne i nienadmierne w stosunku do celu przetwarzania. Obowiązek ten odnosi się do ilości gromadzonych operacyjnych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. W szczególności środki te zapewniają, by domyślnie operacyjne dane osobowe nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych.

Artykuł 86

Współadministratorzy

1. Jeżeli co najmniej dwóch administratorów albo jeden lub większa liczba administratorów wraz z jednym lub większą liczbą administratorów innych, niż instytucje i organy Unii, wspólnie ustalają cele i sposoby przetwarzania, są oni współadministratorami. W drodze wspólnych uzgodnień współadministratorzy w przejrzysty sposób określają odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków ochrony danych, w szczególności w odniesieniu do wykonywania przez osobę, której dane dotyczą, przysługujących jej praw, oraz ich obowiązków w odniesieniu do podawania informacji, o których mowa w art. 79, chyba że – i w zakresie, w jakim – 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, odzwierciedlają odpowiednie zakresy obowiązków współadministratorów oraz relacje pomiędzy nimi a osobą, której dane dotyczą. Zasadnicza treść uzgodnień jest udostępniana osobie, której 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 87

Podmiot przetwarzający

1. Jeżeli przetwarzanie ma odbywać się 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 aktu prawnego ustanawiającego administratora oraz 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 aktu 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 operacyjnych danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora. Ta umowa lub inny akt prawny stanowią w szczególności, że podmiot przetwarzający:

a) działa wyłącznie zgodnie z poleceniami administratora;

b) zapewnia, że osoby upoważnione do przetwarzania operacyjnych danych osobowych zobowiążą się do zachowania poufności lub będą podlegały odpowiedniemu ustawowemu obowiązkowi zachowania poufności;

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

d) po zakończeniu świadczenia usług związanych z przetwarzaniem, w zależności od decyzji administratora, usuwa lub zwraca administratorowi wszelkie operacyjne dane osobowe oraz usuwa wszelkie istniejące kopie tych danych, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie operacyjnych danych osobowych;

e) udostępnia administratorowi wszelkie informacje niezbędne do wykazania wywiązywania się z obowiązków ustanowionych w niniejszym artykule;

f) przestrzega warunków, o których mowa w ust. 2 oraz w niniejszym ustępie, dotyczących zaangażowania innego podmiotu przetwarzającego.

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

5. Jeżeli podmiot przetwarzający naruszy niniejsze rozporządzenie lub akt prawny ustanawiający administratora określając cele i sposoby przetwarzania, uznaje się go za administratora w odniesieniu do tego przetwarzania.

Artykuł 88

Ewidencja czynności

1. Administrator prowadzi ewidencję następujących operacji przetwarzania prowadzonych w zautomatyzowanych systemach przetwarzania: zbieranie, modyfikowanie, dostęp, przeglądanie, ujawnianie wraz z przekazywaniem, łączenie i usuwanie operacyjnych danych osobowych. Ewidencja przeglądania i ujawniania pozwala ustalić zasadność oraz datę i godzinę przeprowadzenia takich operacji, tożsamość osoby, która przeglądała lub ujawniła operacyjne dane osobowe, oraz, w miarę możliwości, tożsamość odbiorców takich operacyjnych danych osobowych.

2. Ewidencję wykorzystuje się wyłącznie do weryfikacji zgodności przetwarzania z prawem, do monitorowania własnej działalności, zapewnienia integralności i bezpieczeństwa operacyjnych danych osobowych oraz na potrzeby postępowania karnego. Wpisy do ewidencji są usuwane po trzech latach, chyba że są wciąż potrzebne do trwających kontroli.

3. Administrator udostępnia ewidencję swojemu inspektorowi ochrony danych oraz Europejskiemu Inspektorowi Ochrony Danych na żądanie.

Artykuł 89

Ocena skutków dla ochrony danych

1. Jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele może skutkować powstaniem wysokiego ryzyka naruszenia praw i wolności osób fizycznych, administrator przed przeprowadzeniem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania pod kątem ochrony operacyjnych danych osobowych.

2. Ocena, o której mowa w ust. 1, zawiera co najmniej ogólny opis planowanych operacji przetwarzania, ocenę ryzyka naruszenia praw i wolności osób, których dane dotyczą, środki planowane w celu zaradzenia takiemu ryzyku, zabezpieczenia, środki i mechanizmy bezpieczeństwa mające zapewnić ochronę operacyjnych danych osobowych i wykazać zgodność z przepisami dotyczącymi ochrony danych, z uwzględnieniem praw i uzasadnionych interesów osób, których dane dotyczą, i innych zainteresowanych osób.

Artykuł 90

Uprzednie konsultacje z Europejskim Inspektorem Ochrony Danych

1. Administrator konsultuje się z Europejskim Inspektorem Ochrony Danych przed przeprowadzeniem przetwarzania, które będzie częścią nowego systemu zbioru danych, w sytuacjach gdy:

a) ocena skutków dla ochrony danych, o której mowa w art. 89, wykaże, że przetwarzanie powodowałoby wysokie ryzyko naruszenia w razie niepodjęcia przez administratora środków w celu zminimalizowania tego ryzyka lub

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

2. Europejski Inspektor Ochrony Danych może sporządzić wykaz operacji przetwarzania, które wymagają uprzednich konsultacji zgodnie z ust. 1.

3. Administrator przedstawia Europejskiemu Inspektorowi Ochrony Danych ocenę skutków dla ochrony danych, o której mowa w art. 89, oraz – na jego wniosek – wszelkie inne informacje umożliwiające Europejskiemu Inspektorowi Ochrony Danych ocenę zgodności przetwarzania z przepisami, w szczególności ocenę zagrożenia ochrony operacyjnych danych osobowych osoby, której dane dotyczą, oraz ocenę powiązanych zabezpieczeń.

4. Jeżeli Europejski Inspektor Ochrony Danych jest zdania, że zamierzone przetwarzanie, o którym mowa w ust. 1, stanowiłoby naruszenie niniejszego rozporządzenia lub aktu prawnego ustanawiającego organ lub jednostkę organizacyjną Unii – w szczególności gdy administrator niedostatecznie zidentyfikował lub zminimalizował ryzyko – Europejski Inspektor Ochrony Danych w terminie do sześciu tygodni po otrzymaniu wniosku o konsultacje udziela administratorowi pisemnej porady. Termin ten można przedłużyć o kolejny miesiąc ze względu na złożony charakter zamierzonego przetwarzania. Europejski Inspektor Ochrony Danych informuje administratora o takim przedłużeniu w terminie jednego miesiąca od otrzymania wniosku w sprawie konsultacji, z podaniem przyczyn tego opóźnienia.

Artykuł 91

Bezpieczeństwo przetwarzania operacyjnych danych osobowych

1. Uwzględniając stan wiedzy technicznej, koszt wdrożenia oraz charakter, zakres, kontekst i cele przetwarzania, a także ryzyko – o różnym prawdopodobieństwie i wadze – naruszenia praw i wolności osób fizycznych, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne dla zagwarantowania poziomu bezpieczeństwa odpowiadającego temu ryzyku, zwłaszcza jeżeli chodzi o przetwarzanie szczególnych kategorii operacyjnych danych osobowych.

2. W odniesieniu do przetwarzania zautomatyzowanego administrator i podmiot przetwarzający, po ocenie ryzyka, wdrażają środki, które:

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

b) zapobiegną nieupoważnionemu odczytywaniu, kopiowaniu, modyfikowaniu lub usuwaniu nośników danych („kontrola nośników danych”);

c) zapobiegną nieupoważnionemu wprowadzaniu operacyjnych danych osobowych oraz nieupoważnionemu kontrolowaniu, zmienianiu lub usuwaniu przechowywanych operacyjnych danych osobowych („kontrola przechowywania”);

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

e) zapewnią osobom uprawnionym do korzystania z systemu zautomatyzowanego przetwarzania dostęp wyłącznie do operacyjnych danych osobowych objętych posiadanym przez nie uprawnieniem („kontrola dostępu do danych”);

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

g) pozwolą na późniejszym etapie zweryfikować i stwierdzić, które operacyjne dane osobowe zostały wprowadzone do systemów zautomatyzowanego przetwarzania operacyjnych danych osobowych, kiedy i przez kogo („kontrola wprowadzania danych”);

h) uniemożliwią nieuprawnione odczytywanie, kopiowanie, modyfikację lub usuwanie operacyjnych danych osobowych podczas przekazów operacyjnych danych osobowych lub podczas przewożenia nośników danych („kontrola transportu");

i) zapewnią – w razie awarii – możliwość przywrócenia zainstalowanych systemów („odzyskiwanie");

j) zapewnią wykonywanie przez system jego funkcji i zgłaszanie występujących w nich błędów (niezawodność) oraz zapobieżenie uszkodzeniom przechowywanych operacyjnych danych osobowych spowodowanym błędnym działaniem systemu („integralność");

Artykuł 92

Zgłaszanie naruszenia ochrony danych osobowych Europejskiemu Inspektorowi Ochrony Danych

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

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

a) opis charakteru naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazanie kategorii i przybliżonej liczby osób, których dane dotyczą, oraz kategorii i przybliżonej liczb wykazów operacyjnych danych osobowych, których dotyczy naruszenie;

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

c) opis możliwych konsekwencji naruszenia ochrony danych osobowych;

d) opis środków zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środków mających na celu zminimalizowania jego ewentualnych negatywnych skutków.

3. Jeżeli i o ile informacji, o których mowa w ust. 2, nie da się przekazać w tym samym czasie, można je przekazywać sukcesywnie bez zbędnej zwłoki.

4. Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, o których mowa w ust. 1, wraz z okolicznościami faktycznymi naruszenia danych osobowych, jego skutkami oraz podjętymi działaniami naprawczymi. Dokumentacja ta umożliwia Europejskiemu Inspektorowi Ochrony Danych weryfikowanie przestrzegania niniejszego artykułu.

5. W przypadku gdy naruszenie ochrony operacyjnych danych osobowych dotyczy danych osobowych przesłanych przez właściwe organy lub do nich, administrator przekazuje bez zbędnej zwłoki informacje, o których mowa w ust. 2, właściwym organom.

Artykuł 93

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. Skierowane do osoby, której dane dotyczą, zawiadomienie wskazane w ust. 1 niniejszego artykułu opisuje jasnym i prostym językiem charakter naruszenia ochrony danych osobowych i zawiera co najmniej informacje i zalecenia, o których mowa w art. 92 ust. 2 lit. b), c) i d).

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

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

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

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

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

5. Skierowane do osoby, której dane dotyczą, zawiadomienie wskazane w ust. 1 można opóźnić, ograniczyć lub pominąć, z zastrzeżeniem warunków i z powodów wskazanych w art. 79 ust. 3.

Artykuł 94

Przekazywanie operacyjnych danych osobowych państwom trzecim i organizacjom międzynarodowym

1. Z zastrzeżeniem ograniczeń i warunków określonych w aktach prawnych ustanawiających organy lub jednostki organizacyjne Unii, administrator może przekazać operacyjne dane osobowe organowi państwa trzeciego lub organizacji międzynarodowej w zakresie, w jakim przekazanie takie jest niezbędne do wykonywania zadań administratora i jedynie w przypadku gdy spełniono warunki określone w niniejszym artykule, a mianowicie:

a) Komisja przyjęła decyzję stwierdzającą odpowiedni stopień ochrony na podstawie art. 36 ust. 3 dyrektywy (UE) 2016/680 uznającą, że dane państwo trzecie lub terytorium, lub sektor, w którym odbywa się przetwarzanie danych w tym państwie trzecim, lub dana organizacja międzynarodowa zapewnia odpowiedni poziom ochrony;

b) w razie braku decyzji Komisji stwierdzającej odpowiedni stopień ochrony, o której mowa w lit. a), została zawarta umowa międzynarodowa między Unią a danym państwem trzecim lub organizacją międzynarodową na podstawie art. 218 TFUE zakładająca odpowiednie zabezpieczenia w odniesieniu do ochrony prywatności oraz podstawowych praw i wolności osób fizycznych;

c) w razie braku decyzji Komisji stwierdzającej odpowiedni stopień ochrony, o której mowa w lit. a), lub porozumienia międzynarodowego, o którym mowa w lit. b), została zawarta umowa o współpracy pozwalająca na wymianę operacyjnych danych osobowych przed rozpoczęciem stosowania aktu prawnego ustanawiającego organ lub jednostkę organizacyjną Unii między tym organem lub tą jednostką organizacyjną Unii a danym państwem trzecim.

2. Akty prawne ustanawiające organy i jednostki organizacyjne Unii mogą zachować lub wprowadzić bardziej szczegółowe przepisy dotyczące warunków międzynarodowego przekazywania operacyjnych danych osobowych, zwłaszcza w odniesieniu do przekazywania danych na podstawie odpowiednich gwarancji i odstępstw w szczególnych sytuacjach.

3. Administrator publikuje na swojej stronie internetowej i uaktualnia wykaz decyzji stwierdzających odpowiedni stopień ochrony, o których mowa w ust. 1 lit. a), umów, porozumień administracyjnych i innych instrumentów dotyczących przekazywania operacyjnych danych osobowych zgodnie z ust. 1.

4. Administrator prowadzi szczegółową ewidencję wszystkich operacji przekazania dokonanych na mocy niniejszego artykułu.

Artykuł 95

Tajemnica postępowania sądowego i postępowania karnego

Akty prawne ustanawiające organy i jednostki organizacyjne Unii wykonujące zadania wchodzące w zakres części trzeciej tytuł V rozdział 4 lub rozdział 5 TFUE, mogą zobowiązywać Europejskiego Inspektora Ochrony Danych, w ramach wykonywania jego uprawnień nadzorczych, do uwzględnienia w najwyższym stopniu tajemnicy postępowania sądowego i postępowania karnego, zgodnie z prawem Unii lub prawem państwa członkowskiego.

ROZDZIAŁ X

AKTY WYKONAWCZE

Artykuł 96

Procedura komitetowa

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

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

ROZDZIAŁ XI

PRZEGLĄD

Artykuł 97

Klauzula przeglądowa

Najpóźniej do dnia 30 kwietnia 2022 r., a następnie co pięć lat, Komisja przedkłada Parlamentowi Europejskiemu i Radzie sprawozdanie w sprawie stosowania niniejszego rozporządzenia, w razie potrzeby wraz z odpowiednimi wnioskami ustawodawczymi.

Artykuł 98

Przegląd aktów prawnych Unii

1. Do dnia 30 kwietnia 2022 r. Komisja dokonuje przeglądu przyjętych na podstawie Traktatów aktów prawnych, które regulują przetwarzanie operacyjnych danych osobowych przez organy lub jednostki organizacyjne Unii wykonujące czynności które wchodzą w zakres części trzeciej tytuł V rozdział 4 lub rozdział 5 TFUE, w celu:

a) dokonania oceny ich zgodności z dyrektywą (UE) 2016/680 i rozdziałem IX niniejszego rozporządzenia;

b) stwierdzenia wszelkich rozbieżności, które mogą utrudniać wymianę operacyjnych danych osobowych między organami i jednostkami organizacyjnymi Unii podczas prowadzenia działań w tych dziedzinach i właściwymi organami; oraz

c) stwierdzenia wszelkich rozbieżności, które mogą spowodować fragmentaryzację przepisów dotyczących ochrony danych w Unii.

2. Na podstawie tego przeglądu, aby zapewnić jednolitą i spójną ochronę osób fizycznych w odniesieniu do przetwarzania danych, Komisja może przedstawić odnośne wnioski ustawodawcze, w tym w szczególności w razie potrzeby modyfikacje rozdziału IX niniejszego rozporządzenia, z myślą o zastosowaniu tego rozdziału do Europolu i Prokuratury Europejskiej.

ROZDZIAŁ XII

PRZEPISY KOŃCOWE

Artykuł 99

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

Rozporządzenie (WE) nr 45/2001 i decyzja nr 1247/2002/WE tracą moc ze skutkiem od dnia 11 grudnia 2018 r. Odesłania do uchylonego rozporządzenia oraz uchylonej decyzji rozumie się jako odesłania do niniejszego rozporządzenia.

Artykuł 100

Środki przejściowe

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

---

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

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

3. Art. 53 ust. 4, 5 i 7 oraz art. 55 i 56 niniejszego rozporządzenia mają zastosowanie do obecnego zastępcy inspektora do końca jego kadencji.

4. Zastępca inspektora pomaga Europejskiemu Inspektorowi Ochrony Danych w wypełnianiu jego obowiązków i zastępuje Europejskiego Inspektora Ochrony Danych podczas jego nieobecności lub w sytuacji pozbawienia go możliwości wykonywania obowiązków do końca obecnej kadencji zastępcy inspektora.

Artykuł 101

Wejście w życie i rozpoczęcie stosowania

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

2. Niniejsze rozporządzenie ma jednak zastosowanie do przetwarzania danych osobowych przez Eurojust od dnia 12 grudnia 2019 r..

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

Sporządzono w Strasburgu dnia 23 października 2018 r.

W imieniu Parlamentu Europejskiego	*W imieniu Rady*
Przewodniczący	*Przewodniczący*
A. TAJANI	K. EDTSTADLER