Dziennik Urzędowy L 295
Unii Europejskiej

Wydanie polskie **Legislacja**

Rocznik 61

21 listopada 2018

Spis treści

([1]) Tekst mający znaczenie dla EOG.

PL

Akty, których tytuły wydrukowano zwykłą czcionką, odnoszą się do bieżącego zarządzania sprawami rolnictwa i generalnie zachowują ważność przez określony czas.

Tytuły wszystkich innych aktów poprzedza gwiazdka, a drukuje się je czcionką pogrubioną.

I

(Akty ustawodawcze)

ROZPORZĄDZENIA

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2018/1724

z dnia 2 października 2018 r.

w sprawie utworzenia jednolitego portalu cyfrowego w celu zapewnienia dostępu do informacji, procedur oraz usług wsparcia i rozwiązywania problemów, a także zmieniające rozporządzenie (UE) nr 1024/2012

(Tekst mający znaczenie dla EOG)

PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 21 ust. 2 i art. 114 ust. 1,

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) Rynek wewnętrzny jest jednym z najbardziej namacalnych osiągnięć Unii. Umożliwiając swobodny przepływ osób, towarów, usług i kapitału oferuje on nowe możliwości obywatelom i przedsiębiorstwom. Niniejsze rozporządzenie jest kluczowym elementem strategii jednolitego rynku określonej w komunikacie Komisji z dnia 28 października 2015 r. zatytułowanym „Usprawnianie jednolitego rynku: więcej możliwości dla obywateli i przedsiębiorstw". Celem tej strategii jest uwolnienie pełnego potencjału rynku wewnętrznego poprzez ułatwienie obywatelom i przedsiębiorstwom przemieszczania się w Unii oraz prowadzenia działalności handlowej, zakładania i rozwijania działalności gospodarczej w wymiarze transgranicznym.

(2) W komunikacie Komisji z dnia 6 maja 2015 r. zatytułowanym „Strategia jednolitego rynku cyfrowego dla Europy" uznano rolę, jaką internet i technologie cyfrowe odgrywają w zmienianiu naszego codziennego życia i sposobu, w jaki obywatele i przedsiębiorstwa uzyskują dostęp do informacji, zdobywają wiedzę, kupują towary i usługi, są uczestnikami rynku i pracownikami, co otwiera możliwości w zakresie innowacji, wzrostu i zatrudnienia. W komunikacie tym, a także w szeregu rezolucji przyjętych przez Parlament Europejski, uznano również, że potrzeby obywateli i przedsiębiorstw w ich własnym kraju oraz za granicą można by lepiej zaspokoić poprzez rozszerzenie i integrację istniejących na poziomie europejskim portali, stron internetowych, sieci, usług i systemów oraz poprzez połączenie ich z różnymi rozwiązaniami na poziomie krajowym, tworząc w ten sposób jednolity portal cyfrowy pełniący funkcję europejskiego punktu kompleksowej obsługi (zwany dalej „Portalem"). W komunikacie Komisji z dnia 19 kwietnia 2016 r. zatytułowanym „Plan działania UE na rzecz administracji elektronicznej na lata 2016–2020 – Przyspieszenie transformacji cyfrowej w administracji" wymieniono Portal jako jedno z działań Komisji przewidzianych na rok 2017. W sprawozdaniu Komisji z dnia 24 stycznia 2017 r. zatytułowanym „Wzmocnienie praw obywateli w Unii demokratycznych zmian. Sprawozdanie na temat obywatelstwa UE z 2017 r." uznano Portal za priorytet w zakresie praw obywateli w Unii.

(3) Parlament Europejski i Rada wielokrotnie apelowały o stworzenie bardziej kompleksowego i przyjaznego dla użytkownika pakietu informacji i wsparcia, aby pomóc obywatelom i przedsiębiorstwom poruszać się po rynku wewnętrznym oraz aby wzmocnić i usprawnić narzędzia rynku wewnętrznego w celu lepszego zaspokojenia potrzeb obywateli i przedsiębiorstw w zakresie ich działalności transgranicznej.

([1]) Dz.U. C 81 z 2.3.2018, s. 88.
([2]) Stanowisko Parlamentu Europejskiego z dnia 13 września 2018 r. (dotychczas nieopublikowane w Dzienniku Urzędowym) oraz decyzja Rady z dnia 27 września 2018 r.

(4) Niniejsze rozporządzenie odpowiada na te apele, oferując obywatelom i przedsiębiorstwom łatwy dostęp do informacji, procedur oraz usług wsparcia i rozwiązywania problemów, potrzebnych im do celów korzystaniu z ich praw na rynku wewnętrznym. Portal mógłby przyczynić się do zwiększenia przejrzystości przepisów i regulacji dotyczących różnych zdarzeń gospodarczych i życiowych, w takich dziedzinach jak podróże, emerytury, edukacja, zatrudnienie, opieka zdrowotna, prawa konsumentów i prawo rodzinne. Ponadto mógłby on przyczynić się do zwiększenia zaufania konsumentów, rozwiązywania problemu braku wiedzy o przepisach dotyczących ochrony konsumentów i rynku wewnętrznego oraz obniżyć koszty przestrzegania przepisów dla przedsiębiorstw. W niniejszym rozporządzeniu ustanawia się przyjazny dla użytkownika, interaktywny Portal, który w oparciu o potrzeby użytkowników powinien im wskazać najbardziej odpowiednie usługi. W tym kontekście Komisja i państwa członkowskie powinny odgrywać ważną rolę w realizacji tych celów.

(5) Portal powinien ułatwiać kontakty między obywatelami i przedsiębiorstwami, z jednej strony, oraz właściwymi organami, z drugiej strony, dzięki zapewnieniu dostępu do rozwiązań internetowych, ułatwianiu codziennych działań obywateli i codziennej działalności przedsiębiorstw oraz minimalizowaniu przeszkód napotykanych na rynku wewnętrznym. Istnienie jednolitego portalu cyfrowego zapewniającego dostęp online do dokładnych i aktualnych informacji, procedur oraz usług wsparcia i rozwiązywania problemów mogłoby pomóc podnieść świadomość użytkowników na temat różnych istniejących usług online oraz zaoszczędzić im czasu i kosztów.

(6) Niniejsze rozporządzenie służy realizacji trzech celów, tj.: zmniejszeniu wszelkich dodatkowych obciążeń administracyjnych dla obywateli i przedsiębiorstw, którzy korzystają lub chcą korzystać z praw przysługujących im na rynku wewnętrznym, w tym ze swobodnego przepływu obywateli, w pełnym poszanowaniu krajowych przepisów i procedur; eliminowaniu dyskryminacji oraz zapewnieniu funkcjonowania rynku wewnętrznego w zakresie zapewniania informacji, procedur oraz usług wsparcia i rozwiązywania problemów. Ponieważ niniejsze rozporządzenie obejmuje swoim zakresem stosowania swobodny przepływ obywateli, czego nie można uznać za mające jedynie charakter dodatkowy, podstawą niniejszego rozporządzenia powinny być art. 21 ust. 2 i art. 114 ust. 1 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE).

(7) Aby obywatele Unii oraz unijni przedsiębiorcy mogli korzystać z przysługującego im prawa do swobodnego przepływu w ramach rynku wewnętrznego, Unia powinna przyjąć konkretne niedyskryminujące środki umożliwiające obywatelom i przedsiębiorstwom łatwy dostęp do wystarczająco kompleksowych i wiarygodnych informacji o ich prawach wynikających z prawa Unii oraz do informacji o mających zastosowanie przepisach i procedurach krajowych, których muszą przestrzegać w przypadku gdy przenoszą się do państwa członkowskiego innego niż własne, mieszkają tam lub studiują lub gdy zakładają lub prowadzą tam działalność gospodarczą. Informacje należy uznać za wystarczająco kompleksowe, jeżeli obejmują one wszystkie informacje niezbędne użytkownikom, aby zrozumieli oni swoje prawa i obowiązki oraz jeżeli informacje te wskazują przepisy mające zastosowanie do tych użytkowników w związku z działaniami, jakie chcą oni podejmować jako użytkownicy transgraniczni. Informacje te powinny być podane w jasny, zwięzły i zrozumiały sposób, powinny być funkcjonalne i dobrze dostosowane do docelowej grupy użytkowników. Informacje na temat procedur powinny obejmować wszystkie możliwe do przewidzenia kroki proceduralne, które mają znaczenie dla użytkowników. Ważne jest, aby obywatele i przedsiębiorstwa, mający do czynienia ze złożonym środowiskiem regulacyjnym, na przykład uczestniczący w handlu elektronicznym i gospodarce współpracy, mogli w łatwy sposób znaleźć mające zastosowanie przepisy oraz dowiedzieć się w jaki sposób przepisy te stosuje się do ich działań lub działalności. Łatwy i przyjazny dla użytkownika dostęp do informacji oznacza umożliwienie użytkownikom łatwego znalezienia informacji, łatwej identyfikacji elementów informacji mających znaczenie w ich konkretnej sytuacji, oraz łatwego zrozumienia odpowiednich informacji. Informacje, które mają być zapewniane na poziomie krajowym, powinny dotyczyć nie tylko przepisów krajowych wdrażających prawo Unii, ale również wszelkich innych przepisów krajowych, które mają zastosowanie zarówno do użytkowników nietransgranicznych, jak i do użytkowników transgranicznych.

(8) Zawarte w niniejszym rozporządzeniu przepisy dotyczące zapewniania informacji nie powinny mieć zastosowania do krajowych systemów wymiaru sprawiedliwości, ponieważ informacje z tej dziedziny mające znaczenie dla użytkowników transgranicznych są już zawarte w portalu „e-Sprawiedliwość". W niektórych sytuacjach objętych zakresem stosowania niniejszego rozporządzenia sądy powinny być uznawane za właściwe organy, na przykład w przypadku gdy prowadzą one rejestry przedsiębiorstw. Ponadto zasada niedyskryminacji powinna mieć zastosowanie także do procedur online, które dają dostęp do postępowań sądowych.

(9) Oczywiste jest, że obywatele i przedsiębiorstwa z innych państw członkowskich mogą być w niekorzystnej sytuacji ze względu na swój brak znajomości krajowych przepisów i systemów administracyjnych, różnice językowe oraz geograficzne oddalenie od właściwych organów w państwach członkowskich innych niż ich własne. Najbardziej skutecznym sposobem zmniejszenia związanych z tym przeszkód w funkcjonowaniu rynku wewnętrznego jest umożliwienie użytkownikom transgranicznym i nietransgranicznym dostępu do informacji online w języku dla nich zrozumiałym w celu umożliwienia im przeprowadzenia procedur niezbędnych do przestrzegania przepisów krajowych w pełni online oraz udzielenie im wsparcia w przypadku gdy przepisy i procedury nie są wystarczająco jasne lub w przypadku gdy napotykają oni na przeszkody w korzystaniu ze swoich praw.

(10) W wielu aktach Unii próbowano znaleźć rozwiązanie poprzez utworzenie sektorowych punktów kompleksowej obsługi, w tym: pojedynczych punktów kontaktowych utworzonych na mocy dyrektywy Parlamentu Europejskiego i Rady 2006/123/WE ([1]), oferujących informacje online, usługi wsparcia oraz dostęp do procedur dotyczących świadczenia usług; punktów kontaktowych ds. produktów utworzonych na mocy rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 764/2008 ([2]) oraz punktów kontaktowych ds. wyrobów budowlanych utworzonych na mocy rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 305/2011 ([3]), zapewniających dostęp do przepisów technicznych dotyczących konkretnych produktów; a także krajowych ośrodków wsparcia ds. kwalifikacji zawodowych utworzonych na mocy dyrektywy Parlamentu Europejskiego i Rady 2005/36/WE ([4]), wspierających specjalistów w zakresie mobilności transgranicznej. Ponadto utworzono sieci, takie jak Europejskie Centra Konsumenckie, w celu propagowania znajomości praw konsumentów Unii oraz wspierania w rozpatrywaniu skarg dotyczących zakupów dokonywanych w innych państwach członkowskich w ramach sieci, podczas podróży lub zakupów przez internet. Ponadto w ramach SOLVIT, o którym mowa w zaleceniu Komisji 2013/461/UE ([5]), dąży się do znalezienia szybkich, skutecznych i nieformalnych rozwiązań dla osób fizycznych i przedsiębiorstw gdy ich prawa na rynku wewnętrznym nie są przestrzegane przez organy publiczne. Utworzono również szereg portali informacyjnych, takich jak „Twoja Europa", w obszarze rynku wewnętrznego, oraz portal „e-Sprawiedliwość", w obszarze sprawiedliwości, aby informować użytkowników o przepisach Unii i przepisach krajowych.

(11) Ze względu na sektorowy charakter tych aktów Unii zapewnianie informacji oraz usług wsparcia i rozwiązywania problemów online wraz z procedurami online dla obywateli i przedsiębiorstw jest obecnie bardzo rozdrobnione. Występują różnice w dostępności informacji i procedur online, jakość usług jest niska, a usługi informacyjne oraz usługi wsparcia i rozwiązywania problemów są mało znane. Użytkownicy transgraniczni napotykają również problemy odnajdywaniu tych usług i uzyskiwaniu do nich dostępu.

(12) W niniejszym rozporządzeniu należy utworzyć jednolity portal cyfrowy pełniący funkcję punktu kompleksowej usługi, za pośrednictwem którego obywatele i przedsiębiorstwa mogą mieć dostęp do informacji na temat przepisów i wymogów, których muszą przestrzegać na mocy prawa Unii lub prawa krajowego. Portal powinien uprościć kontakt obywateli i przedsiębiorstw z usługami wsparcia i rozwiązywania problemów na poziomie Unii lub na poziomie krajowym oraz zwiększyć skuteczność tego kontaktu. Portal powinien również ułatwić dostęp do procedur online i ich przeprowadzanie. Niniejsze rozporządzenie nie powinno w żaden sposób wpływać na istniejące prawa i obowiązki wynikające z prawa Unii lub prawa krajowego w tych obszarach polityki. W odniesieniu do procedur wymienionych w załączniku II do niniejszego rozporządzenia oraz procedur przewidzianych w dyrektywach 2005/36/WE i 2006/123/WE, a także w dyrektywach Parlamentu Europejskiego i Rady 2014/24/UE ([6]) i 2014/25/UE ([7]), niniejsze rozporządzenie powinno wspierać stosowanie zasady jednorazowości i powinno być w pełni zgodne z prawem podstawowym do ochrony danych osobowych, do celów wymiany dowodów między właściwymi organami w różnych państwach członkowskich.

(13) Portal oraz jego zawartość powinny być zorientowane na użytkownika i przyjazne dla użytkownika. Portal powinien mieć na celu unikanie powieleń oraz powinien zawierać linki do istniejących usług. Powinien umożliwiać obywatelom i przedsiębiorstwom kontaktowanie się z organami publicznymi na poziomie krajowym i na poziomie Unii poprzez zapewnianie im możliwości przekazywania informacji zwrotnych zarówno w odniesieniu do usług świadczonych za pośrednictwem Portalu, jak i ich doświadczeń związanych z funkcjonowaniem rynku wewnętrznego. Narzędzie do gromadzenia informacji zwrotnych powinno umożliwiać użytkownikowi zwrócenie uwagi, w sposób umożliwiający mu zachowanie anonimowości, na zauważone problemy, braki i potrzeby, aby zachęcać do ciągłej poprawy jakości usług.

([1]) Dyrektywa 2006/123/WE Parlamentu Europejskiego i Rady z dnia 12 grudnia 2006 r. dotycząca usług na rynku wewnętrznym (Dz.U. L 376 z 27.12.2006, s. 36).

([2]) Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 764/2008 z dnia 9 lipca 2008 r. ustanawiające procedury dotyczące stosowania niektórych krajowych przepisów technicznych do produktów wprowadzonych legalnie do obrotu w innym państwie członkowskim oraz uchylające decyzję nr 3052/95/WE (Dz.U. L 218 z 13.8.2008, s. 21).

([3]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 305/2011 z dnia 9 marca 2011 r. ustanawiające zharmonizowane warunki wprowadzania do obrotu wyrobów budowlanych i uchylające dyrektywę Rady 89/106/EWG (Dz.U. L 88 z 4.4.2011, s. 5).

([4]) Dyrektywa 2005/36/WE Parlamentu Europejskiego i Rady z dnia 7 września 2005 r. w sprawie uznawania kwalifikacji zawodowych (Dz.U. L 255 z 30.9.2005, s. 22).

([5]) Zalecenie Komisji 2013/461/UE z dnia 17 września 2013 r. w sprawie zasad regulujących SOLVIT (Dz.U. L 249 z 19.9.2013, s. 10).

([6]) Dyrektywa Parlamentu Europejskiego i Rady 2014/24/UE z dnia 26 lutego 2014 r. w sprawie zamówień publicznych, uchylająca dyrektywę 2004/18/WE (Dz.U. L 94 z 28.3.2014, s. 65).

([7]) Dyrektywa Parlamentu Europejskiego i Rady 2014/25/UE z dnia 26 lutego 2014 r. w sprawie udzielania zamówień przez podmioty działające w sektorach gospodarki wodnej, energetyki, transportu i usług pocztowych, uchylająca dyrektywę 2004/17/WE (Dz.U. L 94 z 28.3.2014, s. 243).

(14) Sukces Portalu będzie zależał od wspólnego wysiłku Komisji i państw członkowskich. Portal powinien obejmować wspólny interfejs użytkownika, zintegrowany z istniejącym portalem „Twoja Europa", którym będzie zarządzać Komisja. Wspólny interfejs użytkownika powinien zawierać linki do informacji, procedur oraz usług wsparcia i rozwiązywania problemów dostępnych w portalach zarządzanych przez właściwe organy w państwach członkowskich oraz przez Komisję. W celu ułatwienia korzystania z Portalu wspólny interfejs użytkownika powinien być dostępny we wszystkich językach urzędowych instytucji Unii (zwanych dalej „językami urzędowymi Unii"). Istniejący portal „Twoja Europa" oraz strona internetowa zapewniająca główny dostęp do niego, przystosowane do wymogów Portalu, powinny utrzymać to wielojęzyczne podejście do zapewnianych informacji. Funkcjonowanie Portalu powinno opierać się na narzędziach technicznych opracowanych przez Komisję w ścisłej współpracy z państwami członkowskimi.

(15) W karcie elektronicznych pojedynczych punktów kontaktowych w ramach dyrektywy 2006/123/WE, która została zatwierdzona przez Radę w 2013 r., państwa członkowskie podjęły dobrowolne zobowiązanie do przyjęcia podejścia zorientowanego na użytkownika w zapewnianiu informacji za pośrednictwem pojedynczych punktów kontaktowych w celu uwzględnienia obszarów o szczególnym znaczeniu dla przedsiębiorstw, w tym VAT, podatków dochodowych, zabezpieczeń społecznych lub wymogów prawa pracy. W oparciu o kartę oraz w świetle doświadczeń z portalem „Twoja Europa" w informacjach tych należy również zawrzeć opis usług wsparcia i rozwiązywania problemów. Obywatele i przedsiębiorstwa powinny móc korzystać z takich usług w przypadku problemów ze zrozumieniem informacji, z zastosowaniem informacji do swojej sytuacji lub z przeprowadzeniem procedury.

(16) W niniejszym rozporządzeniu powinny zostać wymienione obszary informacji, które mają znaczenie dla obywateli i przedsiębiorstw korzystających ze swoich praw i wypełniających swoje obowiązki na rynku wewnętrznym. Dla tych obszarów na poziomie krajowym, w tym na poziomie regionalnym i lokalnym, oraz na poziomie Unii należy zapewnić wystarczająco kompleksowe informacje dotyczące mających zastosowanie przepisów i obowiązków oraz procedur, które obywatele i przedsiębiorstwa muszą przeprowadzić w celu zapewnienia zgodności z tymi przepisami i obowiązkami. W celu zapewnienia wysokiej jakości oferowanych usług informacje przekazywane za pośrednictwem Portalu powinny być jasne, dokładne i aktualne, stosowanie skomplikowanej terminologii powinno być ograniczone do minimum, a zastosowanie skrótowców powinno być ograniczone do tych, które oznaczają uproszczone i łatwe do zrozumienia terminy niewymagające wcześniejszej znajomości danego zagadnienia lub dziedziny prawa. Informacje te należy zapewniać w taki sposób, aby użytkownicy mogli łatwo zrozumieć podstawowe przepisy i wymogi mające zastosowanie do ich sytuacji w tych obszarach. Użytkownicy powinni być również informowani o braku, w niektórych państwach członkowskich, przepisów krajowych w obszarach informacji wymienionych w załączniku I, zwłaszcza w przypadku gdy obszary te podlegają przepisom krajowym w innych państwach członkowskich. Takie informacje o braku przepisów krajowych mogłyby zostać zawarte w portalu „Twoja Europa".

(17) Na tyle, na ile jest to możliwe, informacje zebrane już przez Komisję od państw członkowskich na podstawie obowiązującego prawa Unii lub dobrowolnych porozumień – takie jak informacje zebrane do celów portalu EURES, utworzonego na mocy rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/589 ([1]), portalu „e-Sprawiedliwość", utworzonego na mocy decyzji Rady 2001/470/WE ([2]), lub bazy danych o zawodach regulowanych utworzonej na mocy dyrektywy 2005/36/WE – powinny być wykorzystane jako część informacji, które mają być udostępniane obywatelom i przedsiębiorstwom na poziomie Unii i na poziomie krajowym zgodnie z niniejszym rozporządzeniem. Państwa członkowskie nie powinny być zobowiązane do podawania na swoich krajowych stronach internetowych informacji, które są już dostępne w odpowiednich bazach danych zarządzanych przez Komisję. W przypadku gdy państwa członkowskie muszą już zapewniać informacje online zgodnie z innymi aktami Unii, takimi jak dyrektywa Parlamentu Europejskiego i Rady 2014/67/UE ([3]), wystarczające powinno być udostępnienie przez państwa członkowskie linków do istniejących informacji online. W przypadku gdy pewne obszary polityki zostały już w pełni zharmonizowane przez prawo Unii, na przykład prawa konsumentów, informacje zapewniane na poziomie Unii na ogół powinny być wystarczające, aby użytkownicy mogli zrozumieć swoje odpowiednie prawa lub obowiązki. W takich przypadkach państwa członkowskie powinny być zobowiązane jedynie do zapewnienia dodatkowych informacji dotyczących ich krajowych procedur administracyjnych i usług

([1]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/589 z dnia 13 kwietnia 2016 r. w sprawie europejskiej sieci służb zatrudnienia (EURES), dostępu pracowników do usług w zakresie mobilności i dalszej integracji rynków pracy oraz zmiany rozporządzeń (UE) nr 492/2011 i (UE) nr 1296/2013 (Dz.U. L 107 z 22.4.2016, s. 1).

([2]) Decyzja Rady 2001/470/WE z dnia 28 maja 2001 r. ustanawiająca Europejską Sieć Sądową w sprawach cywilnych i handlowych (Dz.U. L 174 z 27.6.2001, s. 25).

([3]) Dyrektywa Parlamentu Europejskiego i Rady 2014/67/UE z dnia 15 maja 2014 r. w sprawie egzekwowania dyrektywy 96/71/WE dotyczącej delegowania pracowników w ramach świadczenia usług, zmieniająca rozporządzenie (UE) nr 1024/2012 w sprawie współpracy administracyjnej za pośrednictwem systemu wymiany informacji na rynku wewnętrznym („rozporządzenie w sprawie IMI") (Dz.U. L 159 z 28.5.2014, s. 11).

wsparcia lub wszelkich innych krajowych przepisów administracyjnych, jeżeli informacje te mają znaczenie dla użytkowników. Na przykład, informacje dotyczące praw konsumentów nie powinny mieć wpływu na prawo umów, lecz raczej informować użytkowników o ich prawach wynikających z prawa Unii i prawa krajowego w kontekście transakcji handlowych.

(18) Niniejsze rozporządzenie powinno wzmacniać wymiar rynku wewnętrznego w procedurach online, tym samym przyczyniając się do cyfryzacji rynku wewnętrznego, poprzez utrzymywanie ogólnej zasady niedyskryminacji, między innymi w odniesieniu do dostępu obywateli lub przedsiębiorstw do procedur online już ustanowionych na poziomie krajowym na podstawie prawa Unii lub prawa krajowego oraz do procedur, które mają stać się w pełni dostępne online zgodnie z niniejszym rozporządzeniem. W przypadku gdy użytkownik, w sytuacji ograniczonej wyłącznie do jednego państwa członkowskiego, może mieć dostęp do procedury online oraz przeprowadzić ją w tym państwie członkowskim w obszarze objętym zakresem stosowania niniejszego rozporządzenia, użytkownik transgraniczny również powinien mieć możliwość dostępu do tej procedury online i przeprowadzenia jej za pośrednictwem tego samego rozwiązania technicznego albo alternatywnego, odrębnego technicznie rozwiązania prowadzącego do tego samego rezultatu, bez jakichkolwiek przeszkód o charakterze dyskryminacyjnym. Takie przeszkody mogą obejmować rozwiązania opracowane na poziomie krajowym, takie jak wykorzystywanie pól formularzy, w których należy podać krajowy numer telefonu, krajowe prefiksy numerów telefonu lub krajowe kody pocztowe, płatności, których można dokonać wyłącznie za pośrednictwem systemów nieobsługujących płatności transgranicznych, brak szczegółowych wyjaśnień w języku zrozumiałym dla użytkowników transgranicznych, brak możliwości elektronicznego przedłożenia dowodów pochodzących od organów z innych państw członkowskich oraz nieuznawanie elektronicznych środków identyfikacji wydanych w innych państwach członkowskich. Państwa członkowskie powinny zapewnić rozwiązania służące usunięciu takich przeszkód.

(19) Użytkownicy, przeprowadzając procedury online w wymiarze transgranicznym, powinni mieć możliwość otrzymania wszystkich istotnych wyjaśnień w języku urzędowym Unii, który jest powszechnie rozumiany przez możliwie największą liczbę użytkowników transgranicznych. Nie nakłada to na państwa członkowskie wymogu przetłumaczenia ich formularzy administracyjnych związanych z daną procedurą ani wyniku tej procedury na ten język. Państwa członkowskie zachęca się jednak do stosowania rozwiązań technicznych, które umożliwiałyby użytkownikom przeprowadzanie procedur, w możliwie największej liczbie przypadków, w tym języku, przy jednoczesnym poszanowaniu przepisów państw członkowskich dotyczących stosowania języków.

(20) To, które krajowe procedury online mają znaczenie dla użytkowników transgranicznych, aby umożliwić im korzystanie z ich praw na rynku wewnętrznym, zależy od tego, czy mają oni miejsce pobytu lub siedzibę w danym państwie członkowskim, czy też chcą skorzystać z procedur tego państwa członkowskiego, mając miejsce pobytu lub siedzibę w innym państwie członkowskim. Niniejsze rozporządzenie nie powinno uniemożliwiać państwom członkowskim wymagania od użytkowników transgranicznych mających miejsce pobytu lub siedzibę na ich terytorium, aby uzyskali oni krajowy numer identyfikacyjny w celu uzyskania dostępu do krajowych procedur online, pod warunkiem że nie będzie to pociągało za sobą nieuzasadnionych dodatkowych obciążeń lub kosztów dla tych użytkowników. W przypadku użytkowników transgranicznych, którzy nie mają miejsca pobytu lub siedziby w danym państwie członkowskim, krajowe procedury online, które nie mają znaczenia dla korzystania przez nich z praw na rynku wewnętrznym, na przykład zgłoszenie w celu korzystania z usług lokalnych, takich jak wywóz śmieci i pozwolenia na parkowanie, nie muszą być w pełni dostępne online.

(21) Niniejsze rozporządzenie powinno opierać się na rozporządzeniu Parlamentu Europejskiego i Rady (UE) nr 910/2014 ([1]), które określa warunki uznawania przez państwa członkowskie niektórych środków identyfikacji elektronicznej osób fizycznych i prawnych, objętych notyfikowanym systemem identyfikacji elektronicznej innego państwa członkowskiego. W rozporządzeniu (UE) nr 910/2014 określono warunki, jakie muszą spełnić użytkownicy, aby móc korzystać ze swoich środków elektronicznej identyfikacji i uwierzytelniania elektronicznego w celu uzyskania dostępu do usług publicznych online w sytuacjach transgranicznych. Zachęca się instytucje, organy i jednostki organizacyjne Unii do akceptowania środków identyfikacji elektronicznej i uwierzytelniania elektronicznego w przypadku procedur, za które są odpowiedzialne.

(22) W szeregu sektorowych aktów Unii, na przykład w dyrektywach 2005/36/WE, 2006/123/WE, 2014/24/UE oraz 2014/25/UE, wymaga się pełnej dostępności procedur online. W niniejszym rozporządzeniu należy wprowadzić wymóg pełnego udostępnienia online szeregu innych procedur, które mają kluczowe znaczenie dla większości obywateli i przedsiębiorstw korzystających ze swoich praw oraz wypełniających swoje obowiązki w wymiarze transgranicznym.

([1]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz.U. L 257 z 28.8.2014, s. 73).

(23) Aby umożliwić obywatelom i przedsiębiorstwom bezpośrednie korzystanie z dobrodziejstw rynku wewnętrznego bez zbędnych dodatkowych obciążeń administracyjnych, w niniejszym rozporządzeniu należy wprowadzić wymóg pełnej cyfryzacji interfejsu użytkownika niektórych kluczowych procedur dla użytkowników transgranicznych, które zostały wymienione w załączniku II do niniejszego rozporządzenia. W niniejszym rozporządzeniu należy również ustanowić kryteria określające sposób, w jaki te procedury uznaje się za będące w pełni online. Obowiązek udostępnienia takiej procedury w pełni online powinien mieć zastosowanie jedynie w przypadku gdy procedura ta została ustanowiona w danym państwie członkowskim. Niniejsze rozporządzenie nie powinno obejmować początkowej rejestracji działalności gospodarczej, procedur prowadzących do zakładania spółek lub firm będących podmiotami prawnymi ani też jakiegokolwiek późniejszego składania dokumentów przez takie spółki lub firmy, ponieważ procedury takie wymagają kompleksowego podejścia, którego celem są ułatwienia w zakresie rozwiązań cyfrowych w całym cyklu życia spółki. Przy zakładaniu działalności gospodarczej w innym państwie członkowskim od przedsiębiorstw wymaga się rejestracji w systemach zabezpieczenia społecznego i ubezpieczeń społecznych, aby móc rejestrować ich pracowników i opłacać składki w obu systemach. Przedsiębiorstwa mogłyby być zobowiązane do zgłoszenia swojej działalności gospodarczej, uzyskania zezwoleń lub rejestracji zmian w ich działalności gospodarczej. Procedury te są wspólne dla przedsiębiorstw prowadzących działalność w wielu sektorach gospodarki, w związku z czym należy wymagać, aby te procedury rejestracji były dostępne online.

(24) W niniejszym rozporządzeniu należy wyjaśnić, z czym wiąże się udostępnianie procedury w pełni online. Procedurę należy uznać za w pełni online, jeżeli użytkownik może podjąć wszystkie kroki – od uzyskania dostępu do niej do jej zakończenia – kontaktując się z właściwym organem, tzw. „działem obsługi klienta", elektronicznie, na odległość i za pośrednictwem usługi online. Ta usługa online powinna prowadzić użytkownika poprzez wykaz wszystkich wymogów, które należy spełnić, oraz wszystkich dowodów potwierdzających, które należy dostarczyć, powinna ona umożliwiać użytkownikowi dostarczanie informacji i potwierdzenia spełnienia wszystkich takich wymogów oraz powinna wydawać użytkownikowi automatyczne potwierdzenie odbioru, chyba że wynik tej procedury dostarczany jest natychmiast. Nie powinno to uniemożliwiać właściwym organom bezpośredniego kontaktu z użytkownikami, aby w razie potrzeby otrzymać dalsze wyjaśnienia potrzebne do celów procedury. Wynik procedury, jak określono w niniejszym rozporządzeniu, powinien być również przekazywany użytkownikowi przez właściwe organy drogą elektroniczną, w przypadkach gdy jest to możliwe na mocy mającego zastosowanie prawa Unii i prawa krajowego.

(25) Niniejsze rozporządzenie nie powinno mieć wpływu na istotę procedur wymienionych w załączniku II, które zostały ustanowione na poziomie krajowym, regionalnym lub lokalnym, oraz nie ustanawia przepisów materialnych lub proceduralnych w obszarach objętych zakresem stosowania załącznika II, w tym w obszarze opodatkowania. Celem niniejszego rozporządzenia jest ustanowienie wymogów technicznych z myślą o zapewnieniu, aby takie procedury, w przypadku gdy zostały one ustanowione w danym państwie członkowskim, były w pełni dostępne online.

(26) Niniejsze rozporządzenie nie powinno mieć wpływu na kompetencje organów krajowych w zakresie jakiejkolwiek procedury, w tym w zakresie weryfikacji dokładności i ważności przedłożonych informacji lub dowodów, a także weryfikacji autentyczności w przypadku złożenia dowodu za pośrednictwem środka innego niż system techniczny oparty na zasadzie jednorazowości. Niniejsze rozporządzenie nie powinno również mieć wpływu na przebieg procedury w ramach właściwych organów lub między właściwymi organami, tzw. „działami wewnętrznymi", niezależnie od tego, czy jest on cyfrowy, czy też nie. W razie potrzeby, w ramach niektórych procedur rejestrowania zmian w działalności gospodarczej, państwa członkowskie powinny nadal móc wymagać udziału notariuszy lub prawników, którzy mogliby chcieć stosować środki weryfikacji takie jak wideokonferencja lub inne środki online zapewniające połączenie audiowizualne w czasie rzeczywistym. Jednakże taki udział nie powinien uniemożliwiać przeprowadzenia procedury rejestracji takich zmian w całości online.

(27) W niektórych przypadkach użytkownicy mogliby być zobowiązani do przedstawienia dowodów w celu udowodnienia faktów, których nie można ustalić za pomocą środków elektronicznych. Takie dowody mogłyby obejmować zaświadczenia lekarskie, zaświadczenie o życiu, potwierdzenie zdatności do ruchu drogowego pojazdów silnikowych lub dowód kontroli numerów podwozia. O ile dowody takie mogą zostać przedłożone w formie elektronicznej, nie powinno to stanowić wyjątku od zasady, że procedura powinna być oferowana w pełni online. W innych przypadkach konieczne mogłoby być nadal, aby użytkownicy danej procedury stawiali się osobiście przed właściwym organem w ramach procedury online. Wszelkie takie wyjątki, inne niż wynikające z prawa Unii, powinny być ograniczone do sytuacji, które są uzasadnione nadrzędnym względem interesu publicznego w obszarach bezpieczeństwa publicznego, zdrowia publicznego lub zwalczania nadużyć finansowych. Aby zapewnić przejrzystość, państwa członkowskie powinny udostępniać Komisji i pozostałym państwom członkowskim informacje o takich wyjątkach oraz powody stosowania tych wyjątków oraz okoliczności, w których mogą one być stosowane. Państwa członkowskie nie powinny być zobowiązane do zgłaszania poszczególnych przypadków, w których, w drodze wyjątku, fizyczna obecność była wymagana, ale powinny raczej informować o przepisach krajowych, które przewidują takie przypadki. Najlepsze praktyki na poziomie krajowym oraz rozwój technologiczny pozwalający na dalszą cyfryzację w tym zakresie powinny być regularnie przedmiotem dyskusji na forum grupy koordynacyjnej Portalu.

(28) W sytuacjach transgranicznych procedura rejestracji zmiany adresu mogłaby składać się z dwóch odrębnych procedur – jednej w państwie członkowskim pochodzenia, aby zwrócić się o wyrejestrowanie ze starego adresu, oraz drugiej w państwie członkowskim przeznaczenia, aby zwrócić się o rejestrację pod nowym adresem. Obie procedury powinny być objęte zakresem stosowania niniejszego rozporządzenia.

(29) Ponieważ cyfryzacja wymogów, procedur i formalności związanych z uznawaniem kwalifikacji zawodowych jest już objęta zakresem stosowania dyrektywy 2005/36/WE, niniejsze rozporządzenie powinno obejmować wyłącznie cyfryzację procedury występowania o akademickie uznawanie dyplomów, certyfikatów lub innych świadectw ukończenia kursów w przypadku osób, które chcą rozpocząć lub kontynuować studia, lub też używać tytułu naukowego – w zakresie nieobjętym formalnościami związanymi z uznawaniem kwalifikacji zawodowych.

(30) Niniejsze rozporządzenie nie powinno mieć wpływu na przepisy w zakresie koordynacji zabezpieczenia społecznego określone w rozporządzeniach Parlamentu Europejskiego i Rady (WE) nr 883/2004 ([1]) oraz (WE) nr 987/2009 ([2]), które określają prawa i obowiązki ubezpieczonych i instytucji zabezpieczenia społecznego oraz procedury mające zastosowanie w dziedzinie koordynacji zabezpieczenia społecznego.

(31) Na poziomie Unii i na poziomie krajowym ustanowiono szereg sieci i usług, które mają wspierać obywateli i przedsiębiorstwa w działalności transgranicznej. Ważne jest, aby te usługi, w tym istniejące usługi wsparcia lub rozwiązywania problemów ustanowione na poziomie Unii, takie jak Europejskie Centra Konsumenckie, portal „Twoja Europa – Porady", SOLVIT, Punkt Informacyjny IPR, Europe Direct oraz sieć Enterprise Europe Network, stanowiły część Portalu w celu zapewnienia, aby potencjalni użytkownicy mogli je znaleźć. Usługi wymienione w załączniku III ustanowiono na mocy wiążących aktów Unii, podczas gdy inne usługi funkcjonują na zasadzie dobrowolności. Usługi ustanowione na mocy wiążących aktów Unii powinny podlegać wymogom jakości określonym w niniejszym rozporządzeniu. Usługi funkcjonujące na zasadzie dobrowolności powinny spełniać te wymogi jakości, jeżeli mają być one dostępne za pośrednictwem Portalu. Zakres i charakter tych usług, ich struktury zarządzania, obowiązujące terminy oraz dobrowolna, umowna lub inna podstawa ich funkcjonowania nie powinny być zmieniane niniejszym rozporządzeniem. Na przykład w przypadku gdy wsparcie udzielane za pośrednictwem tych usług ma charakter nieformalny, niniejsze rozporządzenie nie powinno mieć skutku w postaci zmiany takiego wsparcia w doradztwo prawne o wiążącym charakterze.

(32) Ponadto państwa członkowskie i Komisja powinny mieć możliwość dodawania do Portalu innych krajowych usług wsparcia lub rozwiązywania problemów – świadczonych przez właściwe organy lub przez podmioty prywatne lub półprywatne, lub organy publiczne, takie jak izby handlowe – lub pozarządowych usług wsparcia dla obywateli, na warunkach określonych w niniejszym rozporządzeniu. Co do zasady właściwe organy powinny być odpowiedzialne za udzielanie pomocy obywatelom i przedsiębiorstwom w zakresie wszelkich zapytań dotyczących mających zastosowanie przepisów i procedur, na które nie można w pełni odpowiedzieć za pośrednictwem usług online. Jednakże w wysoko wyspecjalizowanych obszarach oraz w przypadku gdy usługa świadczona przez podmioty prywatne lub półprywatne spełnia potrzeby użytkowników, państwa członkowskie mogą zaproponować Komisji uwzględnienie takich usług w Portalu, o ile usługi te spełniają wszystkie warunki określone w niniejszym rozporządzeniu oraz nie powielają już uwzględnionych usług wsparcia lub rozwiązywania problemów.

(33) Aby pomóc użytkownikom w znalezieniu właściwej usługi niniejsze rozporządzenie powinno przewidywać wyszukiwarkę usług wsparcia, automatycznie kierującą użytkowników do właściwej usługi.

(34) Zasadnicze znaczenie dla powodzenia Portalu ma przestrzeganie minimalnego wykazu wymogów jakości, aby zapewnić rzetelność zapewnianych informacji i usług, ponieważ w przeciwnym razie wiarygodność Portalu jako całości byłaby poważnie zagrożona. Nadrzędnym celem osiągnięcia zgodności z przepisami jest zapewnienie, aby informacja lub usługa zostały przedstawione w sposób jasny i przyjazny dla użytkownika. Aby zrealizować ten cel, państwa członkowskie mają obowiązek określić w jaki sposób informacje będą prezentowane w przebiegu ścieżki użytkownika. Na przykład, choć otrzymanie, przed rozpoczęciem procedury, informacji o ogólnie dostępnych środkach odwoławczych dostępnych w przypadku negatywnego wyniku procedury jest dla użytkownika pomocne, dużo bardziej przyjazne dla użytkownika jest podawanie wszelkich konkretnych informacji na temat ewentualnych kolejnych kroków, które należy podjąć w takiej sytuacji, na końcu procedury.

([1]) Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 883/2004 z dnia 29 kwietnia 2004 r. w sprawie koordynacji systemów zabezpieczenia społecznego (Dz.U. L 166 z 30.4.2004, s. 1).

([2]) Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 987/2009 z dnia 16 września 2009 r. dotyczące wykonywania rozporządzenia (WE) nr 883/2004 w sprawie koordynacji systemów zabezpieczenia społecznego (Dz.U. L 284 z 30.10.2009, s. 1).

(35) Dostępność informacji dla użytkowników transgranicznych może ulec znacznej poprawie, jeżeli informacje te będą dostępne w języku urzędowym Unii powszechnie rozumianym przez możliwie największą liczbę użytkowników transgranicznych. Język ten powinien być w większości przypadków językiem obcym, którego uczy się jak najwięcej użytkowników w całej Unii, ale w niektórych szczególnych przypadkach, w szczególności w przypadku gdy informacje mają być udostępniane na poziomie lokalnym przez małe gminy w pobliżu granicy państwa członkowskiego, najbardziej odpowiedni może być język używany jako pierwszy język użytkowników transgranicznych w sąsiednim państwie członkowskim. Tłumaczenie z języka urzędowego lub języków urzędowych danego państwa członkowskiego na ten inny język urzędowy Unii powinno dokładnie oddawać treść informacji przekazanych w języku lub językach oryginału. Tłumaczenie może być ograniczone do informacji, których użytkownicy potrzebują do zrozumienia podstawowych przepisów i wymogów mających zastosowanie do ich sytuacji. Chociaż należy zachęcać państwa członkowskie do przetłumaczenia możliwie jak największej ilości informacji na język urzędowy Unii, który jest powszechnie rozumiany przez możliwie największą liczbę użytkowników transgranicznych, ilość informacji, które mają być przetłumaczone zgodnie z niniejszym rozporządzeniem będzie zależeć od zasobów finansowych dostępnych na ten cel, w szczególności zasobów pochodzących z budżetu Unii. Komisja powinna dokonać odpowiednich ustaleń w celu zapewnienia sprawnego dostarczania tłumaczeń państwom członkowskim na ich wniosek. Grupa koordynacyjna Portalu powinna poddać dyskusji i opracować wytyczne dotyczące języka lub języków urzędowych Unii, na które takie informacje powinny zostać przetłumaczone.

(36) Zgodnie z dyrektywą Parlamentu Europejskiego i Rady (UE) 2016/2102 ([1]) państwa członkowskie są zobowiązane do zapewnienia dostępu do stron internetowych swoich organów publicznych zgodnie z zasadami postrzegalności, funkcjonalności, zrozumiałości i integralności oraz zapewnienia, aby ich strony internetowe były zgodne z wymogami określonymi w tej dyrektywie. Komisja oraz państwa członkowskie powinny zapewnić zgodność z Konwencją Narodów Zjednoczonych o prawach osób niepełnosprawnych, w szczególności z jej art. 9 i 21, oraz w celu poprawy dostępu do informacji dla osób niepełnosprawnych intelektualnie, w jak największym stopniu i zgodnie z zasadą proporcjonalności, zapewnić alternatywne rozwiązania w łatwym do zrozumienia języku. Państwa członkowskie, poprzez ratyfikację tej konwencji, oraz Unia, poprzez jej zawarcie ([2]) zobowiązały się do podjęcia odpowiednich środków, aby zapewnić osobom niepełnosprawnym dostęp na równi z innymi osobami do nowych technologii informacyjno-komunikacyjnych (zwanych dalej „ICT") oraz systemów ICT, w tym internetu, poprzez ułatwienie dostępu do informacji dla osób niepełnosprawnych intelektualnie, zapewniając w jak największym stopniu i proporcjonalnie alternatywne rozwiązania w łatwym do zrozumienia języku.

(37) Dyrektywa (UE) 2016/2102 nie ma zastosowania do stron internetowych i aplikacji mobilnych instytucji, organów i jednostek organizacyjnych Unii, jednak Komisja powinna zapewnić, aby wspólny interfejs użytkownika i strony internetowe, za które jest odpowiedzialna i które mają znaleźć się w Portalu, były dostępne dla osób niepełnosprawnych, co oznacza, że muszą one być postrzegalne, funkcjonalne, zrozumiałe i integralne. Postrzegalność oznacza, że informacje i elementy wspólnego interfejsu użytkownika muszą być przedstawiane użytkownikom w sposób, który potrafią oni dostrzec; funkcjonalność oznacza, że elementy wspólnego interfejsu użytkownika i nawigacja muszą być funkcjonalne; zrozumiałość oznacza, że informacje i obsługa wspólnego interfejsu użytkownika muszą być zrozumiałe; a integralność oznacza, że treści muszą być wystarczająco integralne, aby mogły być skutecznie interpretowane przez różnego rodzaju aplikacje klienckie, w tym technologie wspomagające. W odniesieniu do pojęć postrzegalności, funkcjonalności, zrozumiałości i integralności zachęca się Komisję do zapewnienia zgodności z odpowiednimi zharmonizowanymi normami.

(38) W celu ułatwienia uiszczania opłat wymaganych w ramach procedur online lub za korzystanie z usług wsparcia lub rozwiązywania problemów użytkownicy transgraniczni powinni mieć możliwość korzystania z poleceń przelewu lub poleceń zapłaty, zdefiniowanych w rozporządzeniu Parlamentu Europejskiego i Rady (UE) nr 260/2012 ([3]), lub innych powszechnie stosowanych środków płatności transgranicznych, w tym kart debetowych lub kredytowych.

(39) Przydatne jest, aby użytkownicy byli informowani o przewidywanym czasie trwania procedury. W związku z tym powinni być oni informowani o mających zastosowanie terminach lub ustaleniach dotyczących dorozumianego zatwierdzenia lub milczenia administracji lub – jeśli powyższe nie mają zastosowania – przynajmniej o średnim, szacowanym lub orientacyjnym czasie, jakiego dana procedura zwykle wymaga. Takie szacunki lub wskazania powinny jedynie pomagać użytkownikom w planowaniu ich działań lub wszelkich dalszych kroków administracyjnych i nie powinny wywierać skutków prawnych.

([1]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/2102 z dnia 26 października 2016 r. w sprawie dostępności stron internetowych i mobilnych aplikacji organów sektora publicznego (Dz.U. L 327 z 2.12.2016, s. 1).

([2]) Decyzja Rady 2010/48/WE z dnia 26 listopada 2009 r. w sprawie zawarcia przez Wspólnotę Europejską Konwencji Narodów Zjednoczonych o prawach osób niepełnosprawnych (Dz.U. L 23 z 27.1.2010, s. 35).

([3]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 260/2012 z dnia 14 marca 2012 r. ustanawiające wymogi techniczne i handlowe w odniesieniu do poleceń przelewu i poleceń zapłaty w euro oraz zmieniające rozporządzenie (WE) nr 924/2009 (Dz.U. L 94 z 30.3.2012, s. 22).

(40) W niniejszym rozporządzeniu należy również umożliwić weryfikację dowodów dostarczonych przez użytkowników w formie elektronicznej w przypadku gdy dowody te są przedkładane bez pieczęci lub certyfikacji elektronicznej właściwego organu wydającego, lub w przypadku gdy nie jest dostępne narzędzie techniczne utworzone na mocy niniejszego rozporządzenia lub inny system umożliwiający bezpośrednią wymianę lub weryfikację dowodów między właściwymi organami różnych państw członkowskich. W takich przypadkach niniejsze rozporządzenie powinno przewidywać skuteczny mechanizm współpracy administracyjnej między właściwymi organami państw członkowskich, oparty na systemie wymiany informacji na rynku wewnętrznym (zwanym dalej „IMI"), utworzonym na mocy rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1024/2012 ([1]). W takich przypadkach decyzja właściwego organu o zastosowaniu IMI powinna być dobrowolna, ale z chwilą gdy organ ten zwróci się z wnioskiem o przekazanie informacji lub o współpracę za pośrednictwem IMI, właściwy organ, do którego się zwrócono, powinien być zobowiązany do współpracy i do przekazania odpowiedzi. Wniosek można przesłać za pośrednictwem IMI do właściwego organu wydającego dany dowód albo do organu centralnego, który ma być wyznaczony przez państwa członkowskie zgodnie z ich własnymi przepisami administracyjnymi. Aby uniknąć niepotrzebnego powielania oraz z uwagi na fakt, że rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/1191 ([2]) obejmuje część dowodów mających znaczenie w procedurach objętych zakresem stosowania niniejszego rozporządzenia, warunki współpracy w ramach IMI określone w rozporządzeniu (UE) 2016/1191 mogą być również stosowane w odniesieniu do innych dowodów wymaganych w procedurach objętych zakresem stosowania niniejszego rozporządzenia. Aby umożliwić organom i jednostkom organizacyjnym Unii uczestnictwo w IMI, należy zmienić rozporządzenie (UE) nr 1024/2012.

(41) Usługi online zapewniane przez właściwe organy mają kluczowe znaczenie dla poprawy jakości i bezpieczeństwa usług świadczonych na rzecz obywateli i przedsiębiorstw. Organy administracji publicznej w państwach członkowskich coraz częściej starają się ponownie korzystać z raz przedłożonych danych, odstępując od wymogu wielokrotnego przedkładania tych samych informacji przez obywateli i przedsiębiorstwa. Należy ułatwiać ponowne korzystanie z raz przedłożonych danych w odniesieniu do użytkowników transgranicznych w celu zmniejszenia obciążenia administracyjnego.

(42) Aby umożliwić zgodną z prawem transgraniczną wymianę dowodów i informacji poprzez zastosowanie zasady jednorazowości w całej Unii, niniejsze rozporządzenie oraz zasadę jednorazowości należy stosować zgodnie ze wszystkimi mającymi zastosowanie przepisami dotyczącymi ochrony danych, w tym zasadą minimalizacji danych, dokładności, ograniczenia przechowywania, integralności i poufności, konieczności, proporcjonalności i ograniczenia celu. Należy je również wdrażać z zachowaniem pełnej zgodności z zasadami bezpieczeństwa i ochrony prywatności już w fazie projektowania oraz przestrzegając także praw podstawowych osób fizycznych, w tym praw dotyczących uczciwości i przejrzystości.

(43) Państwa członkowskie powinny zapewnić, aby użytkownicy procedur otrzymywali jasne informacje na temat sposobu przetwarzania danych osobowych, które ich dotyczą, zgodnie z art. 13 i 14 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 ([3]) oraz art. 15 i 16 rozporządzenia (UE) 2018/1725 ([4]).

(44) W celu dalszego ułatwienia korzystania z procedur online, w niniejszym rozporządzeniu, zgodnie z zasadą jednorazowości, należy zapewnić podstawy do stworzenia i stosowania w pełni operacyjnego, bezpiecznego i zabezpieczonego systemu technicznego do zautomatyzowanej transgranicznej wymiany dowodów między podmiotami biorącymi udział w danej procedurze, w przypadku gdy obywatele i przedsiębiorstwa złożą w tym przedmiocie wyraźny wniosek. W przypadku gdy wymiana dowodów obejmuje dane osobowe, wniosek należy uznać za wyraźny, jeśli zawiera dobrowolne, konkretne, świadome i jednoznaczne wskazanie – w drodze oświadczenia albo w drodze działania potwierdzającego – że osoba fizyczna życzy sobie dokonania wymiany odpowiednich danych osobowych. Jeśli użytkownik nie jest osobą, której dotyczą dane, procedura online nie powinna mieć wpływu na prawa tej osoby wynikające z rozporządzenia (UE) 2016/679. Transgraniczne stosowanie zasady jednorazowości powinno skutkować tym, że obywatele i przedsiębiorstwa nie będą musieli przedkładać organom publicznym tych samych danych więcej niż raz oraz tym, że dane te będą mogły być również na wniosek użytkownika wykorzystywane do celów przeprowadzania transgranicznych procedur online dotyczących użytkowników transgranicznych. W odniesieniu do właściwego organu wydającego, obowiązek wykorzystania systemu technicznego zautomatyzowanej wymiany dowodów między różnymi państwami członkowskimi powinien mieć zastosowanie jedynie w przypadku, gdy organy zgodnie z prawem wydają w swoim państwie członkowskim dowody w formacie elektronicznym umożliwiającym taką zautomatyzowaną wymianę.

([1]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1024/2012 z dnia 25 października 2012 r. w sprawie współpracy administracyjnej za pośrednictwem systemu wymiany informacji na rynku wewnętrznym i uchylające decyzję Komisji 2008/49/WE („rozporządzenie w sprawie IMI") (Dz.U. L 316 z 14.11.2012, s. 1).

([2]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/1191 z dnia 6 lipca 2016 r. w sprawie promowania swobodnego przepływu obywateli poprzez uproszczenie wymogów dotyczących przedkładania określonych dokumentów urzędowych w Unii Europejskiej i zmieniające rozporządzenie (UE) nr 1024/2012 (Dz.U. L 200 z 26.7.2016, s. 1).

([3]) 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).

([4]) 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 (zob. s. 39 niniejszego Dziennika Urzędowego).

(45) Wszelka transgraniczna wymiana dowodów powinna mieć odpowiednią podstawę prawną, taką jak dyrektywa 2005/36/WE, 2006/123/WE, 2014/24/UE lub 2014/25/UE, lub – w przypadku procedur wymienionych w załączniku II – inne mające zastosowanie przepisy prawa Unii lub prawa krajowego.

(46) W niniejszym rozporządzeniu należy ustanowić ogólną zasadę, zgodnie z którą transgraniczna zautomatyzowana wymiana dowodów odbywa się na wyraźny wniosek użytkownika. Jednakże wymóg ten nie powinien mieć zastosowania w przypadku gdy odpowiednie przepisy prawa Unii lub prawa krajowego pozwalają na zautomatyzowaną transgraniczną wymianę danych bez wyraźnego wniosku użytkownika.

(47) Korzystanie z systemu technicznego utworzonego na mocy niniejszego rozporządzenia powinno pozostać dobrowolne, a użytkownik powinien mieć możliwość przedkładania dowodów za pomocą innych metod niż system techniczny. Użytkownik powinien mieć możliwość podglądu dowodów oraz prawo do podjęcia decyzji o nieprzeprowadzaniu wymiany dowodów w przypadku, gdy po skorzystaniu z możliwości podglądu dowodów, które mają być wymieniane, odkryje on, że informacje są nieścisłe, nieaktualne lub wykraczają poza to, co jest konieczne w kontekście danej procedury. Danych zawartych w podglądzie nie powinno się przechowywać dłużej niż jest to konieczne z technicznego punktu widzenia.

(48) Zabezpieczony system techniczny, który powinien powstać na potrzeby wymiany dowodów na mocy niniejszego rozporządzenia, powinien również dawać właściwym organom występującym z wnioskiem pewność, że dowody zostały dostarczone przez odpowiedni organ wydający. Przed przyjęciem informacji przekazanych przez użytkownika w kontekście danej procedury właściwy organ powinien móc zweryfikować informacje, w przypadku gdy budzą one wątpliwości, oraz potwierdzić ich dokładność.

(49) Istnieje już szereg modułów oferujących podstawowe możliwości, które można wykorzystać do utworzenia systemu technicznego, takich jak instrument „Łącząc Europę", ustanowiony na mocy rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1316/2013 ([1]), oraz moduły do elektronicznego dostarczania dokumentów i do potwierdzania tożsamości elektronicznej, które stanowią część tego instrumentu. Moduły te obejmują specyfikacje techniczne, przykładowe oprogramowanie i usługi wsparcia, oraz mają na celu zapewnienie interoperacyjności między systemami ICT istniejącymi w różnych państwach członkowskich, tak aby obywatele, przedsiębiorstwa i organy administracyjne, niezależnie od tego, gdzie znajdują się w Unii, mogły bezproblemowo korzystać z cyfrowych usług publicznych.

(50) System techniczny utworzony na mocy niniejszego rozporządzenia powinien być dostępny jako dodatkowy system względem innych systemów zapewniających mechanizmy współpracy między organami, takich jak IMI, oraz nie powinien mieć wpływu na inne systemy, w tym na system przewidziany rozporządzeniu (WE) nr 987/2009, jednolity europejski dokument zamówienia na podstawie dyrektywy 2014/24/UE, system elektronicznej wymiany informacji dotyczących zabezpieczenia społecznego na podstawie rozporządzenia (WE) nr 987/2009, europejską legitymację zawodową na podstawie dyrektywy 2005/36/WE, integrację krajowych rejestrów oraz integrację rejestrów centralnych, handlowych i rejestrów spółek na podstawie dyrektywy Parlamentu Europejskiego i Rady (UE) 2017/1132 ([2]) oraz wzajemne połączenie rejestrów upadłości na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2015/848 ([3]).

(51) W celu zapewnienia jednolitych warunków wdrożenia systemu technicznego umożliwiającego zautomatyzowaną wymianę dowodów, należy powierzyć Komisji uprawnienia wykonawcze do określenia, w szczególności, specyfikacji technicznych i operacyjnych systemu służącego do przetwarzania wniosku użytkownika o wymianę dowodów i do przekazywania takich dowodów, a także uprawnienia wykonawcze do ustanowienia przepisów niezbędnych do zapewnienia integralności i poufności takiego przekazywania. Uprawnienia te powinny być wykonywane zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 182/2011 ([4]).

(52) Mając na uwadze zapewnienie, aby system techniczny zapewniał wysoki poziom bezpieczeństwa transgranicznego stosowania zasady jednorazowości, przy przyjmowaniu aktów wykonawczych określających specyfikacje takiego systemu technicznego, Komisja powinna należycie uwzględnić normy i specyfikacje techniczne opracowane przez europejskie i międzynarodowe organizacje i organy normalizacyjne, w szczególności przez Europejski Komitet

([1]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1316/2013 z dnia 11 grudnia 2013 r. ustanawiające instrument „Łącząc Europę", zmieniające rozporządzenie (UE) nr 913/2010 oraz uchylające rozporządzenia (WE) nr 680/2007 i (WE) nr 67/2010 (Dz.U. L 348 z 20.12.2013, s. 129).

([2]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2017/1132 z dnia 14 czerwca 2017 r. w sprawie niektórych aspektów prawa spółek (Dz.U. L 169 z 30.6.2017, s. 46).

([3]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2015/848 z dnia 20 maja 2015 r. w sprawie postępowania upadłościowego (Dz.U. L 141 z 5.6.2015, s. 19).

([4]) 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).

Normalizacyjny (CEN), Europejski Instytut Norm Telekomunikacyjnych (ETSI), Międzynarodową Organizację Normalizacyjną (ISO) oraz Międzynarodowy Związek Telekomunikacyjny (ITU), a także standardy bezpieczeństwa, o których mowa w art. 32 rozporządzenia (UE) 2016/679 i art. 22 rozporządzenia (UE) 2018/1725.

(53) W przypadku gdy jest to konieczne w celu zapewnienia opracowania, dostępności, utrzymania, nadzoru, monitorowania i zarządzania bezpieczeństwem części systemu technicznego, za które odpowiada Komisja, Komisja powinna zwrócić się o opinię Europejskiego Inspektora Ochrony Danych.

(54) Właściwe organy oraz Komisja powinny zapewnić, aby informacje, procedury i usługi, za które odpowiadają, były zgodne z kryteriami jakości. Koordynatorzy krajowi wyznaczeni na podstawie niniejszego rozporządzenia oraz Komisja powinni w regularnych odstępach czasu nadzorować przestrzeganie kryteriów jakości i kryteriów bezpieczeństwa, odpowiednio na poziomie krajowym i na poziomie Unii, oraz rozwiązywać wszelkie pojawiające się problemy. Koordynatorzy krajowi powinni ponadto pomagać Komisji w monitorowaniu funkcjonowania systemu technicznego umożliwiającego transgraniczną wymianę dowodów. Niniejsze rozporządzenie powinno przyznawać Komisji wachlarz środków umożliwiających reakcję na pogorszenie jakości usług oferowanych za pośrednictwem Portalu, zależnie od wagi i utrzymywania się takiego pogorszenia jakości, z uwzględnieniem, w razie konieczności, udziału grupy koordynacyjnej Portalu. Powinno to pozostać bez uszczerbku dla ogólnej odpowiedzialności Komisji za monitorowanie przestrzegania niniejszego rozporządzenia.

(55) Niniejsze rozporządzenie powinno określać najważniejsze funkcje narzędzi technicznych wspomagających funkcjonowanie Portalu, w szczególności wspólnego interfejsu użytkownika, repozytorium linków oraz wspólnej wyszukiwarki usług wsparcia. Wspólny interfejs użytkownika powinien zapewniać, aby użytkownicy mogli łatwo znaleźć informacje, procedury oraz usługi wsparcia i rozwiązywania problemów na stronach internetowych na poziomie krajowym i na poziomie Unii. Państwa członkowskie oraz Komisja powinny dążyć do podawania linków do jednego źródła informacji wymaganych dla Portalu, aby uniknąć dezorientacji wśród użytkowników wynikającej z podania różnych lub całkowicie lub częściowo powielających się źródeł tych samych informacji. Nie powinno to uniemożliwiać podawania linków do tych samych informacji oferowanych przez lokalne lub regionalne właściwe organy, a dotyczących różnych obszarów geograficznych. Nie powinno to również uniemożliwiać powielania pewnych informacji, w przypadku gdy jest to nieuniknione lub pożądane, na przykład w przypadku gdy na krajowych stronach internetowych przypomina się lub opisuje niektóre unijne prawa, obowiązki i przepisy, aby poprawić łatwość obsługi. Aby zminimalizować ręczną obsługę przy aktualizacji linków, które mają być wykorzystywane przez wspólny interfejs użytkownika, należy tam, gdzie jest to technicznie możliwe, wprowadzić bezpośrednie połączenie między odpowiednimi systemami technicznymi państw członkowskich i repozytorium linków. Wspólne wspomagające narzędzia ICT mogłyby korzystać ze słownika podstawowych usług publicznych (zwanego dalej „CPSV"), aby ułatwić interoperacyjność z krajowymi katalogami usług i z semantyką krajową. Państwa członkowskie należy zachęcać do stosowania CPSV, ale mogą one zdecydować się na stosowanie rozwiązań krajowych. Informacje zawarte w repozytorium linków powinny być publicznie dostępne w otwartym, powszechnie używanym i nadającym się do odczytu maszynowego formacie danych, na przykład za pomocą interfejsów programowania aplikacji (API), aby umożliwić ich ponowne wykorzystanie.

(56) Wyszukiwarka we wspólnym interfejsie użytkownika powinna prowadzić użytkowników do informacji, których potrzebują, niezależnie od tego, czy znajdują się one na stronach internetowych na poziomie Unii, czy na poziomie krajowym. Ponadto, jako alternatywny sposób kierowania użytkowników do użytecznych informacji, nadal przydatne będzie tworzenie linków między istniejącymi i uzupełniającymi się witrynami lub stronami internetowymi, usprawniając i grupując je w możliwie największym stopniu, oraz tworzenie linków między stronami internetowymi i witrynami na poziomie Unii i na poziomie krajowym, zapewniającymi dostęp do usług i informacji online.

(57) Niniejsze rozporządzenie powinno również określać wymogi jakości w odniesieniu do wspólnego interfejsu użytkownika. Komisja powinna zapewniać, aby wspólny interfejs użytkownika spełniał te wymogi, a interfejs ten powinien w szczególności być dostępny i udostępniany online za pośrednictwem różnych kanałów, a także powinien być łatwy w obsłudze.

(58) W celu zapewnienia jednolitych warunków wdrożenia rozwiązań technicznych wspomagających Portal, należy powierzyć Komisji uprawnienia wykonawcze do określania, w stosownych przypadkach, mających zastosowanie norm i wymogów dotyczących interoperacyjności w celu ułatwienia wyszukiwania informacji dotyczących przepisów i obowiązków, procedur oraz usług wsparcia i rozwiązywania problemów, za które odpowiadają państwa członkowskie oraz Komisja. Uprawnienia te powinny być wykonywane zgodnie z rozporządzeniem (UE) nr 182/2011.

(59) Niniejsze rozporządzenie powinno również jasno rozdzielać między Komisję i państwa członkowskie odpowiedzialność za opracowanie, dostępność, utrzymanie i bezpieczeństwo aplikacji ICT wspomagających Portal. W ramach wykonywania zadań związanych z utrzymaniem Portalu Komisja i państwa członkowskie powinny regularnie monitorować prawidłowość funkcjonowania tych aplikacji ICT.

(60) Aby rozwinąć pełny potencjał różnych obszarów informacji, procedur oraz usług wsparcia i rozwiązywania problemów, które powinny zostać uwzględnione w Portalu, należy znacząco poprawić świadomość odbiorców docelowych na temat ich istnienia i sposobu funkcjonowania. Uwzględnienie tych informacji, procedur i usług w Portalu powinno znacznie ułatwić użytkownikom wyszukiwanie potrzebnych im informacji, procedur oraz usług wsparcia i rozwiązywania problemów, nawet jeżeli nie wiedzą oni o istnieniu którychkolwiek z nich. Ponadto niezbędne będą skoordynowane działania promocyjne w celu zapewnienia, aby obywatele i przedsiębiorstwa w całej Unii dowiedzieli się o istnieniu Portalu i wynikających z niego korzyściach. Takie działania promocyjne powinny obejmować optymalizację wyszukiwarek oraz inne internetowe działania służące budowaniu świadomości, ponieważ właśnie one są najbardziej efektywne kosztowo oraz mają potencjał dotarcia do największej liczby odbiorców docelowych. Aby osiągnąć najwyższą skuteczność, należy skoordynować te działania promocyjne w ramach grupy koordynacyjnej Portalu, a państwa członkowskie powinny dopasować swoje działania promocyjne w taki sposób, aby we wszystkich mających znaczenie kontekstach pojawiała się wspólna marka z zachowaniem możliwości łączenia marki Portalu z inicjatywami krajowymi.

(61) Wszystkie instytucje, organy i jednostki organizacyjne Unii należy zachęcać do promowania Portalu poprzez umieszczanie jego logo i linków do niego na wszystkich odpowiednich stronach internetowych, za które odpowiadają.

(62) Nazwa, pod którą Portal ma być znany i promowany publicznie, powinna brzmieć „Your Europe". Wspólny interfejs użytkownika powinien być widoczny i łatwy do znalezienia, szczególnie na odpowiednich unijnych i krajowych stronach internetowych. Logo Portalu powinno być widoczne na odpowiednich unijnych i krajowych stronach internetowych.

(63) Aby uzyskać odpowiednie informacje umożliwiające pomiar i poprawę funkcjonowania Portalu, niniejsze rozporządzenie powinno wprowadzić wymóg, aby właściwe organy i Komisja gromadziły i analizowały dane dotyczące korzystania z różnych obszarów informacji, procedur i usług oferowanych za pośrednictwem Portalu. Gromadzenie danych statystycznych dotyczących użytkowników, takich jak dane dotyczące liczby odwiedzin na określonych stronach internetowych, liczby użytkowników w danym państwie członkowskim w porównaniu z liczbą użytkowników z innych państw członkowskich, terminów stosowanych przy wyszukiwaniu, najczęściej odwiedzanych stron internetowych, stron internetowych, z których pochodzą odesłania, lub liczby, miejsca pochodzenia i przedmiotu wniosków o wsparcie, powinno poprawić funkcjonowanie Portalu, pomagając w identyfikacji odbiorców, rozwoju działań promocyjnych oraz poprawie jakości oferowanych usług. Aby uniknąć powielania, gromadzenie takich danych powinno uwzględniać przeprowadzaną co roku przez Komisję analizę porównawczą dotyczącą administracji elektronicznej.

(64) W celu zapewnienia jednolitych warunków wykonywania niniejszego rozporządzenia, należy powierzyć Komisji uprawnienia wykonawcze do określenia jednolitych przepisów dotyczących metody gromadzenia i wymiany danych statystycznych dotyczących użytkowników. Uprawnienia te powinny być wykonywane zgodnie z rozporządzeniem (UE) nr 182/2011.

(65) Jakość Portalu zależy od jakości unijnych i krajowych usług zapewnianych za pośrednictwem Portalu. Dlatego jakość informacji, procedur oraz usług wsparcia i rozwiązywania problemów dostępnych za pośrednictwem Portalu należy również regularnie monitorować poprzez narzędzie do gromadzenia informacji zwrotnych od użytkowników, za pośrednictwem którego użytkownicy proszeni są o ocenę zakresu i jakości informacji, procedur oraz usług wsparcia i rozwiązywania problemów, z których skorzystali, oraz o przekazanie informacji zwrotnych na ten temat. Te informacje zwrotne powinny być gromadzone we wspólnym narzędziu, do którego dostęp powinny mieć Komisja, właściwe organy i koordynatorzy krajowi. W celu zapewnienia jednolitych warunków wykonywania niniejszego rozporządzenia w odniesieniu do wspólnych funkcji narzędzi do gromadzenia informacji zwrotnych od użytkowników oraz szczegółowych ustaleń dotyczących gromadzenia i udostępniania informacji zwrotnych od użytkowników, należy powierzyć Komisji uprawnienia wykonawcze. Uprawnienia te powinny być wykonywane zgodnie z rozporządzeniem (UE) nr 182/2011. Komisja powinna publikować online, w zanonimizowanej formie, przegląd problemów wynikających z informacji, głównych danych statystycznych dotyczących użytkowników oraz głównych informacji zwrotnych od użytkowników, zgromadzonych zgodnie z niniejszym rozporządzeniem.

(66) Ponadto, Portal powinien obejmować narzędzie do gromadzenia informacji zwrotnych, umożliwiające użytkownikom sygnalizowanie, dobrowolnie i anonimowo, wszelkich problemów i trudności napotkanych przez nich podczas korzystania z ich praw na rynku wewnętrznym. Narzędzie to powinno być traktowane jedynie jako uzupełnienie mechanizmów rozpatrywania skarg, ponieważ nie można w nim zapewnić spersonalizowanych odpowiedzi dla użytkowników. Otrzymane informacje powinny być połączone ze zagregowanymi informacjami pochodzącymi z usług wsparcia i rozwiązywania problemów na temat rozpatrywanych spraw w celu uzyskania oglądu rynku wewnętrznego, takiego jak jest on postrzegany przez użytkowników, oraz w celu określenia obszarów problematycznych wymagających podjęcia działań w przyszłości, aby poprawić funkcjonowanie rynku wewnętrznego. Ogląd ten powinien być powiązany z istniejącymi narzędziami sprawozdawczymi, takimi jak tabela wyników jednolitego rynku.

(67) Niniejsze rozporządzenie nie powinno mieć wpływu na prawo państw członkowskich do decydowania o tym, kto powinien pełnić rolę koordynatora krajowego. Państwa członkowskie powinny móc dostosowywać funkcje i obowiązki swoich koordynatorów krajowych związane z Portalem do swoich wewnętrznych struktur administracyjnych. Państwa członkowskie powinny móc wyznaczać dodatkowych koordynatorów krajowych do wykonywania – samodzielnie lub wspólnie z innymi – zadań wynikających z niniejszego rozporządzenia, odpowiedzialnych za dział administracji lub region geograficzny, lub w oparciu o inne kryteria. Państwa członkowskie powinny poinformować Komisję o tożsamości jednego koordynatora krajowego, który został przez nie wyznaczony do kontaktów z Komisją.

(68) Należy powołać grupę koordynacyjną Portalu złożoną z koordynatorów krajowych i pod przewodnictwem Komisji w celu ułatwienia stosowania niniejszego rozporządzenia, w szczególności poprzez wymianę najlepszych praktyk i współpracę na rzecz poprawy spójności prezentacji informacji wymaganych na mocy niniejszego rozporządzenia. Prace grupy koordynacyjnej Portalu powinny uwzględniać cele określone w rocznym programie prac, który Komisja powinna przedstawić tej grupie do rozpatrzenia. Roczny program prac powinien mieć formę wytycznych lub zaleceń, mających charakter niewiążący dla państw członkowskich. Na wniosek Parlamentu Europejskiego Komisja może podjąć decyzję, aby zwrócić się do Parlamentu o wysłanie ekspertów do udziału w posiedzeniach grupy koordynacyjnej Portalu.

(69) W niniejszym rozporządzeniu należy wyjaśnić, które części Portalu mają być finansowane z budżetu Unii, a za które będą odpowiadały państwa członkowskie. Komisja powinna pomagać państwom członkowskim w identyfikowaniu modułów ICT, które można ponownie wykorzystać, oraz w zakresie finansowania za pośrednictwem różnych funduszy i programów na poziomie Unii, które mogą wnieść wkład w pokrycie kosztów dostosowania i rozwoju ICT potrzebnego na poziomie krajowym do zapewnienia zgodności z niniejszym rozporządzeniem. Budżet niezbędny do wykonania niniejszego rozporządzenia powinien być zgodny z mającymi zastosowanie wieloletnimi ramami finansowymi.

(70) Państwa członkowskie zachęca się do większej koordynacji, wymiany i współpracy między sobą w celu zwiększenia ich możliwości strategicznych, operacyjnych, badawczych i rozwojowych w obszarze cyberbezpieczeństwa, w szczególności poprzez wdrożenie bezpieczeństwa sieci i informacji, o którym mowa w dyrektywie Parlamentu Europejskiego i Rady (UE) 2016/1148 ([1]), aby wzmocnić bezpieczeństwo i odporność ich administracji publicznej i usług publicznych. Państwa członkowskie zachęca się do zwiększenia bezpieczeństwa transakcji i do zapewnienia wystarczającego poziomu zaufania do środków elektronicznych poprzez skorzystanie z ram eIDAS określonych w rozporządzeniu (UE) nr 910/2014, a w szczególności odpowiednich poziomów bezpieczeństwa. Państwa członkowskie mogą podejmować środki zgodnie z prawem Unii, aby zagwarantować cyberbezpieczeństwo oraz zapobiegać oszustwom dotyczącym tożsamości lub innym formom oszustw.

(71) W przypadku gdy stosowanie niniejszego rozporządzenia wiąże się z przetwarzaniem danych osobowych, powinno ono odbywać się zgodnie z prawem Unii dotyczącym ochrony danych osobowych, w szczególności z rozporządzeniem (UE) 2016/679 i rozporządzeniem (UE) 2018/1725. W kontekście niniejszego rozporządzenia zastosowanie powinna mieć również dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 ([2]). Jak przewidziano w rozporządzeniu (UE) 2016/679 państwa członkowskie mogą zachować lub wprowadzić dalsze warunki, w tym ograniczenia, w odniesieniu do przetwarzania danych dotyczących zdrowia, a także mogą przewidzieć bardziej szczegółowe przepisy dotyczące przetwarzania danych osobowych pracowników w kontekście zatrudnienia.

(72) Niniejsze rozporządzenie powinno promować i ułatwić usprawnienie struktur zarządzania dla usług objętych Portalem. W tym celu Komisja, w ścisłej współpracy z państwami członkowskimi, powinna dokonać przeglądu istniejących struktur zarządzania i w razie konieczności dostosować je, aby unikać powielania i niedociągnięć.

(73) Celem niniejszego rozporządzenia jest zapewnienie użytkownikom działającym w innych państwach członkowskich dostępu online do pełnych, wiarygodnych, przystępnych i zrozumiałych informacji unijnych i krajowych na temat praw, przepisów i obowiązków, do procedur online w pełni funkcjonalnych dla użytkowników transgranicznych oraz do usług wsparcia i rozwiązywania problemów. Ponieważ cel ten nie może zostać osiągnięty w sposób wystarczający przez państwa członkowskie, natomiast ze względu na rozmiary i skutki niniejszego rozporządzenia, możliwe jest jego lepsze osiągnięcie na poziomie Unii, może ona podjąć działania zgodnie z zasadą pomocniczości określoną w art. 5 Traktatu o Unii Europejskiej. Zgodnie z zasadą proporcjonalności określoną w tym artykule, niniejsze rozporządzenie nie wykracza poza to, co jest konieczne do osiągnięcia tego celu.

([1]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.U. L 194 z 19.7.2016, s. 1).

([2]) 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).

(74) Aby państwa członkowskie i Komisja mogły opracować i wdrożyć narzędzia niezbędne do nadania skuteczności niniejszemu rozporządzeniu, stosowanie niektórych jego przepisów należy rozpocząć po upływie dwóch lat od jego wejścia w życie. Organom gminnym należy umożliwić wdrożenie wymogu udostępniania informacji dotyczących przepisów, procedur oraz usług wsparcia i rozwiązywania problemów, za które odpowiadają, w terminie czterech lat po wejściu w życie niniejszego rozporządzenia. Przepisy niniejszego rozporządzenia dotyczące procedur, które mają być oferowane w pełni online, transgranicznego dostępu do procedur online oraz systemu technicznego służącego do zautomatyzowanej transgranicznej wymiany dowodów zgodnie z zasadą jednorazowości powinny zostać wdrożone w terminie najpóźniej przed upływem pięciu lat po wejściu w życie niniejszego rozporządzenia.

(75) Niniejsze rozporządzenie nie narusza praw podstawowych i jest zgodne z zasadami uznanymi w szczególności w Karcie praw podstawowych Unii Europejskiej oraz powinno być wykonywane zgodnie z tymi prawami i zasadami.

(76) Zgodnie z art. 28 ust. 2 rozporządzenia (WE) nr 45/2001 Parlamentu Europejskiego i Rady ([1]) skonsultowano się z Europejskim Inspektorem Ochrony Danych, który wydał opinię w dniu 1 sierpnia 2017 r. ([2]),

PRZYJMUJĄ NINIEJSZE ROZPORZĄDZENIE:

ROZDZIAŁ I

PRZEPISY OGÓLNE

Artykuł 1

Przedmiot

1. Niniejsze rozporządzenie ustanawia przepisy dotyczące:

a) tworzenia i funkcjonowania jednolitego portalu cyfrowego, aby zapewnić obywatelom i przedsiębiorstwom łatwy dostęp do wysokiej jakości informacji, efektywnych procedur oraz skutecznych usług wsparcia i rozwiązywania problemów w odniesieniu do przepisów unijnych i krajowych mających zastosowanie do obywateli i przedsiębiorstw korzystających lub zamierzających korzystać ze swoich praw wynikających z prawa Unii w dziedzinie rynku wewnętrznego w rozumieniu art. 26 ust. 2 TFUE;

b) korzystania z procedur przez użytkowników transgranicznych oraz wdrożenia zasady jednorazowości w związku z procedurami wymienionymi w załączniku II do niniejszego rozporządzenia oraz procedurami przewidzianymi w dyrektywach 2005/36/WE, 2006/123/WE, 2014/24/UE i 2014/25/UE;

c) zgłaszania przeszkód na rynku wewnętrznym w oparciu o gromadzenie informacji zwrotnych od użytkowników oraz danych statystycznych dotyczących usług objętych jednolitym portalem cyfrowym.

2. W przypadku sprzeczności między niniejszym rozporządzeniem a przepisami innego aktu Unii regulującymi określone aspekty przedmiotu objętego zakresem stosowania niniejszego rozporządzenia pierwszeństwo mają przepisy tego innego aktu Unii.

3. Niniejsze rozporządzenie nie ma wpływu na istotę jakichkolwiek procedur określonych na poziomie Unii lub na poziomie krajowym w którymkolwiek z obszarów objętych zakresem stosowania niniejszego rozporządzenia, ani na prawa przyznane poprzez takie procedury. Ponadto, niniejsze rozporządzenie nie ma również wpływu na środki podjęte zgodnie z prawem Unii w celu zagwarantowania cyberbezpieczeństwa oraz w celu zapobiegania oszustwom.

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

([2]) Dz.U. C 340 z 11.10.2017, s. 6.

Artykuł 2

Utworzenie jednolitego portalu cyfrowego

1. Jednolity portal cyfrowy (zwany dalej „Portalem") zostaje utworzony przez Komisję i państwa członkowskie zgodnie z niniejszym rozporządzeniem. Portal składa się ze wspólnego interfejsu użytkownika zarządzanego przez Komisję (zwanego dalej „wspólnym interfejsem użytkownika"), który jest zintegrowany z portalem „Twoja Europa" oraz umożliwia dostęp do odpowiednich unijnych i krajowych stron internetowych.

2. Portal umożliwia dostęp do:

a) informacji na temat praw, obowiązków i przepisów określonych w prawie Unii i prawie krajowym, które mają zastosowanie do użytkowników korzystających lub zamierzających korzystać ze swoich praw wynikających z prawa Unii w dziedzinie rynku wewnętrznego w obszarach wymienionych w załączniku I;

b) informacji na temat procedur online i offline oraz linków do procedur online, w tym procedur objętych załącznikiem II, ustanowionych na poziomie Unii lub na poziomie krajowym, aby umożliwić użytkownikom korzystanie z praw i przestrzeganie obowiązków i przepisów w dziedzinie rynku wewnętrznego w obszarach wymienionych w załączniku I;

c) informacji na temat usług wsparcia i rozwiązywania problemów oraz linków do tych usług, wymienionych w załączniku III lub o których mowa w art. 7, z których mogą korzystać obywatele i przedsiębiorstwa w przypadku pytań lub problemów dotyczących praw, obowiązków, przepisów lub procedur, o których mowa w lit. a) i b) niniejszego ustępu.

3. Wspólny interfejs użytkownika musi być dostępny we wszystkich językach urzędowych Unii.

Artykuł 3

Definicje

Do celów niniejszego rozporządzenia stosuje się następujące definicje:

1) „użytkownik" oznacza obywatela Unii, osobę fizyczną mającą miejsce pobytu w państwie członkowskim albo osobę prawną mającą siedzibę statutową w państwie członkowskim, korzystających za pośrednictwem Portalu z informacji, procedur lub usług wsparcia i rozwiązywania problemów, o których mowa w art. 2 ust. 2;

2) „użytkownik transgraniczny" oznacza użytkownika znajdującego się w sytuacji, która nie ogranicza się pod każdym względem do jednego państwa członkowskiego;

3) „procedura" oznacza sekwencję czynności, które użytkownicy muszą wykonać w celu spełnienia wymogów lub uzyskania od właściwego organu decyzji, aby móc korzystać ze swoich praw, o których mowa w art. 2 ust. 2 lit. a);

4) „właściwy organ" oznacza każdy organ lub podmiot państwa członkowskiego utworzony na poziomie krajowym, regionalnym lub lokalnym, który ma określone obowiązki dotyczące informacji, procedur oraz usług wsparcia i rozwiązywania problemów objętych zakresem stosowania niniejszego rozporządzenia;

5) „dowody" oznaczają wszelkie dokumenty lub dane, w tym tekst lub nagrania dźwiękowe, wizualne lub audiowizualne, niezależnie od zastosowanego nośnika, wymagane przez właściwy organ w celu udowodnienia faktów lub spełnienia wymogów procedur, o których mowa w art. 2 ust. 2 lit. b).

ROZDZIAŁ II

USŁUGI PORTALU

Artykuł 4

Dostęp do informacji

1. Państwa członkowskie zapewniają, aby użytkownicy mieli łatwy dostęp online na ich krajowych stronach internetowych do następujących informacji:

a) informacji na temat tych praw, obowiązków i przepisów, o których mowa w art. 2 ust. 2 lit. a), które wynikają z prawa krajowego;

b) informacji na temat tych procedur, o których mowa w art. 2 ust. 2 lit. b), które określone są na poziomie krajowym;

c) informacji na temat tych usług wsparcia i rozwiązywania problemów, o których mowa w art. 2 ust. 2 lit. c), które zapewniane są na poziomie krajowym.

2. Komisja zapewnia, aby portal „Twoja Europa" umożliwiał użytkownikom łatwy dostęp online do następujących informacji:

a) informacji na temat tych praw, obowiązków i przepisów, o których mowa w art. 2 ust. 2 lit. a), które wynikają z prawa Unii;

b) informacji na temat tych procedur, o których mowa w art. 2 ust. 2 lit. b), które określone są na poziomie Unii;

c) informacji na temat tych usług wsparcia i rozwiązywania problemów, o których mowa w art. 2 ust. 2 lit. c), które zapewniane są na poziomie Unii.

Artykuł 5

Dostęp do informacji nieobjętych załącznikiem I

1. Państwa członkowskie oraz Komisja mogą udostępniać linki do informacji niewymienionych w załączniku I, oferowanych przez właściwe organy, Komisję lub organy i jednostki organizacyjne Unii, pod warunkiem że informacje te są objęte zakresem Portalu określonym w art. 1 ust. 1 lit. a) oraz spełniają wymogi jakości określone w art. 9.

2. Linki do informacji, o których mowa w ust. 1 niniejszego artykułu, udostępnia się zgodnie z art. 19 ust. 2 i 3.

3. Przed aktywowaniem jakichkolwiek linków Komisja sprawdza, czy warunki określone w ust. 1 są spełnione oraz konsultuje się z grupą koordynacyjną Portalu.

Artykuł 6

Procedury, które mają być oferowane w pełni online

1. Każde państwo członkowskie zapewnia, aby użytkownicy mieli dostęp do każdej z procedur wymienionych w załączniku II w pełni online oraz mogli je przeprowadzać w pełni online, w przypadku gdy takie procedury zostały ustanowione w danym państwie członkowskim.

2. Procedury, o których mowa w ust. 1, uznawane są za w pełni online w przypadku gdy:

a) identyfikacja użytkowników, dostarczanie informacji i dowodów potwierdzających oraz podpis i ostateczne przedłożenie mogą zostać przeprowadzone drogą elektroniczną na odległość za pośrednictwem kanału usług, który umożliwia użytkownikom spełnienie wymogów związanych z daną procedurą w przyjazny dla użytkownika i uporządkowany sposób;

b) użytkownikom wydawane jest automatycznie potwierdzenia odbioru, chyba że wynik danej procedury dostarczany jest natychmiast;

c) wynik procedury jest dostarczany drogą elektroniczną lub, gdy jest to konieczne do zapewnienia zgodności z mającym zastosowanie prawem Unii lub prawem krajowym, dostarczany jest fizycznie; oraz

d) użytkownicy otrzymują elektroniczne powiadomienie o zakończeniu procedury.

3. W przypadku gdy, w wyjątkowych okolicznościach uzasadnionych nadrzędnym interesem publicznym w obszarach bezpieczeństwa publicznego, zdrowia publicznego lub zwalczania nadużyć finansowych, zamierzonego celu nie można osiągnąć w pełni online, państwa członkowskie mogą wymagać od użytkownika stawienia się osobiście przed właściwym organem na pewnym etapie procedury. W takich wyjątkowych przypadkach państwa członkowskie ograniczają taką fizyczną obecność do tego, co jest ściśle niezbędne i obiektywnie uzasadnione, oraz zapewniają, aby pozostałe etapy procedury mogły być przeprowadzone w pełni online. Państwa członkowskie zapewniają również, aby wymóg fizycznej obecności nie prowadził do dyskryminacji użytkowników transgranicznych.

4. Państwa członkowskie powiadamiają i wyjaśniają za pośrednictwem wspólnego repozytorium dostępnego Komisji i innym państwom członkowskim powody i okoliczności, w których obecność fizyczna może być wymagana w związku z etapami procedury, o których mowa w ust. 3, oraz powody i okoliczności, w których konieczne jest fizyczne dostarczenie wyniku procedury, o czym mowa w ust. 2 lit. c).

5. Niniejszy artykuł nie uniemożliwia państwom członkowskim oferowania użytkownikom dodatkowych możliwości dostępu do procedur i przeprowadzania procedur, o których mowa w art. 2 ust. 2 lit. b), w inny sposób niż kanałami online ani bezpośredniego kontaktowania się z użytkownikami.

Artykuł 7

Dostęp do usług wsparcia i rozwiązywania problemów

1. Państwa członkowskie oraz Komisja zapewniają użytkownikom, w tym użytkownikom transgranicznym, łatwy dostęp online za pośrednictwem różnych kanałów do usług wsparcia i rozwiązywania problemów, o których mowa w art. 2 ust. 2 lit. c).

2. Koordynatorzy krajowi, o których mowa w art. 28, oraz Komisja mogą udostępniać linki do usług wsparcia i rozwiązywania problemów zapewnianych przez właściwe organy, Komisję lub organy i jednostki organizacyjne Unii, innych niż usługi wymienione w załączniku III, zgodnie z art. 19 ust. 2 i 3, o ile usługi takie spełniają wymogi jakości określone w art. 11 i 16.

3. W przypadku gdy jest to konieczne do zaspokojenia potrzeb użytkowników, koordynator krajowy może zaproponować Komisji, aby w Portalu uwzględnione zostały linki do usług wsparcia i rozwiązywania problemów zapewnianych przez podmioty prywatne lub półprywatne, jeżeli usługi te spełniają następujące warunki:

a) oferują informacje lub wsparcie w obszarach i w celach objętych zakresem stosowania niniejszego rozporządzenia oraz mają charakter uzupełniający w stosunku do usług już uwzględnionych w Portalu;

b) są oferowane bezpłatnie lub w cenach przystępnych dla mikroprzedsiębiorstw, organizacji non-profit i obywateli; oraz

c) spełniają wymogi określone w art. 8, 11 i 16.

4. W przypadku gdy koordynator krajowy proponuje uwzględnienie linku zgodnie z ust. 3 niniejszego artykułu oraz udostępnia taki link zgodnie z art. 19 ust. 3, Komisja ocenia, czy usługa, która ma zostać dodana za pomocą linku, spełnia warunki określone w ust. 3 niniejszego artykułu, a jeśli tak, aktywuje dany link.

Jeżeli Komisja stwierdzi, że usługa, która ma zostać dodana, nie spełnia warunków określonych w ust. 3, informuje koordynatora krajowego o powodach nieaktywowania linku.

Artykuł 8

Wymogi jakości dotyczące dostępności sieci

Komisja zwiększa dostępność tych witryn i stron internetowych, za pomocą których udziela dostępu do informacji, o których mowa w art. 4 ust. 2, oraz do usług wsparcia i rozwiązywania problemów, o których mowa w art. 7, dzięki zwiększeniu postrzegalności, funkcjonalności, zrozumiałości i integralności tych witryn i stron internetowych.

ROZDZIAŁ III

WYMOGI JAKOŚCI

SEKCJA 1

Wymogi jakości dotyczące informacji na temat praw, obowiązków i przepisów, na temat procedur oraz na temat usług wsparcia i rozwiązywania problemów

Artykuł 9

Jakość informacji na temat praw, obowiązków i przepisów

1. W przypadku gdy państwa członkowskie oraz Komisja są odpowiedzialne zgodnie z art. 4 za zapewnienie dostępu do informacji, o których mowa w art. 2 ust. 2 lit. a), zapewniają one, aby takie informacje spełniały następujące wymogi:

a) muszą być przyjazne dla użytkownika, umożliwiając użytkownikom łatwe znalezienie i zrozumienie informacji oraz łatwą identyfikację elementów informacji mających znaczenie w ich konkretnej sytuacji;

b) muszą być dokładne i wystarczająco kompleksowe, aby obejmować informacje, które są potrzebne użytkownikom do korzystania z ich praw w sposób w pełni zgodny z mającymi zastosowanie przepisami i obowiązkami;

c) muszą zawierać w stosownych przypadkach odniesienia, linki do aktów prawnych, specyfikacje techniczne i wytyczne;

d) muszą zawierać nazwę właściwego organu lub podmiotu odpowiedzialnego za treść informacji;

e) muszą zawierać dane kontaktowe wszelkich odpowiednich usług wsparcia i rozwiązywania problemów, takie jak numer telefonu, adres poczty elektronicznej, formularz zapytania online lub wszelkie inne powszechnie używane środki komunikacji elektronicznej, które są najbardziej odpowiednie dla rodzaju oferowanych usług i dla docelowych odbiorców tych usług;

f) muszą zawierać datę ostatniej aktualizacji informacji, jeżeli jej dokonano, lub, jeżeli informacje nie zostały zaktualizowane, datę publikacji informacji;

g) muszą być dobrze zorganizowane oraz przedstawione, tak aby użytkownicy szybko mogli znaleźć informacje, których potrzebują;

h) muszą być aktualizowane; oraz

i) muszą być napisane jasnym i prostym językiem, dostosowanym do potrzeb docelowych użytkowników.

2. Państwa członkowskie udostępniają informacje, o których mowa w ust. 1 niniejszego artykułu, w języku urzędowym Unii, który jest powszechnie rozumiany przez możliwie największą liczbę użytkowników transgranicznych, zgodnie z art. 12.

Artykuł 10

Jakość informacji na temat procedur

1. Do celów przestrzegania art. 4 państwa członkowskie oraz Komisja zapewniają, aby, zanim użytkownicy będą musieli podać swoją tożsamość przed rozpoczęciem procedury, zostały im udostępnione w stosownych przypadkach wystarczająco kompleksowe, jasne i przyjazne dla użytkownika wyjaśnienia na temat następujących elementów procedur, o których mowa w art. 2 ust. 2 lit. b):

a) odpowiednich etapów procedury, przez które musi przejść użytkownik, w tym wszelkich wyjątków, na mocy art. 6 ust. 3, od obowiązku oferowania przez państwa członkowskie procedury w pełni online;

b) nazwy właściwego organu lub podmiotu odpowiedzialnego za procedurę, w tym jego danych kontaktowych;

c) akceptowanych sposobów uwierzytelniania, identyfikacji i podpisu dla danej procedury;

d) rodzaju i formatu dowodów, które należy przedłożyć;

e) środków dochodzenia roszczeń lub środków odwoławczych na ogół dostępnych w razie sporu z właściwymi organami;

f) mających zastosowanie opłat i metod płatności online;

g) wszelkich terminów, których powinien przestrzegać użytkownik lub właściwy organ, a w przypadku gdy nie ma takich terminów, średniego, szacowanego lub orientacyjnego czasu, jakiego potrzebuje właściwy organ do przeprowadzenia procedury;

h) wszelkich przepisów dotyczących braku odpowiedzi ze strony właściwego organu oraz jego konsekwencji prawnych dla użytkowników, w tym ustaleń dotyczących dorozumianego zatwierdzenia lub milczenia administracji;

i) każdego dodatkowego języka, w którym procedura może być prowadzona.

2. W przypadku braku ustaleń dotyczących dorozumianego zatwierdzenia, milczenia administracji lub podobnych ustaleń właściwe organy w stosownych przypadkach informują użytkowników o wszelkich opóźnieniach i o każdym przedłużeniu terminów lub o wszelkich ich konsekwencjach.

3. W przypadku gdy wyjaśnienia, o których mowa w ust. 1, są już dostępne dla użytkowników nietransgranicznych, mogą one zostać wykorzystane lub wykorzystane ponownie do celów niniejszego rozporządzenia, pod warunkiem że obejmują one również, w stosownych przypadkach, sytuację użytkowników transgranicznych.

4. Państwa członkowskie udostępniają wyjaśnienia, o których mowa w ust. 1 niniejszego artykułu, w języku urzędowym Unii, który jest powszechnie rozumiany przez możliwie największą liczbę użytkowników transgranicznych, zgodnie z art. 12.

Artykuł 11

Jakość informacji na temat usług wsparcia i rozwiązywania problemów

1. Do celów przestrzegania art. 4 państwa członkowskie i Komisja zapewniają, aby, zanim użytkownicy złożą wniosek o usługę, o której mowa w art. 2 ust. 2 lit. c), zostały im udostępnione jasne i przyjazne dla użytkownika wyjaśnienia na temat następujących kwestii:

a) rodzaju, celu i spodziewanych wyników oferowanej usługi;

b) danych kontaktowych podmiotów odpowiedzialnych za usługę, takich jak numer telefonu, adres poczty elektronicznej, formularz zapytania online lub wszelkie inne powszechnie używane środki komunikacji elektronicznej, które są najbardziej odpowiednie dla rodzaju oferowanych usług i dla docelowych odbiorców tych usług;

c) w stosownych przypadkach odpowiednich opłat i metod płatności online;

d) wszelkich mających zastosowanie terminów, których należy przestrzegać, a w przypadku gdy nie ma takich terminów, średniego lub przewidywanego czasu niezbędnego do dostarczenia usługi;

e) wszelkich dodatkowych języków, w których można złożyć wniosek i które mogą być używane w późniejszych kontaktach.

2. Państwa członkowskie udostępniają wyjaśnienia, o których mowa w ust. 1 niniejszego artykułu, w języku urzędowym Unii, który jest powszechnie rozumiany przez możliwie największą liczbę użytkowników transgranicznych, zgodnie z art. 12.

Artykuł 12

Tłumaczenie informacji

1. W przypadku gdy państwo członkowskie nie podaje informacji, wyjaśnień i instrukcji określonych w art. 9, 10 i 11 oraz art. 13 ust. 2 lit. a) w języku urzędowym Unii powszechnie rozumianym przez możliwie największą liczbę użytkowników transgranicznych, to państwo członkowskie występuje do Komisji z wnioskiem o zapewnienie tłumaczenia na ten język, w granicach dostępnego budżetu Unii, o których mowa w art. 32 ust. 1 lit. c).

2. Państwa członkowskie zapewniają, aby teksty przedłożone do tłumaczenia zgodnie z ust. 1 niniejszego artykułu obejmowały przynajmniej podstawowe informacje we wszystkich obszarach wymienionych w załączniku I oraz aby, o ile dostępny jest wystarczający budżet Unii, obejmowały wszelkie dalsze informacje, wyjaśnienia i instrukcje, o których mowa w art. 9, 10 i 11 oraz art. 13 ust. 2 lit. a), z uwzględnieniem najważniejszych potrzeb użytkowników transgranicznych. Państwa członkowskie przekazują do repozytorium linków, o którym mowa w art. 19, linki do takich przetłumaczonych informacji.

3. Język, o którym mowa w ust. 1, musi być językiem urzędowym Unii, którego użytkownicy w całej Unii najczęściej uczą się jako języka obcego. W drodze wyjątku, w przypadku gdy oczekuje się, że informacje, wyjaśnienia lub instrukcje, które mają zostać przetłumaczone, będą przedmiotem zainteresowania głównie użytkowników transgranicznych pochodzących z jednego innego państwa członkowskiego, język, o którym mowa w ust. 1, może być językiem urzędowym Unii używanym jako pierwszy język przez tych użytkowników transgranicznych.

4. W przypadku gdy państwo członkowskie występuje z wnioskiem o tłumaczenie na język urzędowy Unii niebędący językiem, którego użytkownicy w całej Unii najczęściej uczą się jako języka obcego, uzasadnia swój wniosek. W przypadku gdy Komisja stwierdzi, że warunki wyboru innego języka, o których mowa w ust. 3, nie są spełnione, może odrzucić ten wniosek i poinformować państwo członkowskie o powodach tego odrzucenia.

SEKCJA 2

Wymogi dotyczące procedur online

Artykuł 13

Transgraniczny dostęp do procedur online

1. Państwa członkowskie zapewniają, aby w przypadku gdy procedura, o której mowa w art. 2 ust. 2 lit. b), ustanowiona na poziomie krajowym, jest dostępna online dla użytkowników nietransgranicznych i może być przez nich przeprowadzona online, była ona również dostępna online dla użytkowników transgranicznych i mogła być przez nich przeprowadzona online w sposób niedyskryminujący za pomocą tego samego lub alternatywnego rozwiązania technicznego.

2. Państwa członkowskie zapewniają, aby w odniesieniu do procedur, o których mowa w ust. 1 niniejszego artykułu, spełnione były co najmniej następujące wymogi:

a) użytkownicy muszą mieć dostęp do instrukcji przeprowadzenia procedury w języku urzędowym Unii, który jest powszechnie rozumiany przez możliwie największą liczbę użytkowników transgranicznych, zgodnie z art. 12;

b) użytkownicy transgraniczni muszą mieć możliwość przedłożenia wymaganych informacji, w tym w przypadku gdy struktura takich informacji różni się od struktury podobnych informacji w danym państwie członkowskim;

c) użytkownicy transgraniczni muszą mieć możliwość podania swojej tożsamości i uwierzytelnienia jej, elektronicznego podpisania lub opieczętowania dokumentów, jak przewidziano w rozporządzeniu (UE) nr 910/2014, we wszystkich przypadkach, w których jest to możliwe również dla użytkowników nietransgranicznych;

d) użytkownicy transgraniczni muszą mieć możliwość przedłożenia dowodu zgodności z mającymi zastosowanie wymogami oraz otrzymania wyniku procedury w formacie elektronicznym we wszystkich przypadkach, w których jest to możliwe również dla użytkowników nietransgranicznych;

e) w przypadku gdy przeprowadzenie procedury wymaga płatności, użytkownicy muszą mieć możliwość uiszczenia wszelkich opłat online poprzez powszechnie dostępną transgraniczną usługę płatniczą, bez dyskryminacji ze względu na miejsce prowadzenia działalności przez dostawcę usług płatniczych, miejsce wydania instrumentu płatniczego lub lokalizację rachunku płatniczego w Unii.

3. W przypadku gdy procedura nie wymaga elektronicznej identyfikacji lub uwierzytelnienia, o których mowa w ust. 2 lit. c), oraz w przypadku gdy właściwym organom umożliwiono na podstawie mającego zastosowanie prawa krajowego lub mającej zastosowanie praktyki administracyjnej akceptowanie cyfrowych kopii nieelektronicznych dowodów tożsamości w przypadku użytkowników nietransgranicznych, takich jak dowody tożsamości lub paszporty, organy te akceptują również takie kopie cyfrowe w przypadku użytkowników transgranicznych.

Artykuł 14

System techniczny transgranicznej zautomatyzowanej wymiany dowodów oraz stosowanie zasady jednorazowości

1. Do celów wymiany dowodów w procedurach online wymienionych w załączniku II do niniejszego rozporządzenia oraz procedurach przewidzianych w dyrektywach 2005/36/WE, 2006/123/WE, 2014/24/UE i 2014/25/UE Komisja we współpracy z państwami członkowskimi tworzy system techniczny zautomatyzowanej wymiany dowodów między właściwymi organami w różnych państwach członkowskich (zwany dalej „systemem technicznym").

2. W przypadku gdy właściwe organy zgodnie z prawem wydają w swoim państwie członkowskim oraz w formacie elektronicznym pozwalającym na zautomatyzowaną wymianę dowody, które mają znaczenie dla procedur online, o których mowa w ust. 1, udostępniają one takie dowody występującym z wnioskiem właściwym organom z innych państw członkowskich w formacie elektronicznym pozwalającym na zautomatyzowaną wymianę.

3. System techniczny w szczególności:

a) musi umożliwiać przetwarzanie wniosków o dowody na wyraźny wniosek użytkownika;

b) musi umożliwiać przetwarzanie wniosków o dowody, które mają zostać udostępnione lub wymienione;

c) musi umożliwiać przekazywanie dowodów między właściwymi organami;

d) musi umożliwiać przetwarzanie dowodów przez właściwy organ występujący z wnioskiem;

e) musi zapewniać poufność i integralność dowodów;

f) musi umożliwiać użytkownikowi podgląd dowodów, które mają być wykorzystane przez właściwy organ występujący z wnioskiem, oraz dokonanie wyboru czy wymiana dowodów ma być przeprowadzona;

g) musi zapewniać odpowiedni poziom interoperacyjności z innymi odpowiednimi systemami;

h) musi zapewniać wysoki poziom bezpieczeństwa przy przekazywaniu i przetwarzaniu dowodów;

i) nie może przetwarzać dowodów w zakresie wykraczającym poza to, co jest niezbędne pod względem technicznym do wymiany dowodów, oraz nie dłużej niż przez czas niezbędny do tego celu.

4. Stosowanie systemu technicznego nie jest obowiązkowe dla użytkowników i jest dopuszczalne jedynie na ich wyraźny wniosek, chyba że prawo Unii lub prawo krajowe stanowią inaczej. Użytkownicy mogą przedkładać dowody za pomocą metod innych niż system techniczny, bezpośrednio właściwemu organowi występującemu z wnioskiem.

5. Nie wymaga się zapewnienia możliwości podglądu dowodów, o której mowa w ust. 3 lit. f) niniejszego artykułu, w przypadku procedur, w których mające zastosowanie prawo Unii lub prawo krajowe dopuszcza zautomatyzowaną transgraniczną wymianę danych bez takiego podglądu. Możliwość podglądu dowodów pozostaje bez uszczerbku dla obowiązku podawania informacji na podstawie art. 13 i 14 rozporządzenia (UE) 2016/679.

6. Państwa członkowskie włączają w pełni operacyjny system techniczny do procedur, o których mowa w ust. 1.

7. Właściwe organy odpowiedzialne za procedury online, o których mowa w ust. 1, na wyraźny, dobrowolny, konkretny, świadomy i jednoznaczny wniosek użytkownika, którego to dotyczy, występują z wnioskiem o dowody bezpośrednio do właściwych organów wydających dowody w innych państwach członkowskich za pośrednictwem systemu technicznego. Właściwe organy wydające, o których mowa w ust. 2, udostępniają, zgodnie z ust. 3 lit. e), takie dowody za pośrednictwem tego samego systemu.

8. Dowody udostępniane właściwemu organowi występującemu z wnioskiem ograniczają się do tego, czego dotyczył wniosek, i są używane przez ten organ wyłącznie do celów procedury, w odniesieniu do której wymieniono dowody. Dowody wymieniane za pośrednictwem systemu technicznego, dla celów właściwego organu występującego z wnioskiem, są uznawane za autentyczne.

9. Do dnia 12 czerwca 2021 r. Komisja przyjmie akty wykonawcze w celu określenia specyfikacji technicznych i operacyjnych systemu technicznego niezbędnych do wykonania niniejszego artykułu. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 37 ust. 2.

10. Ust. 1–8 nie stosuje się do procedur ustanowionych na poziomie Unii, które przewidują inne mechanizmy wymiany dowodów, chyba że system techniczny niezbędny do wykonania niniejszego artykułu jest włączony do tych procedur zgodnie z przepisami aktów Unii, w których ustanowiono te procedury.

11. Komisja oraz każde z państw członkowskich odpowiadają za opracowanie, dostępność, utrzymanie, nadzór, monitorowanie i zarządzanie bezpieczeństwem swoich odpowiednich części systemu technicznego.

Artykuł 15

Weryfikacja dowodów między państwami członkowskimi

W przypadku gdy nie jest dostępny system techniczny lub inne systemy wymiany lub weryfikacji dowodów między państwami członkowskimi, lub gdy takie systemy nie mają zastosowania, lub w przypadku gdy użytkownik nie występuje z wnioskiem o stosowanie systemu technicznego, właściwe organy współpracują ze sobą za pośrednictwem systemu wymiany informacji na rynku wewnętrznym (zwanego dalej „IMI"), jeżeli jest to konieczne w celu weryfikacji autentyczności dowodów przedłożonych przez użytkownika jednemu z tych organów w formie elektronicznej do celów procedury online.

SEKCJA 3

Wymogi jakości dotyczące usług wsparcia i rozwiązywania problemów

Artykuł 16

Wymogi jakości dotyczące usług wsparcia i rozwiązywania problemów

Właściwe organy oraz Komisja zapewniają, w ramach swoich odpowiednich kompetencji, aby usługi wsparcia i rozwiązywania problemów wymienione w załączniku III oraz usługi, które zostały uwzględnione w Portalu zgodnie z art. 7 ust. 2, 3 i 4, były zgodne z następującymi wymogami jakości:

a) usługi te muszą być świadczone w rozsądnym terminie, z uwzględnieniem złożoności wniosku;

b) w przypadku przedłużenia terminów użytkownicy muszą być informowani z wyprzedzeniem o powodach takiego przedłużenia i o nowym terminie;

c) w przypadku gdy świadczenie usługi wymaga płatności, użytkownicy muszą mieć możliwość uiszczenia wszelkich opłat online poprzez powszechnie dostępną transgraniczną usługę płatniczą, bez dyskryminacji ze względu na miejsce prowadzenia działalności przez dostawcę usług płatniczych, miejsce wydania instrumentu płatniczego lub lokalizację rachunku płatniczego w Unii.

SEKCJA 4

Monitorowanie jakości

Artykuł 17

Monitorowanie jakości

1. Koordynatorzy krajowi, o których mowa w art. 28, oraz Komisja, w ramach swoich odpowiednich kompetencji, regularnie monitorują zgodność informacji, procedur oraz usług wsparcia i rozwiązywania problemów dostępnych za pośrednictwem Portalu z wymogami jakości określonymi w art. 8–13 i art. 16. Monitorowanie prowadzi się na podstawie danych zgromadzonych zgodnie z art. 24 i 25.

2. W przypadku pogorszenia się jakości informacji, procedur oraz usług wsparcia i rozwiązywania problemów, o których mowa w ust. 1, zapewnianych przez właściwe organy, Komisja, uwzględniając wagę i utrzymywanie się pogorszenia jakości, podejmuje przynajmniej jeden z następujących środków:

a) informuje odpowiedniego koordynatora krajowego i zwraca się o działania zaradcze;

b) poddaje pod dyskusję w grupie koordynacyjnej Portalu zalecane działania w celu poprawy zgodności z wymogami jakości;

c) wysyła pismo z zaleceniami dla danego państwa członkowskiego;

d) czasowo wyłącza informacje, procedurę lub usługę wsparcia lub rozwiązywania problemów z Portalu.

3. W przypadku gdy usługa wsparcia lub rozwiązywania problemów, do której podano link zgodnie z art. 7 ust. 3, systematycznie nie spełnia wymogów określonych w art. 11 i 16 lub, w świetle z danych zgromadzonych zgodnie z art. 24 i 25, nie spełnia już potrzeb użytkowników, Komisja może wyłączyć usługę z Portalu po konsultacji z odpowiednim koordynatorem krajowym oraz, w razie konieczności, z grupą koordynacyjną Portalu.

ROZDZIAŁ IV

ROZWIĄZANIA TECHNICZNE

Artykuł 18

Wspólny interfejs użytkownika

1. Komisja, w ścisłej współpracy z państwami członkowskimi, zapewnia zintegrowany z portalem „Twoja Europa” wspólny interfejs użytkownika, aby zapewnić prawidłowe funkcjonowanie Portalu.

2. Wspólny interfejs użytkownika zapewnia dostęp do informacji, procedur oraz usług wsparcia i rozwiązywania problemów za pośrednictwem linków do odpowiednich witryn lub stron internetowych na poziomie Unii i na poziomie krajowym, zawartych w repozytorium linków, o którym mowa w art. 19.

3. Państwa członkowskie oraz Komisja, działając w zakresie swoich zadań i obowiązków, jak przewidziano w art. 4, zapewniają, aby informacje dotyczące przepisów i obowiązków, procedur oraz usług wsparcia i rozwiązywania problemów były zorganizowane i oznaczone w sposób ułatwiający ich wyszukiwanie poprzez wspólny interfejs użytkownika.

4. Komisja zapewnia, aby wspólny interfejs użytkownika był zgodny z następującymi wymogami jakości:

a) musi być łatwy w obsłudze;

b) musi być dostępny w internecie za pośrednictwem różnych urządzeń elektronicznych;

c) musi być opracowany i zoptymalizowany z myślą o różnych przeglądarkach internetowych;

d) musi spełniać następujące wymogi dotyczące dostępności sieci: postrzegalność, funkcjonalność, zrozumiałość i integralność.

5. Komisja może przyjmować akty wykonawcze ustanawiające wymogi w zakresie interoperacyjności, aby ułatwić wyszukiwanie za pośrednictwem wspólnego interfejsu użytkownika informacji dotyczących przepisów i obowiązków, procedur oraz usług wsparcia i rozwiązywania problemów. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 37 ust. 2.

Artykuł 19

Repozytorium linków

1. Komisja, w ścisłej współpracy z państwami członkowskimi, tworzy i utrzymuje elektroniczne repozytorium linków do informacji, procedur oraz usług wsparcia i rozwiązywania problemów, o których mowa w art. 2 ust. 2, umożliwiając powiązanie takich usług ze wspólnym interfejsem użytkownika.

2. Komisja przesyła do repozytorium linków linki do informacji, procedur, usług wsparcia i rozwiązywania problemów dostępnych na stronach internetowych zarządzanych na poziomie Unii oraz zapewnia ich dokładność i aktualność.

3. Koordynatorzy krajowi przesyłają do repozytorium linków linki do informacji, procedur, usług wsparcia i rozwiązywania problemów dostępnych na stronach internetowych zarządzanych przez właściwe organy lub podmioty prywatne, lub półprywatne, o których mowa w art. 7 ust. 3, oraz zapewniają ich dokładność i aktualność.

4. W przypadku gdy jest to technicznie wykonalne, przesyłanie linków, o którym mowa w ust. 3, może odbywać się automatycznie między odpowiednimi systemami państw członkowskich a repozytorium linków.

5. Komisja podaje informacje uwzględnione w repozytorium linków do wiadomości publicznej w otwartym i nadającym się do odczytu maszynowego formacie.

6. Komisja oraz koordynatorzy krajowi zapewniają, aby linki do informacji, procedur oraz usług wsparcia i rozwiązywania problemów oferowanych za pośrednictwem Portalu nie zawierały jakichkolwiek zbędnych całościowych lub częściowych powieleń i pokrywających się informacji, które mogą być mylące dla użytkowników.

7. W przypadku gdy udostępnianie informacji, o których mowa w art. 4, zostało przewidziane w innych przepisach prawa Unii, Komisja oraz koordynatorzy krajowi mogą przesyłać linki do tych informacji w celu spełnienia wymogów tego artykułu.

Artykuł 20

Wspólna wyszukiwarka usług wsparcia

1. W celu ułatwienia dostępu do usług wsparcia i rozwiązywania problemów, wymienionych w załączniku III lub o których mowa w art. 7 ust. 2 i 3, właściwe organy oraz Komisja zapewniają użytkownikom możliwość dostępu do nich poprzez wspólną wyszukiwarkę usług wsparcia i rozwiązywania problemów (zwaną dalej „wspólną wyszukiwarką usług wsparcia") dostępną w Portalu.

2. Komisja opracowuje wspólną wyszukiwarkę usług wsparcia, zarządza nią oraz decyduje o strukturze i formacie, w których należy przekazywać opisy i dane kontaktowe usług wsparcia i rozwiązywania problemów, aby umożliwić prawidłowe funkcjonowanie wspólnej wyszukiwarki usług wsparcia.

3. Koordynatorzy krajowi przekazują Komisji opisy i dane kontaktowe, o których mowa w ust. 2.

Artykuł 21

Odpowiedzialność za aplikacje ICT wspomagające Portal

1. Komisja odpowiada za opracowanie, dostępność, monitorowanie, aktualizację, utrzymanie, bezpieczeństwo i hosting następujących aplikacji ICT i stron internetowych:

a) portalu „Twoja Europa", o którym mowa w art. 2 ust. 1;

b) wspólnego interfejsu użytkownika, o którym mowa w art. 18 ust. 1, w tym wyszukiwarki lub innego narzędzia ICT, które umożliwia wyszukiwanie informacji i usług internetowych;

c) repozytorium linków, o którym mowa w art. 19 ust. 1;

d) wspólnej wyszukiwarki usług wsparcia, o której mowa w art. 20 ust. 1;

e) narzędzi do gromadzenia informacji zwrotnych od użytkowników, o których mowa w art. 25 ust. 1 i art. 26 ust. 1 lit. a).

Komisja, w ścisłej współpracy z państwami członkowskimi, opracowuje aplikacje ICT.

2. Państwa członkowskie odpowiadają za opracowanie, dostępność, monitorowanie, aktualizację, utrzymanie oraz bezpieczeństwo aplikacji ICT powiązanych ze swoimi krajowymi witrynami internetowymi i stronami internetowymi, które są połączone ze wspólnym interfejsem użytkownika.

ROZDZIAŁ V

PROMOCJA

Artykuł 22

Nazwa, logo i znak jakości

1. Portal powinien być znany i promowany publicznie pod nazwą „Your Europe".

Logo, pod którym Portal ma być znany i promowany publicznie, określi Komisja w ścisłej współpracy z grupą koordynacyjną Portalu do dnia 12 czerwca 2019 r.

Logo Portalu i link do Portalu muszą być widoczne i dostępne na odpowiednich, połączonych z Portalem stronach internetowych na poziomie Unii i na poziomie krajowym.

2. Na dowód przestrzegania wymogów jakości, o których mowa w art. 9, 10 i 11, nazwa i logo Portalu służą również jako znak jakości. Jednakże logo Portalu może być używane jako znak jakości wyłącznie przez strony i witryny internetowe włączone do repozytorium linków, o którym mowa w art. 19.

Artykuł 23

Promocja

1. Państwa członkowskie i Komisja propagują wiedzę na temat Portalu i korzystanie z niego wśród obywateli i przedsiębiorstw oraz zapewniają powszechną widoczność Portalu i zawartych w nim informacji, procedur oraz usług wsparcia i rozwiązywania problemów, a także łatwość ich wyszukiwania poprzez publicznie dostępne wyszukiwarki.

2. Państwa członkowskie i Komisja koordynują swoje działania promocyjne, o których mowa w ust. 1, i w ramach tych działań odnoszą się do Portalu oraz korzystają z jego logo, w stosownych przypadkach w połączeniu z wszelkimi innymi nazwami marek.

3. Państwa członkowskie oraz Komisja zapewniają, aby Portal był łatwy do wyszukania poprzez powiązane strony internetowe, za które odpowiadają, oraz aby wyraźne linki do wspólnego interfejsu użytkownika były dostępne na wszelkich odpowiednich stronach internetowych na poziomie Unii i na poziomie krajowym.

4. Koordynatorzy krajowi promują Portal wśród właściwych organów krajowych.

ROZDZIAŁ VI

GROMADZENIE DANYCH STATYSTYCZNYCH I INFORMACJI ZWROTNYCH OD UŻYTKOWNIKÓW

Artykuł 24

Dane statystyczne dotyczące użytkowników

1. Abu poprawić funkcjonalność Portalu, właściwe organy oraz Komisja zapewniają, w sposób gwarantujący anonimowość użytkowników, gromadzenie danych statystycznych wizyt użytkowników w Portalu i na stronach internetowych, do których linki zamieszczono w Portalu.

2. Właściwe organy, podmioty świadczące usługi wsparcia lub rozwiązywania problemów, o których mowa w art. 7 ust. 3, oraz Komisja gromadzą i wymieniają – w formie zagregowanej – informacje o liczbie, pochodzeniu i przedmiocie wniosków o świadczenie usług wsparcia i rozwiązywania problemów oraz swoim czasie reakcji.

3. Dane statystyczne zgromadzone zgodnie z ust. 1 i 2 dotyczące informacji, procedur oraz usług wsparcia i rozwiązywania problemów, do których prowadzą linki z Portalu, muszą zawierać następujące kategorie danych:

a) dane dotyczące liczby, pochodzenia i rodzaju użytkowników Portalu;

b) dane dotyczące preferencji i ścieżek użytkownika;

c) dane dotyczące przydatności, łatwości wyszukiwania oraz jakości informacji, procedur oraz usług wsparcia i rozwiązywania problemów.

Dane te podaje się do wiadomości publicznej w otwartym i powszechnie używanym formacie nadającym się do odczytu maszynowego.

4. Komisja przyjmuje akty wykonawcze określające metodę gromadzenia i wymiany danych statystycznych dotyczących użytkowników, o których to danych mowa w ust. 1, 2 i 3 niniejszego artykułu. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 37 ust. 2.

Artykuł 25

Informacje zwrotne użytkowników na temat usług Portalu

1. W celu gromadzenia bezpośrednio od użytkowników informacji na temat ich zadowolenia z usług świadczonych za pośrednictwem Portalu oraz informacji w nim udostępnionych Komisja zapewnia użytkownikom za pośrednictwem Portalu przyjazne dla użytkownika narzędzie do gromadzenia informacji zwrotnych, umożliwiające im, niezwłocznie po skorzystaniu z którejkolwiek z usług, o których mowa w art. 2 ust. 2, anonimowe przekazywanie uwag na temat jakości i dostępności usług zapewnianych za pośrednictwem Portalu, udostępnianych w nim informacji oraz wspólnego interfejsu użytkownika.

2. Właściwe organy oraz Komisja zapewniają, aby użytkownicy mieli dostęp do narzędzia, o którym mowa w ust. 1, na wszystkich stronach internetowych, które są częścią Portalu.

3. Komisja, właściwe organy oraz koordynatorzy krajowi mają bezpośredni dostęp do informacji zwrotnych od użytkowników zgromadzonych za pomocą narzędzia, o którym mowa w ust. 1, do celów rozwiązywania wszelkich zgłoszonych problemów.

4. Właściwe organy nie są zobowiązane do zapewnienia użytkownikom dostępu do narzędzia do gromadzenia informacji zwrotnych od użytkowników, o którym mowa w ust. 1, na swoich stronach internetowych będących częścią Portalu, jeżeli na stronach internetowych tych organów jest już dostępne, w celu monitorowania jakości usług, inne narzędzie do gromadzenia informacji zwrotnych od użytkowników o podobnych funkcjach, co narzędzie do gromadzenia informacji zwrotnych od użytkowników, o którym mowa w ust. 1. Właściwe organy gromadzą informacje zwrotne od użytkowników uzyskane z ich własnego narzędzia do gromadzenia informacji zwrotnych od użytkowników oraz wymieniają je z Komisją i koordynatorami krajowymi w innych państwach członkowskich.

5. Komisja przyjmuje akty wykonawcze określające zasady gromadzenia i wymiany informacji zwrotnych od użytkowników. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 37 ust. 2.

Artykuł 26

Sprawozdawczość dotycząca funkcjonowania rynku wewnętrznego

1. Komisja:

a) zapewnia użytkownikom Portalu łatwe w obsłudze narzędzie do anonimowego zgłaszania i przekazywania informacji zwrotnych na temat wszelkich przeszkód napotkanych przez nich w korzystaniu z ich praw na rynku wewnętrznym;

b) gromadzi zagregowane informacje z będących częścią Portalu usług wsparcia i rozwiązywania problemów dotyczące tematów pytań i odpowiedzi.

2. Komisja, właściwe organy oraz koordynatorzy krajowi muszą mieć bezpośredni dostęp do informacji zwrotnych zgromadzonych zgodnie z ust. 1 lit. a).

3. Państwa członkowskie i Komisja analizują i badają problemy zgłoszone przez użytkowników na podstawie niniejszego artykułu i w miarę możliwości rozwiązują je za pomocą odpowiednich środków.

Artykuł 27

Przegląd problemów online

Komisja publikuje online w formie zanonimizowanej przegląd problemów wynikających z informacji zgromadzonych zgodnie z art. 26 ust. 1, głównych danych statystycznych dotyczących użytkowników, o których mowa w art. 24, oraz głównych informacji zwrotnych od użytkowników, o których mowa w art. 25.

ROZDZIAŁ VII

ZARZĄDZANIE PORTALEM

Artykuł 28

Koordynatorzy krajowi

1. Każde państwo członkowskie wyznacza koordynatora krajowego. Oprócz obowiązków zgodnie z art. 7, 17, 19, 20, 23 i 25 koordynatorzy krajowi:

a) działają jako punkt kontaktowy w ramach swoich odpowiednich administracji we wszystkich kwestiach dotyczących Portalu;

b) propagują jednolite stosowanie art. 9–16 przez swoje odpowiednie właściwe organy;

c) zapewniają właściwe wdrożenie zaleceń, o których mowa w art. 17 ust. 2 lit. c).

2. Każde państwo członkowskie może wyznaczyć, stosownie do swojej wewnętrznej struktury administracyjnej, jednego koordynatora lub większą ich liczbę na potrzeby wykonywania zadań wymienionych w ust. 1. Jeden koordynator krajowy z każdego państwa członkowskiego odpowiada za kontakty z Komisją we wszystkich kwestiach związanych z Portalem.

3. Każde państwo członkowskie przekazuje pozostałym państwom członkowskim oraz Komisji imię i nazwisko oraz dane kontaktowe swojego koordynatora krajowego.

Artykuł 29

Grupa koordynacyjna

Powołuje się grupę koordynacyjną (zwaną dalej „grupą koordynacyjną Portalu"). W skład grupy koordynacyjnej Portalu wchodzi po jednym koordynatorze krajowym z każdego państwa członkowskiego, a przewodniczy jej przedstawiciel Komisji. Grupa koordynacyjna Portalu przyjmuje swój regulamin wewnętrzny. Komisja zapewnia sekretariat.

Artykuł 30

Zadania grupy koordynacyjnej Portalu

1. Grupa koordynacyjna Portalu wspiera wykonywanie niniejszego rozporządzenia. W szczególności:

a) ułatwia wymianę i regularną aktualizację najlepszych praktyk;

b) zachęca do wprowadzania procedur dostępnych w pełni online, wykraczających poza procedury wymienione w załączniku II do niniejszego rozporządzenia, a także internetowych narzędzi uwierzytelnienia i identyfikacji oraz podpisów elektronicznych, w szczególności tych, które przewidziano w rozporządzeniu (UE) nr 910/2014;

c) poddaje dyskusji udoskonalenia przyjaznej dla użytkownika prezentacji informacji w obszarach wymienionych w załączniku I, w szczególności na podstawie danych zgromadzonych zgodnie z art. 24 i 25;

d) wspiera Komisję w opracowywaniu wspólnych rozwiązań ICT wspomagających Portal;

e) poddaje dyskusji projekt rocznego programu prac;

f) wspiera Komisję w monitorowaniu wykonania rocznego programu prac;

g) poddaje dyskusji dodatkowe informacje przekazywane zgodnie z art. 5 w celu zachęcenia innych państw członkowskich do dostarczania podobnych informacji, jeżeli są one istotne dla użytkowników;

h) wspiera Komisję w monitorowaniu przestrzegania wymogów określonych w art. 8–16, zgodnie z art. 17;

i) informuje o wykonywaniu art. 6 ust. 1;

j) poddaje dyskusji oraz zaleca właściwym organom i Komisji działania mające na celu uniknięcie lub wyeliminowanie zbędnego powielania usług dostępnych za pośrednictwem Portalu;

k) wydaje opinie w sprawie procedur lub środków służących skutecznemu rozwiązywaniu problemów z jakością usług, zgłoszonych przez użytkowników, lub zgłasza propozycje dotyczące jej poprawy;

l) poddaje dyskusji stosowanie zasad bezpieczeństwa i ochrony prywatności już w fazie projektowania w kontekście niniejszego rozporządzenia;

m) poddaje dyskusji kwestie związane z gromadzeniem informacji zwrotnych od użytkowników i danych statystycznych, o których mowa w art. 24 i 25, tak aby usługi oferowane na poziomie Unii i na poziomie krajowym były stale ulepszane;

n) poddaje dyskusji kwestie związane z wymogami jakości usług zapewnianych za pośrednictwem Portalu;

o) wymienia się najlepszymi praktykami oraz wspiera Komisję w zakresie organizacji, struktury i prezentacji usług, o których mowa w art. 2 ust. 2, aby umożliwić właściwe funkcjonowanie wspólnego interfejsu użytkownika;

p) ułatwia opracowanie i wdrożenie skoordynowanej promocji;

q) współpracuje z organami zarządzającymi usługami informacyjnymi oraz usługami wsparcia i rozwiązywania problemów lub sieciami usług informacyjnych oraz usług wsparcia lub rozwiązywania problemów;

r) zapewnia wytyczne dotyczące dodatkowego języka urzędowego lub dodatkowych języków urzędowych Unii, które mają być stosowane przez właściwe organy zgodnie z art. 9 ust. 2, art. 10 ust. 4, art. 11 ust. 2 oraz art. 13 ust. 2 lit. a).

2. Komisja może konsultować się z grupą koordynacyjną Portalu we wszelkich kwestiach związanych ze stosowaniem niniejszego rozporządzenia.

Artykuł 31

Roczny program prac

1. Komisja przyjmuje roczny program prac, w którym określa się w szczególności:

a) działania na rzecz poprawy prezentacji poszczególnych informacji w obszarach wymienionych w załączniku I oraz działania na rzecz ułatwienia terminowego wdrożenia, przez właściwe organy wszystkich szczebli, w tym na szczeblu gminy, wymogu zapewniania informacji;

b) działania ułatwiające przestrzeganie art. 6 i 13;

c) działania niezbędne do zapewnienia spójnego przestrzegania wymogów określonych w art. 9–12;

d) działania związane z promocją Portalu zgodnie z art. 23.

2. Przygotowując projekt rocznego programu prac, Komisja uwzględnia dane statystyczne dotyczące użytkowników i informacje zwrotne od użytkowników, zgromadzone zgodnie z art. 24 i 25, oraz wszelkie sugestie zgłoszone przez państwa członkowskie. Komisja, przed przyjęciem rocznego programu prac przedkłada jego projekt pod dyskusję grupie koordynacyjnej Portalu.

ROZDZIAŁ VIII

PRZEPISY KOŃCOWE

Artykuł 32

Koszty

1. Z budżetu ogólnego Unii Europejskiej pokrywa się koszty:

a) opracowania i utrzymania narzędzi ICT wspomagających wykonywanie niniejszego rozporządzenia na poziomie Unii;

b) promocji Portalu na poziomie Unii;

c) tłumaczenia informacji, wyjaśnień i instrukcji zgodnie z art. 12 w ramach przypadającej na każde państwo członkowskie maksymalnej rocznej objętości, bez uszczerbku dla ewentualnych przesunięć, w przypadku gdy jest to konieczne, aby umożliwić pełne wykorzystanie dostępnego budżetu.

2. Koszty związane z krajowymi portalami internetowymi, platformami informacyjnymi, usługami wsparcia oraz procedurami ustanowionymi na poziomie państw członkowskich są pokrywane z budżetów poszczególnych państw członkowskich, o ile prawodawstwo Unii nie stanowi inaczej.

Artykuł 33

Ochrona danych osobowych

Przetwarzanie danych osobowych przez właściwe organy w ramach niniejszego rozporządzenia musi być zgodne z rozporządzeniem (UE) 2016/679. Przetwarzanie danych osobowych przez Komisję w ramach niniejszego rozporządzenia musi być zgodne z rozporządzeniem (UE) 2018/1725.

Artykuł 34

Współpraca z innymi sieciami zapewniającymi informacje i wsparcie

1. Po konsultacjach z państwami członkowskimi Komisja decyduje, które z istniejących nieformalnych struktur zarządzania w zakresie usług wsparcia i rozwiązywania problemów wymienionych w załączniku III lub w zakresie obszarów informacji objętych załącznikiem I mają zostać objęte zakresem obowiązków grupy koordynacyjnej Portalu.

2. W przypadku gdy usługi lub sieci zapewniające informacje i wsparcie zostały utworzone na mocy prawnie wiążącego aktu Unii w zakresie któregokolwiek z obszarów informacji objętych załącznikiem I, Komisja koordynuje prace grupy koordynacyjnej Portalu oraz organów zarządzających takimi usługami lub sieciami w celu osiągnięcia synergii i uniknięcia powielania działań.

Artykuł 35

System wymiany informacji na rynku wewnętrznym

1. Do celów art. 6 ust. 4 i art. 15 oraz zgodnie z tymi przepisami stosuje się system wymiany informacji na rynku wewnętrznym (zwany dalej „IMI") utworzony na mocy rozporządzenia (UE) nr 1024/2012.

2. Komisja może zadecydować o stosowaniu IMI jako elektronicznego repozytorium linków, o których mowa w art. 19 ust. 1.

Artykuł 36

Sprawozdania i przegląd

Do dnia 12 grudnia 2022 r., a następnie co dwa lata, Komisja dokonuje przeglądu stosowania niniejszego rozporządzenia oraz przedstawia Parlamentowi Europejskiemu i Radzie sprawozdanie z oceny dotyczące funkcjonowania Portalu oraz funkcjonowania rynku wewnętrznego na podstawie danych statystycznych i informacji zwrotnych, zgromadzonych zgodnie z art. 24, 25 i 26. W przeglądzie ocenia się w szczególności zakres art. 14, biorąc pod uwagę zmiany technologiczne, rynkowe i prawne w zakresie wymiany dowodów między właściwymi organami.

Artykuł 37

Procedura komitetowa

1. Komisję wspomaga komitet. Komitet ten jest komitetem w rozumieniu rozporządzenia (UE) nr 182/2011.

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

Artykuł 38

Zmiana rozporządzenia (UE) nr 1024/2012

W rozporządzeniu (UE) nr 1024/2012 wprowadza się następujące zmiany:

1) art. 1 otrzymuje brzmienie:

„*Artykuł 1*

Przedmiot

Niniejsze rozporządzenie ustanawia zasady wykorzystywania systemu wymiany informacji na rynku wewnętrznym (zwanego dalej »IMI«) na potrzeby współpracy administracyjnej między uczestnikami IMI, w tym przetwarzania danych osobowych.";

2) art. 3 ust. 1 otrzymuje brzmienie:

„1. IMI jest wykorzystywany na potrzeby wymiany informacji, w tym danych osobowych, między uczestnikami IMI oraz na potrzeby przetwarzania tych informacji w którymkolwiek z następujących celów:

a) współpraca administracyjna wymagana zgodnie z aktami wymienionymi w załączniku;

b) współpraca administracyjna objęta projektem pilotażowym realizowanym zgodnie z art. 4.";

3) w art. 5 akapit drugi wprowadza się następujące zmiany:

a) lit. a) otrzymuje brzmienie:

„a) »IMI« oznacza narzędzie elektroniczne udostępnione przez Komisję w celu usprawnienia współpracy administracyjnej między uczestnikami IMI;";

b) lit. b) otrzymuje brzmienie:

„b) »współpraca administracyjna« oznacza współpracę pomiędzy uczestnikami IMI w drodze wymiany i przetwarzania informacji w celu lepszego stosowania prawa Unii;";

c) lit. g) otrzymuje brzmienie:

„g) »uczestnicy IMI« oznaczają właściwe organy, koordynatorów IMI, Komisję oraz organy i jednostki organizacyjne Unii;";

4) w art. 8 ust. 1 dodaje się punkt w brzmieniu:

„f) zapewnia koordynację z organami i jednostkami organizacyjnymi Unii oraz przyznaje im prawa dostępu do IMI.";

5) art. 9 ust. 4 otrzymuje brzmienie:

„4. Państwa członkowskie, Komisja oraz organy i jednostki organizacyjne Unii wprowadzają stosowne środki, aby umożliwić użytkownikom IMI dostęp do danych osobowych przetwarzanych w IMI, wyłącznie w zakresie niezbędnym do wykonywania ich obowiązków oraz wyłącznie w obszarze lub obszarach rynku wewnętrznego, w których użytkownikom tym przyznano prawa dostępu zgodnie z ust. 3.";

6) w art. 21 wprowadza się następujące zmiany:

a) ust. 2 otrzymuje brzmienie:

„2. Europejski Inspektor Ochrony Danych odpowiada za monitorowanie i zapewnianie stosowania niniejszego rozporządzenia w przypadkach gdy Komisja lub organy i jednostki organizacyjne Unii, działające w charakterze uczestników IMI, przetwarzają dane osobowe. Zastosowanie mają odpowiednio obowiązki i uprawnienia określone w art. 57 i 58 rozporządzenia (UE) nr 2018/1725 (*).

(*) 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 (Dz. U. L 295 z 21.11.2018, s. 39).";

b) ust. 3 otrzymuje brzmienie:

„3. Krajowe organy nadzorcze oraz Europejski Inspektor Ochrony Danych, działając w ramach swoich odpowiednich kompetencji, współpracują ze sobą w celu zapewnienia skoordynowanego nadzoru nad IMI oraz nad korzystaniem z niego przez uczestników IMI zgodnie z art. 62 rozporządzenia (UE) 2018/1725.";

c) uchyla się ust. 4;

7) uchyla się art. 29 ust. 1;

8) w załączniku dodaje się punkty w brzmieniu:

„11. 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) (*): art. 56, art. 60–66 i art. 70 ust. 1.

12. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 2 października 2018 r. w sprawie utworzenia jednolitego portalu cyfrowego w celu zapewnienia dostępu do informacji, procedur oraz usług wsparcia i rozwiązywania problemów, a także zmieniające rozporządzenie (UE) nr 1024/2012 (**): art. 6 ust. 4, art. 15 i 19.

(*) Dz.U. L 119 z 4.5.2016, s. 1.
(**) Dz.U. L 295 z 21.11.2018, s. 39."

Artykuł 39

Wejście w życie

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

Art. 2, art. 4, art. 7–12, art. 16, art. 17, art. 18 ust. 1–4, art. 19, art. 20, art. 24 ust. 1, 2 i 3, art. 25 ust. 1–4, art. 26 i art. 27 stosuje się od dnia 12 grudnia 2020 r.

Art. 6, art. 13, art. 14 ust. 1–8 i ust. 10 oraz art. 15 stosuje się od dnia 12 grudnia 2023 r.

Niezależnie od daty rozpoczęcia stosowania art. 2, 9, 10 i 11 organy gminne udostępnią informacje, wyjaśnienia i instrukcje, o których mowa w tych artykułach, najpóźniej do dnia 12 grudnia 2022 r.

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

Sporządzono w Strasburgu dnia 2 października 2018 r.

W imieniu Parlamentu Europejskiego	*W imieniu Rady*
A. TAJANI	J. BOGNER-STRAUSS
Przewodniczący	*Przewodniczący*

ZAŁĄCZNIK I

Wykaz obszarów informacji, o których mowa w art. 2 ust. 2 lit. a), które mają znaczenie dla obywateli i przedsiębiorstw korzystających ze swoich praw na rynku wewnętrznym

Obszary informacji dotyczących obywateli:

Obszar	INFORMACJE DOTYCZĄCE PRAW, OBOWIĄZKÓW I PRZEPISÓW WYNIKAJĄCYCH Z PRAWA UNII I PRAWA KRAJOWEGO
A. Podróże w Unii	1. dokumenty wymagane od obywateli Unii, członków ich rodzin, którzy nie są obywatelami Unii, małoletnich podróżujących samotnie oraz osób niebędących obywatelami Unii przekraczających granice w Unii (dowód tożsamości, wiza, paszport) 2. prawa i obowiązki osób podróżujących samolotem, pociągiem, statkiem lub autobusem w Unii i z Unii oraz osób wykupujących imprezy turystyczne lub powiązane usługi turystyczne 3. pomoc w związku z ograniczoną możliwością poruszania się przy podróżowaniu w Unii i z Unii 4. przewóz zwierząt, roślin, alkoholu, tytoniu, papierosów i innych towarów przy podróżowaniu w Unii 5. połączenia głosowe oraz wysyłanie i otrzymywanie wiadomości i danych drogą elektroniczną w Unii
B. Praca i przejście na emeryturę w Unii	1. poszukiwanie zatrudnienia w innym państwie członkowskim 2. podjęcie zatrudnienia w innym państwie członkowskim 3. uznawanie kwalifikacji z myślą o zatrudnieniu w innym państwie członkowskim 4. opodatkowanie w innym państwie członkowskim 5. przepisy dotyczące odpowiedzialności i obowiązkowego ubezpieczenia w związku z pobytem lub zatrudnieniem w innym państwie członkowskim 6. warunki zatrudnienia, w tym pracowników delegowanych, ustanowione na mocy ustawy lub aktów wykonawczych (w tym informacje o godzinach pracy, urlopie płatnym, uprawnieniach urlopowych, prawach i obowiązkach dotyczących pracy w godzinach nadliczbowych, kontrolach stanu zdrowia, rozwiązywaniu umów, zwolnieniach i redukcjach etatów) 7. równe traktowanie (przepisy zabraniające dyskryminacji w miejscu zatrudnienia, przepisy dotyczące równości wynagrodzeń dla mężczyzn i kobiet oraz równości wynagrodzeń dla pracowników zatrudnionych na czas określony albo nieokreślony) 8. obowiązki w zakresie zdrowia i bezpieczeństwa w zależności od różnych rodzajów działalności 9. prawa i obowiązki w dziedzinie zabezpieczenia społecznego w Unii, w tym prawa i obowiązki dotyczące uprawnień emerytalnych i rentowych
C. Pojazdy w Unii	1. czasowe lub stałe sprowadzenie pojazdu silnikowego do innego państwa członkowskiego 2. uzyskanie i przedłużenie ważności prawa jazdy 3. zawarcie obowiązkowego ubezpieczenia pojazdu silnikowego 4. kupno i sprzedaż pojazdu silnikowego w innym państwie członkowskim 5. krajowe przepisy ruchu drogowego i wymagania dotyczące kierowców, w tym ogólne zasady korzystania z krajowej infrastruktury drogowej: opłaty czasowe (winiety), opłaty uzależnione od przebytej odległości (opłaty za przejazd), nalepki ekologiczne

Obszar	INFORMACJE DOTYCZĄCE PRAW, OBOWIĄZKÓW I PRZEPISÓW WYNIKAJĄCYCH Z PRAWA UNII I PRAWA KRAJOWEGO
D. Pobyt w innym państwie członkowskim	1. czasowe lub stałe przeniesienie się do innego państwa członkowskiego 2. zakup i sprzedaż nieruchomości, w tym wszelkie warunki i obowiązki dotyczące opodatkowania, własności lub użytkowania takiej nieruchomości, w tym jako drugiego miejsca pobytu 3. udział w wyborach lokalnych i wyborach do Parlamentu Europejskiego 4. wymagania dotyczące kart pobytowych dla obywateli Unii i członków ich rodzin, w tym członków rodzin, którzy nie są obywatelami Unii 5. warunki mające zastosowanie do naturalizacji obywateli innego państwa członkowskiego 6. przepisy mające zastosowanie w przypadku śmierci, w tym przepisy dotyczące repatriacji zwłok do innego państwa członkowskiego
E. Kształcenie lub praktyka zawodowa w innym państwie członkowskim	1. system kształcenia w innym państwie członkowskim, w tym system wczesnej edukacji i opieki nad dziećmi, kształcenia podstawowego i średniego, szkolnictwa wyższego i uczenia się dorosłych 2. wolontariat w innym państwie członkowskim 3. praktyki zawodowe w innym państwie członkowskim 4. prowadzenie badań naukowych w innym państwie członkowskim jako część programu kształcenia
F. Opieka zdrowotna	1. korzystanie z opieki zdrowotnej w innym państwie członkowskim 2. zakup przepisanych produktów farmaceutycznych w innym państwie członkowskim niż państwo, w którym wystawiono receptę, przez internet lub osobiście 3. przepisy dotyczące ubezpieczenia zdrowotnego mające zastosowanie w przypadku krótkoterminowego lub długoterminowego pobytu w innym państwie członkowskim, w tym dotyczące tego, jak ubiegać się o europejską kartę ubezpieczenia zdrowotnego 4. ogólne informacje dotyczące praw dostępu do dostępnych działań publicznych z zakresu profilaktyki zdrowotnej i obowiązku uczestnictwa w takich działaniach; 5. usługi świadczone za pośrednictwem krajowych numerów alarmowych, w tym numerów „112” i „116” 6. prawa i warunki przeniesienia do domu opieki
G. Prawa obywatelskie i rodzinne	1. urodzenie dziecka, piecza nad małoletnimi dziećmi, władza rodzicielska, przepisy dotyczące macierzyństwa zastępczego i przysposobienia, w tym przysposobienia niepełnego, obowiązki alimentacyjne wobec dzieci, których sytuacja rodzinna obejmuje element transgraniczny 2. związek osób posiadających różne obywatelstwa, w tym osób tej samej płci (małżeństwo, związek partnerski lub zarejestrowany związek partnerski, separacja, rozwód, małżeńskie prawa majątkowe, prawa konkubentów) 3. zasady uznania płci 4. prawa spadkowe oraz obowiązki związane z dziedziczeniem w innym państwie członkowskim, łącznie z przepisami podatkowymi 5. prawa i przepisy mające zastosowanie w przypadku transgranicznego uprowadzenia dziecka przez jednego z rodziców

Obszar	INFORMACJE DOTYCZĄCE PRAW, OBOWIĄZKÓW I PRZEPISÓW WYNIKAJĄCYCH Z PRAWA UNII I PRAWA KRAJOWEGO
H. Prawa konsumenta	1. zakup towarów, treści cyfrowych lub usług (w tym usług finansowych) w innym państwie członkowskim, przez internet lub osobiście 2. posiadanie rachunku bankowego w innym państwie członkowskim 3. przyłączenie do sieci infrastruktury technicznej, na przykład gazowej, elektroenergetycznej, wodnej, kanalizacyjnej, telekomunikacyjnej i internetowej 4. płatności, w tym polecenia przelewu, opóźnienia w płatnościach transgranicznych 5. prawa i gwarancje konsumenckie związane z kupnem towarów i usług, w tym procedury rozwiązywania sporów konsumenckich i procedury odszkodowawcze 6. bezpieczeństwo produktów konsumpcyjnych 7. wynajem pojazdu silnikowego
I. Ochrona danych osobowych	1. korzystanie przez osobę, której dane dotyczą z jej praw związanych z ochroną danych osobowych

Obszary informacji dotyczących przedsiębiorstw:

Obszar	INFORMACJE DOTYCZĄCE PRAW, OBOWIĄZKÓW I PRZEPISÓW
J. Rozpoczęcie, prowadzenie i zakończenie działalności gospodarczej	1. rejestracja, zmiana formy prawnej lub zakończenie działalności gospodarczej (procedury rejestracji i formy prawne prowadzenia działalności gospodarczej) 2. przeniesienie działalności gospodarczej do innego państwa członkowskiego 3. prawa własności intelektualnej (zgłoszenia patentowe, rejestracja znaku towarowego, rysunku lub wzoru, uzyskanie licencji na zwielokrotnianie) 4. uczciwość i przejrzystość praktyk handlowych, w tym prawa i gwarancje konsumenckie związane ze sprzedażą towarów i usług 5. udostępnianie narzędzi online do dokonywania płatności transgranicznych przy sprzedaży online towarów i usług 6. prawa i obowiązki wynikające z prawa zobowiązań, w tym odsetki za opóźnienia w płatnościach 7. postępowanie upadłościowe i likwidacja spółek 8. ubezpieczenie kredytu 9. łączenie spółek lub sprzedaż przedsiębiorstwa 10. odpowiedzialność cywilna osób zarządzających spółkami i członków zarządu spółek 11. zasady i obowiązki dotyczące przetwarzania danych osobowych

Obszar	INFORMACJE DOTYCZĄCE PRAW, OBOWIĄZKÓW I PRZEPISÓW
K. Pracownicy	1. warunki zatrudnienia ustanowione na mocy ustawy lub aktów wykonawczych (w tym godziny pracy, urlop płatny, uprawnienia urlopowe, prawa i obowiązki dotyczące pracy w godzinach nadliczbowych, kontrole stanu zdrowia, rozwiązywanie umów, zwolnienia i redukcje etatów) 2. prawa i obowiązki w dziedzinie zabezpieczenia społecznego w Unii (rejestracja pracodawcy, rejestracja pracowników, zgłoszenie rozwiązania umowy z pracownikiem, płatność składek na ubezpieczenie społeczne, prawa i obowiązki dotyczące uprawnień emerytalnych i rentowych) 3. zatrudnianie pracowników w innych państwach członkowskich (delegowanie pracowników, przepisy dotyczące swobody świadczenia usług, warunki przyznania prawa pobytu pracownikom) 4. równe traktowanie (przepisy zabraniające dyskryminacji w miejscu zatrudnienia, przepisy dotyczące równości wynagrodzeń dla mężczyzn i kobiet oraz równości wynagrodzeń dla pracowników zatrudnionych na czas określony albo nieokreślony) 5. przepisy dotyczące reprezentacji pracowniczej
L. Podatki	1. VAT: informacje o ogólnych zasadach, stawkach i zwolnieniach, rejestracja do celów VAT i płatność VAT, uzyskiwanie zwrotu 2. podatek akcyzowy: informacje o ogólnych zasadach, stawkach i zwolnieniach, rejestracja do celów podatku akcyzowego i płatność podatku akcyzowego, uzyskiwanie zwrotu 3. należności celne i inne podatki oraz opłaty pobierane od przywozu towarów 4. procedury celne dotyczące przywozu i wywozu zgodnie z unijnym kodeksem celnym 5. inne podatki: płatność, stawki, deklaracje podatkowe
M. Towary	1. uzyskanie oznakowania CE 2. przepisy i wymogi dotyczące produktów 3. ustalenie mających zastosowanie norm, specyfikacji technicznych oraz przeprowadzenie certyfikacji produktów 4. wzajemne uznawanie produktów niepodlegających specyfikacjom unijnym 5. wymagania dotyczące klasyfikacji, oznakowania i pakowania niebezpiecznych substancji chemicznych 6. sprzedaż na odległość i poza lokalem przedsiębiorstwa: informacje, których należy udzielać kupującym przed zawarciem umowy, potwierdzenie umowy na piśmie, odstąpienie od umowy, dostawa towarów, inne szczegółowe obowiązki 7. produkty wadliwe: prawa i gwarancje konsumenckie, odpowiedzialność posprzedażna, środki dochodzenia roszczeń przez poszkodowaną stronę 8. certyfikacja, etykiety (EMAS, etykiety energetyczne, ekoprojekt, oznakowanie ekologiczne UE) 9. recykling i gospodarowanie odpadami
N. Usługi	1. uzyskiwanie koncesji, zezwoleń lub pozwoleń z myślą o rozpoczęciu i prowadzeniu działalności gospodarczej 2. powiadamianie władz o działalności transgranicznej 3. uznawanie kwalifikacji zawodowych, w tym kształcenia i szkolenia zawodowego

Obszar	INFORMACJE DOTYCZĄCE PRAW, OBOWIĄZKÓW I PRZEPISÓW
O. Finansowanie działalności gospodarczej	1. uzyskiwanie dostępu do finansowania na poziomie Unii, w tym unijne programy finansowania i dotacje na działalność gospodarczą 2. uzyskiwanie dostępu do finansowania na poziomie krajowym 3. inicjatywy skierowane do przedsiębiorców (wymiany organizowane dla nowych przedsiębiorców, programy opieki mentorskiej itd.)
P. Zamówienia publiczne	1. udział w postępowaniach o udzielenie zamówienia publicznego: przepisy i procedury 2. składanie oferty online w odpowiedzi na publicznego zaproszenia do składania ofert 3. zgłaszanie nieprawidłowości w związku z procedurą o udzielenie zamówienia publicznego
Q. Bezpieczeństwo i higiena pracy	1. obowiązki w zakresie zdrowia i bezpieczeństwa w zależności od różnych rodzajów działalności, w tym zapobieganie zagrożeniom, informowanie i szkolenia

ZAŁĄCZNIK II

Procedury, o których mowa w art. 6 ust. 1

Zdarzenia życiowe	Procedury	Oczekiwany wynik z zastrzeżeniem, w stosownych przypadkach, oceny wniosku przez właściwy organ zgodnie z prawem krajowym
Narodziny dziecka	Wniosek o wydanie dowodu rejestracji urodzenia	Dowód rejestracji urodzenia lub akt urodzenia
Pobyt	Wniosek o wydanie dowodu miejsca pobytu	Potwierdzenie rejestracji pod aktualnym adresem
Nauka	Ubieganie się o finansowanie studiów w szkolnictwie wyższym, takie jak stypendia naukowe i kredyty studenckie z organu publicznego lub instytucji publicznej	Decyzja dotycząca wniosku o finansowanie lub potwierdzenie przyjęcia
	Przedłożenie wstępnego podania o przyjęcie do publicznej instytucji szkolnictwa wyższego	Potwierdzenie przyjęcia podania
	Wniosek o akademickie uznanie dyplomów, świadectw lub innych dokumentów potwierdzających ukończenie studiów lub kursów	Decyzja w sprawie wniosku o uznanie
Praca	Wniosek o określanie mającego zastosowanie ustawodawstwa zgodnie z tytułem II rozporządzenia (WE) nr 883/2004 ([1])	Decyzja w sprawie mającego zastosowanie ustawodawstwa
	Powiadomienie o zmianach w sytuacji osobistej lub zawodowej osoby otrzymującej świadczenia z zabezpieczenia społecznego, mających znaczenie w przypadku takich świadczeń	Potwierdzenie otrzymania powiadomienia o takich zmianach
	Wniosek o europejską kartę ubezpieczenia zdrowotnego (EKUZ)	Europejska karta ubezpieczenia zdrowotnego (EKUZ)
	Złożenie deklaracji podatkowej dotyczącej podatku dochodowego	Potwierdzenie przyjęcia deklaracji podatkowej
Przeprowadzka	Rejestracja zmiany adresu	Potwierdzenie wyrejestrowania z poprzedniego adresu oraz rejestracji pod nowym adresem
	Rejestracja pojazdu silnikowego, w procedurach standardowych, pochodzącego z państwa członkowskiego lub już zarejestrowanego w państwie członkowskim ([2])	Potwierdzenie rejestracji pojazdu silnikowego
	Otrzymanie nalepek zezwalających na użytkowanie krajowej infrastruktury drogowej: opłaty czasowe (winiety), opłaty uzależnione od przebytej odległości (opłaty za przejazd), wydawane przez organ publiczny lub instytucję publiczną	Otrzymanie nalepki potwierdzającej uiszczenie opłaty za przejazd lub winiety, lub innego dowodu płatności
	Otrzymanie nalepki ekologicznej wydanej przez organ publiczny lub instytucję publiczną	Otrzymanie nalepki ekologicznej lub innego dowodu płatności

Zdarzenia życiowe	Procedury	Oczekiwany wynik z zastrzeżeniem, w stosownych przypadkach, oceny wniosku przez właściwy organ zgodnie z prawem krajowym
Przejście na emeryturę	Ubieganie się o świadczenia emerytalno-rentowe i przedemerytalne z systemów obowiązkowych	Potwierdzenie przyjęcia wniosku lub decyzja dotycząca wniosku o przyznanie emerytury lub renty lub świadczeń przedemerytalnych
	Zwrócenie się o udzielenie informacji na temat danych dotyczących świadczeń emerytalno-rentowych z systemów obowiązkowych	Oświadczenie dotyczące danych osobowych dotyczących emerytury lub renty
Rozpoczęcie, prowadzenie i zakończenie działalności gospodarczej	Powiadomienie o działalności gospodarczej, zezwolenie na prowadzenie działalności gospodarczej, zmiana działalności gospodarczej i zakończenie takiej działalności nieobejmujące procedur dotyczących niewypłacalności lub likwidacji, z wyłączeniem procedur dotyczących początkowej rejestracji działalności gospodarczej w rejestrze przedsiębiorców oraz z wyłączeniem procedur dotyczących zakładania spółek oraz późniejszego zgłaszania składania dokumentów przez spółki, w rozumieniu art. 54 akapit drugi TFUE	Potwierdzenie otrzymania zgłoszenia lub zmiany działalności gospodarczej, lub wniosku o zezwolenie na prowadzenie działalności gospodarczej
	Rejestracja pracodawcy (osoby fizycznej) w obowiązkowych systemach emerytalno-rentowych i ubezpieczeniowych	Potwierdzenie rejestracji lub numer rejestracyjny ubezpieczenia społecznego
	Rejestracja pracowników w obowiązkowych systemach emerytalno-rentowych i ubezpieczeniowych	Potwierdzenie rejestracji lub numer rejestracyjny ubezpieczenia społecznego
	Złożenie deklaracji podatkowej dotyczącej podatku od osób prawnych	Potwierdzenie przyjęcia deklaracji podatkowej
	Zgłoszenie w systemach zabezpieczenia społecznego rozwiązania umowy z pracownikiem, z wyłączeniem procedur grupowego rozwiązywania umów z pracownikami	Potwierdzenie otrzymania zgłoszenia
	Płatność składek na ubezpieczenia społeczne pracowników	Pokwitowanie lub inna forma potwierdzenia płatności składek na ubezpieczenia społeczne pracowników

([1]) Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 883/2004 z dnia 29 kwietnia 2004 r. w sprawie koordynacji systemów zabezpieczenia społecznego (Dz.U. L 166 z 30.4.2004, s. 1).

([2]) Procedury obejmujące następujące pojazdy: a) którykolwiek z pojazdów silnikowych lub przyczep, o których mowa w art. 3 dyrektywy Parlamentu Europejskiego i Rady 2007/46/WE (Dz. L 263 z 9.10.2007, s. 1); oraz b) którykolwiek z dwu- lub trzykołowych pojazdów mechanicznych, z kołami podwójnymi lub innymi, przeznaczonych do poruszania się po drogach, o których mowa w art. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 168/2013 (Dz.U. L 60 z 2.3.2013, s. 52).

ZAŁĄCZNIK III

Wykaz usług wsparcia i rozwiązywania problemów, o których mowa w art. 2 ust. 2 lit. c)

1) Pojedyncze punkty kontaktowe ([1])
2) Punkty kontaktowe ds. produktów ([2])
3) Punkty kontaktowe ds. wyrobów budowlanych ([3])
4) Krajowe ośrodki wsparcia ds. kwalifikacji zawodowych ([4])
5) Krajowe punkty kontaktowe do spraw transgranicznej opieki zdrowotnej ([5])
6) Europejska sieć służb zatrudnienia (EURES) ([6])
7) Internetowy system rozstrzygania sporów (ODR) ([7])

([1]) Dyrektywa 2006/123/WE Parlamentu Europejskiego i Rady z dnia 12 grudnia 2006 r. dotycząca usług na rynku wewnętrznym (Dz.U. L 376 z 27.12.2006, s. 36).

([2]) Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 764/2008 z dnia 9 lipca 2008 r. ustanawiające procedury dotyczące stosowania niektórych krajowych przepisów technicznych do produktów wprowadzonych legalnie do obrotu w innym państwie członkowskim oraz uchylające decyzję nr 3052/95/WE (Dz.U. L 218 z 13.8.2008, s. 21).

([3]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 305/2011 z dnia 9 marca 2011 r. ustanawiające zharmonizowane warunki wprowadzania do obrotu wyrobów budowlanych i uchylające dyrektywę Rady 89/106/EWG (Dz.U. L 88 z 4.4.2011, s. 5).

([4]) Dyrektywa 2005/36/WE Parlamentu Europejskiego i Rady z dnia 7 września 2005 r. w sprawie uznawania kwalifikacji zawodowych (Dz.U. L 255 z 30.9.2005, s. 22).

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

([6]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/589 z dnia 13 kwietnia 2016 r. w sprawie europejskiej sieci służb zatrudnienia (EURES), dostępu pracowników do usług w zakresie mobilności i dalszej integracji rynków pracy oraz zmiany rozporządzeń (UE) nr 492/2011 i (UE) nr 1296/2013 (Dz.U. L 107 z 22.4.2016, s. 1).

([7]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 524/2013 z dnia 21 maja 2013 r. w sprawie internetowego systemu rozstrzygania sporów konsumenckich oraz zmiany rozporządzenia (WE) nr 2006/2004 i dyrektywy 2009/22/WE (rozporządzenie w sprawie ODR w sporach konsumenckich) (Dz.U. L 165 z 18.6.2013, s. 1).

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

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2018/1726

z dnia 14 listopada 2018 r.

w sprawie Agencji Unii Europejskiej ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości (eu-LISA), zmiany rozporządzenia (WE) nr 1987/2006 i decyzji Rady 2007/533/WSiSW oraz uchylenia rozporządzenia (UE) nr 1077/2011

PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 74, art. 77 ust. 2 lit. a) i b), art. 78 ust. 2 lit. e), art. 79 ust. 2 lit. c), art. 82 ust. 1 lit. d), art. 85 ust. 1, art. 87 ust. 2 lit. a) oraz art. 88 ust. 2,

uwzględniając wniosek Komisji Europejskiej,

po przekazaniu projektu aktu ustawodawczego parlamentom narodowym,

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą ([1]),

a także mając na uwadze, co następuje:

(1) System Informacyjny Schengen (SIS II) został ustanowiony rozporządzeniem (WE) nr 1987/2006 Parlamentu Europejskiego i Rady ([2]) oraz decyzją Rady 2007/533/WSiSW ([3]). Rozporządzenie (WE) nr 1987/2006 i decyzja 2007/533/WSiSW przewidują, że za zarządzanie operacyjne systemem centralnym SIS II (zwanym dalej „centralnym SIS II") w okresie przejściowym ma odpowiadać Komisja. Po zakończeniu okresu przejściowego za zarządzanie operacyjne centralnym SIS II oraz niektórymi elementami infrastruktury łączności ma odpowiadać organ zarządzający.

(2) Wizowy system informacyjny (VIS) został ustanowiony decyzją Rady 2004/512/WE ([4]). Rozporządzenie (WE) nr 767/2008 Parlamentu Europejskiego i Rady ([5]) stanowi, że za zarządzanie operacyjne VIS w okresie przejściowym ma odpowiadać Komisja. Po zakończeniu okresu przejściowego za zarządzanie operacyjne systemem centralnym VIS i interfejsami krajowymi oraz niektórymi elementami infrastruktury łączności ma odpowiadać organ zarządzający.

([1]) Stanowisko Parlamentu Europejskiego z dnia 5 lipca 2018 r. (dotychczas nieopublikowane w Dzienniku Urzędowym) i decyzja Rady z dnia 9 listopada 2018 r.

([2]) Rozporządzenie (WE) nr 1987/2006 Parlamentu Europejskiego i Rady z dnia 20 grudnia 2006 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II) (Dz.U. L 381 z 28.12.2006, s. 4).

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

([4]) Decyzja Rady 2004/512/WE z dnia 8 czerwca 2004 r. w sprawie ustanowienia Wizowego Systemu Informacyjnego (VIS) (Dz.U. L 213 z 15.6.2004, s. 5).

([5]) Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 767/2008 z dnia 9 lipca 2008 r. w sprawie wizowego systemu informacyjnego (VIS) oraz wymiany danych pomiędzy państwami członkowskimi na temat wiz krótkoterminowych (rozporządzenie w sprawie VIS) (Dz.U. L 218 z 13.8.2008, s. 60).

(3) Eurodac ustanowiono w rozporządzeniu Rady (WE) nr 2725/2000 ([1]). Rozporządzenie Rady (WE) nr 407/2002 ([2]) ustanowiło stosowne przepisy wykonawcze. Te akty prawne zostały uchylone i zastąpione rozporządzeniem (UE) nr 603/2013 Parlamentu Europejskiego i Rady ([3]) ze skutkiem od 20 lipca 2015 r.

(4) Europejska Agencja ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości, powszechnie zwana eu-LISA, została ustanowiona rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 1077/2011 ([4]) w celu zapewnienia zarządzania operacyjnego systemem SIS, VIS i Eurodac oraz niektórymi elementami ich infrastruktur łączności oraz ewentualnie także innymi wielkoskalowymi systemami informatycznymi w przestrzeni wolności, bezpieczeństwa i sprawiedliwości, z zastrzeżeniem przyjęcia odrębnych unijnych aktów prawnych. Rozporządzenie (UE) nr 1077/2011 zostało zmienione rozporządzeniem (UE) nr 603/2013 w celu odzwierciedlenia zmian wprowadzonych do systemu Eurodac.

(5) Ponieważ organ zarządzający powinien posiadać autonomię prawną, administracyjną i finansową, dlatego ustanowiono go w formie agencji regulacyjnej (zwanej dalej „Agencją") posiadającej osobowość prawną. Stosownie do uzgodnień, siedziba Agencji została ustanowiona w Tallinie, w Estonii. Jednak z uwagi na fakt, iż zadania związane z rozwojem technicznym i przygotowaniami do zarządzania operacyjnego SIS II i VIS są prowadzone w Strasburgu, we Francji, a obiekt zapasowy tych systemów został umieszczony w Sankt Johann im Pongau, w Austrii, zgodnie z lokalizacjami systemów SIS II i VIS ustanowionymi na mocy stosownych unijnych aktów prawnych, nie należy zmieniać tego stanu rzeczy. Te dwie lokalizacje powinny również pozostać miejscami, w których – odpowiednio – prowadzone są działania związane z zarządzaniem operacyjnym Eurodac oraz gdzie znajduje się obiekt zapasowy Eurodac. Te dwie lokalizacje powinny również być miejscami – odpowiednio – rozwoju technicznego innych wielkoskalowych systemów informatycznych w przestrzeni wolności, bezpieczeństwa i sprawiedliwości i operacyjnego zarządzania nimi oraz lokalizacji obiektu zapasowego zdolnego zapewnić funkcjonowanie wielkoskalowego systemu informatycznego w przypadku awarii tego wielkoskalowego systemu informatycznego. Aby zapewnić maksymalne wykorzystywanie obiektu zapasowego, obiekt ten mógłby również być wykorzystywany do równoczesnej obsługi systemów, przy jednoczesnym spełnieniu warunku podtrzymania zdolności działania w przypadku awarii jednego lub większej liczby systemów. Ze względu na wysoki poziom bezpieczeństwa, dostępności oraz kluczowe znaczenie systemów, w przypadku gdy potencjał hostingowy istniejących centrów technicznych stałby się niewystarczający, zarząd Agencji (zwany dalej „zarządem") powinien mieć możliwość zaproponowania, w przypadku gdy jest to uzasadnione w oparciu o ocenę skutków oraz analizę kosztów i korzyści, stworzenia drugiego odrębnego centrum technicznego w Strasburgu albo w Sankt Johann im Pongau, albo, w razie potrzeby, w obu tych miejscach w celu zapewnienia hostingu tych systemów. Przed powiadomieniem Parlamentu Europejskiego i Rady (zwanych dalej „władzą budżetową") o zamiarze zrealizowania jakiegokolwiek projektu związanego z nieruchomością zarząd powinien skonsultować się z Komisją i uwzględnić jej opinię.

(6) Z chwilą podjęcia obowiązków w dniu 1 grudnia 2012 r. Agencja przejęła zadania powierzone organowi zarządzającemu w odniesieniu do VIS na mocy rozporządzenia (WE) nr 767/2008 i decyzji Rady 2008/633/WSiSW ([5]). W kwietniu 2013 r. Agencja przejęła również zadania powierzone organowi zarządzającemu w odniesieniu do systemu SIS II na mocy rozporządzenia (WE) nr 1987/2006 i decyzji Rady 2007/533/WSiSW, po uruchomieniu systemu, a w czerwcu 2013 r. przejęła zadania powierzone Komisji w odniesieniu do Eurodac zgodnie z rozporządzeniami (WE) nr 2725/2000 i (WE) nr 407/2002.

(7) Pierwsza ocena pracy Agencji przeprowadzona w latach 2015–2016 na podstawie niezależnej oceny zewnętrznej wykazała, że Agencja skutecznie zapewnia zarządzanie operacyjne wielkoskalowymi systemami informatycznymi oraz wypełnia inne powierzone jej zadania, lecz także że w rozporządzeniu (UE) nr 1077/2011 potrzeba szeregu zmian, takich jak przekazanie Agencji zadań z zakresu infrastruktury łączności pozostających w gestii Komisji. Opierając się na tej zewnętrznej ocenie, Komisja wzięła pod uwagę zmiany polityczne, prawne oraz zmiany

([1]) Rozporządzenie Rady (WE) nr 2725/2000 z dnia 11 grudnia 2000 r. dotyczące ustanowienia systemu „Eurodac" do porównywania odcisków palców w celu skutecznego stosowania konwencji dublińskiej (Dz.U. L 316 z 15.12.2000, s. 1).

([2]) Rozporządzenie Rady (WE) nr 407/2002 z dnia 28 lutego 2002 r. ustanawiające niektóre zasady wykonania rozporządzenia (WE) nr 2725/2000 dotyczącego ustanowienia systemu „Eurodac" do porównywania odcisków palców w celu skutecznego stosowania Konwencji dublińskiej (Dz.U. L 62 z 5.3.2002, s. 1).

([3]) Rozporządzenie (UE) nr 603/2013 Parlamentu Europejskiego i Rady z dnia 26 czerwca 2013 r. w sprawie ustanowienia systemu Eurodac do porównywania odcisków palców w celu skutecznego stosowania rozporządzenia (UE) nr 604/2013 w sprawie ustanowienia kryteriów i mechanizmów ustalania państwa członkowskiego odpowiedzialnego za rozpatrzenie wniosku o udzielenie ochrony międzynarodowej złożonego w jednym z państw członkowskich przez obywatela państwa trzeciego lub bezpaństwowca oraz w sprawie występowania o porównanie z danymi Eurodac przez organy ścigania państw członkowskich i Europol na potrzeby ochrony porządku publicznego, oraz zmieniające rozporządzenie (UE) nr 1077/2011 ustanawiające Europejską Agencję ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości (Dz.U. L 180 z 29.6.2013, s. 1).

([4]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1077/2011 z dnia 25 października 2011 r. ustanawiające Europejską Agencję ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości (Dz.U. L 286 z 1.11.2011, s. 1).

([5]) Decyzja Rady 2008/633/WSiSW z dnia 23 czerwca 2008 r. w sprawie dostępu wyznaczonych organów państw członkowskich i Europolu do Wizowego Systemu Informacyjnego (VIS) do celów jego przeglądania, w celu zapobiegania przestępstwom terrorystycznym i innym poważnym przestępstwom, ich wykrywania i ścigania (Dz.U. L 218 z 13.8.2008, s. 129).

okoliczności faktycznych i zaproponowała, w szczególności w swoim sprawozdaniu z dnia 29 czerwca 2017 r. dotyczącym działania Europejskiej Agencji ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości (eu-LISA) (zwanym dalej „sprawozdaniem z oceny"), aby zakres uprawnień Agencji został rozszerzony na wykonywanie zadań wynikających z przyjęcia przez współprawodawców wniosków ustawodawczych powierzających Agencji nowe systemy oraz zadań, o których mowa w komunikacie Komisji z dnia 6 kwietnia 2016 r. zatytułowanym „Sprawniejsze i bardziej inteligentne systemy informacyjne do celów zarządzania granicami i zapewnienia bezpieczeństwa", w sprawozdaniu końcowym grupy ekspertów wysokiego szczebla ds. systemów informacyjnych i interoperacyjności z dnia 11 maja 2017 r. oraz w komunikacie Komisji z dnia 16 maja 2017 r. zatytułowanym „Siódme sprawozdanie z postępu prac nad stworzeniem rzeczywistej i skutecznej unii bezpieczeństwa", pod warunkiem przyjęcia w stosownych przypadkach odpowiednich unijnych aktów prawnych. Agencji powinno się w szczególności powierzyć zadanie wypracowywania rozwiązań w zakresie interoperacyjności, określonych w komunikacie z dnia 6 kwietnia 2016 r. jako zdolność systemów informacyjnych do wymiany danych oraz do umożliwienia dzielenia się informacjami. W stosownych przypadkach we wszelkich wykonywanych działaniach w zakresie interoperacyjności należy się kierować komunikatem Komisji z dnia 23 marca 2017 r. zatytułowanym „Europejskie ramy interoperacyjności – strategia wdrażania". Załącznik II do tego komunikatu przewiduje ogólne wytyczne, zalecenia i najlepsze praktyki dla osiągnięcia interoperacyjności oraz przynajmniej stworzenia środowiska umożliwiającego stworzenie większej interoperacyjności przy projektowaniu i wdrażaniu europejskich usług publicznych oraz zarządzaniu nimi.

(8) W sprawozdaniu z oceny stwierdzono również, że zakres uprawnień Agencji powinien zostać rozszerzony w celu umożliwienia jej doradzania państwom członkowskim w zakresie połączenia systemów krajowych z systemami centralnymi wielkoskalowych systemów informatycznych, którymi Agencja zarządza (zwanymi dalej „systemami") oraz w razie potrzeby świadczenia pomocy i wsparcia ad hoc, a także świadczenia pomocy i wsparcia służbom Komisji w kwestiach technicznych związanych z nowymi systemami.

(9) Należy powierzyć Agencji przygotowywanie i rozwijanie systemu wjazdu/wyjazdu (EES) ustanowionego rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2017/2226 ([1]) oraz zarządzanie operacyjne tym systemem.

(10) Należy również powierzyć Agencji zarządzanie operacyjne osobnym bezpiecznym kanałem transmisji elektronicznej zwanym DubliNet, ustanowionym na mocy art. 18 rozporządzenia Komisji (WE) nr 1560/2003 ([2]), z którego organy państw członkowskich właściwe w sprawach azylu powinny korzystać do celów wymiany informacji o osobach ubiegających się o ochronę międzynarodową.

(11) Ponadto należy powierzyć Agencji przygotowywanie i rozwijanie europejskiego systemu informacji o podróży i zezwoleń na podróż (ETIAS) ustanowionego rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2018/1284 ([3]) oraz operacyjne zarządzanie nim.

(12) Główną rolą Agencji powinno być nadal wykonywanie zadań z zakresu zarządzania operacyjnego systemów SIS II, VIS, Eurodac, EES, DublinNet, ETIAS, a także, jeśli zostanie tak postanowione, innymi wielkoskalowymi systemami informatycznymi w przestrzeni wolności, bezpieczeństwa i sprawiedliwości. Agencja powinna także odpowiadać za środki techniczne, które są niezbędne do wykonywania nałożonych na nią nienormatywnych zadań. Obowiązki te powinny pozostawać bez uszczerbku dla zadań normatywnych zastrzeżonych dla samej Komisji lub dla Komisji wspomaganej przez odpowiedni komitet w odpowiednich unijnych aktach prawnych regulujących systemy.

(13) Agencja powinna być w stanie wdrażać rozwiązania techniczne służące spełnieniu wymogów dostępności określonych w unijnych aktach prawnych regulujących systemy, w pełni przestrzegając przy tym przepisów szczególnych tych aktów w odniesieniu do architektury technicznej danych systemów. W przypadku gdy te rozwiązania techniczne wymagają zduplikowania systemu lub elementów systemu, należy przeprowadzić niezależną ocenę skutków oraz analizę kosztów i korzyści, a decyzję powinien podjąć zarząd po zasięgnięciu opinii Komisji.

([1]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/2226 z dnia 30 listopada 2017 r. ustanawiające system wjazdu/wyjazdu (EES) w celu rejestrowania danych dotyczących wjazdu i wyjazdu obywateli państw trzecich przekraczających granice zewnętrzne państw członkowskich i danych dotyczących odmowy wjazdu w odniesieniu do takich obywateli oraz określające warunki dostępu do EES na potrzeby ochrony porządku publicznego i zmieniające konwencję wykonawczą do układu z Schengen i rozporządzenia (WE) nr 767/2008 i (UE) nr 1077/2011 (Dz.U. L 327 z 9.12.2017, s. 20).

([2]) Rozporządzenie Komisji (WE) nr 1560/2003 z dnia 2 września 2003 r. ustanawiające szczegółowe zasady stosowania rozporządzenia Rady (WE) nr 343/2003 ustanawiającego kryteria i mechanizmy określania państwa członkowskiego właściwego dla rozpatrywania wniosku o azyl, wniesionego w jednym z państw członkowskich przez obywatela państwa trzeciego (Dz.U. L 222 z 5.9.2003, s. 3).

([3]) Rozporządzenie Parlamentu Europejskiego i Rady 2018/1240 z dnia 12 września 2018 r. ustanawiające europejski system informacji o podróży oraz zezwoleń na podróż (ETIAS) i zmieniające rozporządzenia (UE) nr 1077/2011, (UE) nr 515/2014, (UE) 2016/399, (UE) 2016/1624 i (UE) 2017/2226 (Dz.U. L 236 z 19.9.2018, s. 1).

Ocena wpływu powinna również obejmować analizę potrzeb istniejących centrów technicznych w zakresie hostingu, związanych z rozwijaniem takich rozwiązań technicznych, a także analizę ewentualnych zagrożeń wynikających z aktualnej konfiguracji operacyjnej.

(14) Nie jest już uzasadnione, aby w gestii Komisji pozostawały niektóre zadania związane z infrastrukturą łączności systemów, dlatego zadania te powinny zostać przekazane Agencji, aby poprawić spójność zarządzania infrastrukturą łączności. Jednakże w przypadku systemów korzystających z EuroDomain – zabezpieczonej infrastruktury łączności zapewnianej przez TESTA-ng (nowej generacji transeuropejską telematyczną sieć komunikacyjną między administracjami), utworzonej jako część programu ISA ustanowionego decyzją Parlamentu Europejskiego i Rady nr 9922/2009/WE ([1]) oraz kontynuowanej jako część programu ISA2 ustanowionego decyzją Parlamentu Europejskiego i Rady (UE) 2015/2240 ([2]), zadania z zakresu wykonywania budżetu, nabywania i odnawiania oraz kwestii umownych powinny pozostać w gestii Komisji.

(15) Agencja powinna mieć możliwość powierzenia zadań związanych z dostarczaniem, tworzeniem, utrzymywaniem i monitorowaniem infrastruktury łączności podmiotom lub instytucjom zewnętrznym z sektora prywatnego zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE, Euratom) 2018/1046 ([3]). Agencja powinna dysponować wystarczającymi zasobami budżetowymi i kadrowymi, aby w jak największym stopniu ograniczyć konieczność zlecania podwykonawstwa swoich zadań i obowiązków podmiotom lub instytucjom zewnętrznym z sektora prywatnego.

(16) Agencja powinna nadal wykonywać zadania związane ze szkoleniami w zakresie technicznego użytkowania systemów SIS II, VIS i Eurodac oraz innych systemów powierzanych jej w przyszłości.

(17) Aby pomóc w kształtowaniu opartej na dowodach unijnej polityki w dziedzinie migracji i bezpieczeństwa oraz w monitorowaniu prawidłowego funkcjonowania systemów, Agencja powinna zestawiać i publikować statystyki, opracowywać sprawozdania statystyczne i udostępniać je stosownym podmiotom zgodnie z unijnymi aktami prawnymi regulującymi te systemy, na przykład w celu monitorowania wykonania rozporządzenia Rady (UE) nr 1053/2013 ([4]) i na potrzeby przeprowadzania analizy ryzyka i oceny narażenia zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/1624 ([5]).

(18) Powinno być możliwe nałożenie na Agencję odpowiedzialności za przygotowywanie i rozwijanie dodatkowych wielkoskalowych systemów informatycznych oraz za zarządzanie operacyjne tymi systemami na podstawie art. 67–89 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE). Przykładami takich systemów mogłyby być scentralizowany system identyfikacji państw członkowskich posiadających informacje o wyrokach skazujących wydanych wobec obywateli państw trzecich i bezpaństwowców na potrzeby uzupełnienia i wsparcia europejskiego systemu przekazywania informacji z rejestrów karnych (system ECRIS-TCN) lub skomputeryzowany system łączności transgranicznej w postępowaniach cywilnych i karnych (e-CODEX). Takie systemy można jednak powierzyć Agencji jedynie w drodze kolejnych, odrębnych unijnych aktów prawnych, po przeprowadzeniu oceny skutków.

(19) Zakres uprawnień Agencji w zakresie badań powinien zostać rozszerzony, tak aby zwiększyć jej możliwości w obszarze aktywniejszego proponowania właściwych i potrzebnych zmian technicznych w systemach. Agencja powinna nie tylko mieć możliwość monitorowania działań badawczych istotnych dla zarządzania operacyjnego systemami, lecz także wnoszenia własnego wkładu w realizację odpowiednich części programu ramowego w zakresie badań naukowych i innowacji, w przypadku gdy Komisja przekazała Agencji stosowne uprawnienia. Agencja powinna co najmniej raz w roku przekazywać Parlamentowi Europejskiemu, Radzie oraz, w przypadku gdy przetwarzane są dane osobowe, Europejskiemu Inspektorowi Ochrony Danych informacje na temat takiego monitoringu.

([1]) Decyzja Parlamentu Europejskiego i Rady nr 922/2009/WE z dnia 16 września 2009 r. w sprawie rozwiązań interoperacyjnych dla europejskich administracji publicznych (ISA), (Dz.U. L 280 z 3.10.2009, s. 20).

([2]) Decyzja Parlamentu Europejskiego i Rady (UE) 2015./2240 z dnia 25 listopada 2015 r. ustanawiająca program na rzecz rozwiązań interoperacyjnych i wspólnych ram dla europejskich administracji publicznych, przedsiębiorstw i obywateli (program ISA2) jako środek modernizacji sektora publicznego (Dz.U. L 318 z 4.12.2015, s. 1).

([3]) Rozporządzenie Parlamentu Europejskiego i Rady (UE, Euratom) 2018/1046 z dnia 18 lipca 2018 r. w sprawie zasad finansowych mających zastosowanie do budżetu ogólnego Unii, zmieniające rozporządzenia (UE) nr 1296/2013, (UE) nr 1301/2013, (UE) nr 1303/2013, (UE) nr 1304/2013, (UE) nr 1309/2013, (UE) nr 1316/2013, (UE) nr 223/2014 i (UE) nr 283/2014 oraz decyzję nr 541/2014/UE, a także uchylające rozporządzenie (UE, Euratom) nr 966/2012 (Dz.U. L 193 z 30.7.2018, s. 1).

([4]) Rozporządzenie Rady (UE) nr 1053/2013 z dnia 7 października 2013 r. w sprawie ustanowienia mechanizmu oceny i monitorowania w celu weryfikacji stosowania dorobku Schengen oraz uchylenia decyzji komitetu wykonawczego z dnia 16 września 1998 r. dotyczącej utworzenia Stałego Komitetu ds. Oceny i Wprowadzania w Życie Dorobku Schengen (Dz.U. L 295 z 6.11.2013, s. 27).

([5]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/1624 z dnia 14 września 2016 r. w sprawie Europejskiej Straży Granicznej i Przybrzeżnej, zmieniające rozporządzenie Parlamentu Europejskiego (UE) 2016/399 oraz uchylające rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 863/2007, rozporządzenie Rady (WE) nr 2007/2004 i decyzję Rady 2005/267/WE (Dz.U. L 251 z 16.9.2016, s. 1).

(20) Komisja powinna mieć możliwość powierzenia Agencji odpowiedzialności za realizację projektów pilotażowych o charakterze eksperymentalnym mających na celu zbadanie wykonalności działania i jego użyteczności, które można wdrożyć bez przyjmowania aktu podstawowego, zgodnie z rozporządzeniem (UE, Euratom) 2018/1046. Powinna ona ponadto mieć możliwość powierzenia Agencji zadań związanych z wykonaniem budżetu dla weryfikacji poprawności projektu finansowanego w ramach instrumentu na rzecz wsparcia finansowego w zakresie granic zewnętrznych i wiz ustanowionego w rozporządzeniu Parlamentu Europejskiego i Rady (UE) nr 515/2014 ([1]), zgodnie z rozporządzeniem (UE, Euratom) 2018/1046, po poinformowaniu o tym Parlamentu Europejskiego. Agencja powinna również mieć możliwość planowania i realizowania testów w sprawach ściśle objętych niniejszym rozporządzeniem oraz unijnymi aktami prawnymi regulującymi rozwijanie, ustanawianie, funkcjonowanie i użytkowanie systemów, takich jak testy koncepcji wirtualizacji. W przypadku powierzenia jej zadania związanego z realizacją projektu pilotażowego, Agencja powinna zwrócić szczególną uwagę na strategię Unii Europejskiej w zakresie zarządzania informacjami.

(21) Agencja powinna również udzielać państwom członkowskim, na ich wniosek, porad w zakresie połączenia systemów krajowych z systemami centralnymi przewidzianymi w unijnych aktach prawnych regulujących te systemy.

(22) Agencja powinna także udzielać państwom członkowskim, na ich wniosek i z zastrzeżeniem procedury określonej w niniejszym rozporządzeniu, doraźnego wsparcia, w przypadku gdy wymagają tego wyjątkowe wyzwania lub potrzeby w zakresie bezpieczeństwa lub migracji. W szczególności dane państwo członkowskie powinno móc zwrócić się o wzmocnienie operacyjne i techniczne i z niego skorzystać w przypadkach, w których państwo to stoi w obliczu szczególnych i wyjątkowo trudnych wyzwań związanych z migracją na konkretnych odcinkach swoich granic zewnętrznych, a wyzwania te polegają na dużym napływie migrantów. Takie wzmocnienie powinno być zapewniane na obszarach hotspotów przez zespoły wspierające zarządzanie migracjami, złożone z ekspertów z właściwych agencji Unii. W przypadku gdy w tym kontekście wymagane będzie wsparcie Agencji w zakresie spraw związanych z systemami, zainteresowane państwo członkowskie powinno przesłać wniosek o wsparcie do Komisji, która po przeprowadzaniu oceny faktycznej zasadności takiego wsparcia powinna niezwłocznie przesłać wniosek o wsparcie do Agencji. Agencja powinna poinformować o tym wniosku zarząd. Komisja powinna również sprawdzać, czy Agencja udziela we właściwym czasie odpowiedzi na wniosek o doraźne wsparcie. Roczne sprawozdanie Agencji z działalności powinno zawierać szczegółowe informacje o działaniach podjętych przez Agencję w celu udzielenia państwom członkowskim doraźnego wsparcia oraz o poniesionych w związku z tym kosztach.

(23) Agencja powinna również, w stosownych przypadkach, wspierać służby Komisji w kwestiach technicznych związanych z istniejącymi lub nowymi systemami, zwłaszcza przy przygotowywaniu nowych wniosków dotyczących wielkoskalowych systemów informatycznych, które zostaną powierzone Agencji.

(24) Grupa państw członkowskich powinna posiadać możliwość powierzenia Agencji opracowania wspólnego elementu informatycznego, zarządzania nim lub jego hostingu, aby pomóc im we wdrażaniu technicznych aspektów obowiązków wynikających z unijnych aktów prawnych dotyczących zdecentralizowanych systemów informatycznych w przestrzeni wolności, bezpieczeństwa i sprawiedliwości. Powinno to pozostawać bez uszczerbku dla obowiązków tych państw członkowskich wynikających z mających zastosowanie unijnych aktów prawnych, w szczególności w odniesieniu do struktury tych systemów. Powinno to wymagać wcześniejszej zgody Komisji, pozytywnej decyzji zarządu oraz odnotowania w umowie o delegowaniu zadań zawartej między zainteresowanym państwem członkowskim a Agencją, a finansowanie powinno być zapewniane w pełni przez zainteresowane państwo członkowskie. Agencja powinna poinformować Parlament Europejski i Radę o zatwierdzonej umowie o delegowaniu zadań oraz o wszelkich jej modyfikacjach. Inne państwa członkowskie powinny mieć możliwość uczestnictwa w takich wspólnych rozwiązaniach informatycznych, pod warunkiem że taką możliwość przewidziano w umowie o delegowaniu zadań i że w umowie tej wprowadzono niezbędne zmiany. Zadanie to nie powinno niekorzystnie wpływać na zarządzanie operacyjne systemami przez Agencję.

(25) Powierzenie Agencji zarządzania operacyjnego wielkoskalowymi systemami informatycznymi w przestrzeni wolności, bezpieczeństwa i sprawiedliwości nie powinno mieć wpływu na przepisy szczególne mające zastosowanie do tych systemów. W szczególności w pełni mają zastosowanie przepisy szczególne regulujące cel, prawa dostępu, środki bezpieczeństwa oraz dalsze wymogi w zakresie ochrony danych w odniesieniu do każdego takiego systemu.

(26) W celu skutecznego kontrolowania funkcjonowania Agencji państwa członkowskie i Komisja powinny być reprezentowane w zarządzie. Zarządowi należy powierzyć funkcje niezbędne w szczególności do przyjmowania rocznego programu prac, pełnienia funkcji związanych z budżetem Agencji, przyjmowania przepisów finansowych mających zastosowanie do Agencji oraz ustanawiania procedur podejmowania przez dyrektora wykonawczego decyzji związanych z zadaniami operacyjnymi Agencji. Zarząd powinien wykonywać te zadania w skuteczny

([1]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 515/2014 z dnia 16 kwietnia 2014 r. ustanawiające, w ramach Funduszu Bezpieczeństwa Wewnętrznego, instrument na rzecz wsparcia finansowego w zakresie granic zewnętrznych i wiz oraz uchylające decyzję nr 574/2007/WE (Dz.U. L 150 z 20.5.2014, s. 143).

i przejrzysty sposób. Po zorganizowaniu odpowiedniej procedury wyboru przez Komisję oraz po przesłuchaniu zaproponowanych kandydatów we właściwej komisji lub właściwych komisjach Parlamentu Europejskiego, zarząd powinien również powoływać dyrektora wykonawczego.

(27) Uwzględniając fakt, że do 2020 r. znacznie wzrośnie liczba wielkoskalowych systemów informatycznych powierzonych Agencji i że przydziela się jej znacznie więcej zadań, do roku 2020 odpowiednio zwiększy się liczba pracowników Agencji. Należy zatem stworzyć stanowisko zastępcy dyrektora wykonawczego Agencji, biorąc również pod uwagę fakt, że zadania związane z rozwojem systemów i z zarządzaniem operacyjnym tymi systemami będą wymagać zwiększonego i specjalnego nadzoru oraz że siedziba i centra techniczne Agencji znajdują się w trzech państwach członkowskich. Zastępcę dyrektora wykonawczego powinien powoływać zarząd.

(28) Agencją należy zarządzać i administrować z uwzględnieniem zasad wspólnego podejścia do zdecentralizowanych agencji Unii, przyjętego w dniu 19 lipca 2012 r. przez Parlament Europejski, Radę i Komisję.

(29) W odniesieniu do systemu SIS II, Agencja Unii Europejskiej ds. Współpracy Organów Ścigania (Europol) oraz Europejska Jednostka Współpracy Sądowej (Eurojust), które mają prawo bezpośredniego dostępu do danych wprowadzonych do systemu SIS II oraz bezpośredniego wyszukiwania tych danych zgodnie z decyzją 2007/533/WSiSW, powinny mieć status obserwatorów podczas posiedzeń zarządu, których porządek obrad obejmuje kwestię związaną ze stosowaniem tej decyzji. Europejska Agencja Straży Granicznej i Przybrzeżnej, która ma prawo dostępu do systemu SIS II oraz przeszukiwania tego systemu zgodnie z rozporządzeniem (UE) 2016/1624, powinna mieć status obserwatora podczas posiedzeń zarządu, których porządek obejmuje kwestię odnoszącą się do stosowania tego rozporządzenia. Europol, Eurojust oraz Europejska Agencja Straży Granicznej i Przybrzeżnej powinny mieć możliwość wyznaczenia po jednym przedstawicielu do grupy doradczej ds. SIS II ustanowionej na mocy niniejszego rozporządzenia.

(30) W odniesieniu do VIS Europol powinien mieć status obserwatora podczas posiedzeń zarządu, których porządek obejmuje kwestię odnoszącą się do stosowania decyzji 2008/633/WSiSW. Europol powinien mieć możliwość wyznaczenia przedstawiciela do grupy doradczej ds. VIS ustanowionej na mocy niniejszego rozporządzenia.

(31) W odniesieniu do Eurodac Europol powinien mieć status obserwatora podczas posiedzeń zarządu, których porządek obejmuje kwestię odnoszącą się do stosowania rozporządzenia (UE) nr 603/2013. Europol powinien mieć możliwość wyznaczenia przedstawiciela do grupy doradczej ds. Eurodac ustanowionej w niniejszym rozporządzeniu.

(32) W odniesieniu do systemu EES Europol powinien mieć status obserwatora podczas posiedzeń zarządu, których porządek obejmuje kwestię odnoszącą się do rozporządzenia (UE) 2017/2226.

(33) W odniesieniu do ETIAS Europol powinien mieć status obserwatora podczas posiedzeń zarządu, których porządek obejmuje kwestię odnoszącą się do rozporządzenia (UE) 2018/1240. Europejska Agencja Straży Granicznej i Przybrzeżnej również powinna mieć status obserwatora podczas posiedzeń zarządu, których porządek obejmuje kwestię odnoszącą się do ETIAS w związku ze stosowaniem tego rozporządzenia. Europol oraz Europejska Agencja Straży Granicznej i Przybrzeżnej powinny mieć możliwość wyznaczenia przedstawiciela do grupy doradczej ds. EES-ETIAS ustanowionej w niniejszym rozporządzeniu.

(34) Państwa członkowskie powinny mieć prawo głosu w zarządzie w zakresie wielkoskalowego systemu informatycznego, w przypadku gdy są one związane na mocy prawa Unii jakimkolwiek aktem prawnym regulującym rozwijanie, ustanawianie, funkcjonowanie i użytkowanie tego konkretnego systemu. Także Dania powinna mieć prawo głosu w odniesieniu do wielkoskalowego systemu informatycznego, jeżeli podejmie decyzję, na mocy art. 4 protokołu nr 22 w sprawie stanowiska Danii, załączonego do Traktatu o Unii Europejskiej (TUE) i TFUE, o wprowadzeniu do swojego prawa krajowego unijnego aktu prawnego regulującego rozwijanie, ustanawianie, funkcjonowanie i użytkowanie tego konkretnego systemu.

(35) Państwa członkowskie powinny wyznaczać członka grupy doradczej zajmującej się wielkoskalowym systemem informatycznym, jeżeli są one związane na mocy prawa Unii unijnym aktem prawnym regulującym rozwijanie, ustanawianie, funkcjonowanie i użytkowanie tego konkretnego systemu. Ponadto Dania powinna wyznaczać członka grupy doradczej zajmującej się wielkoskalowym systemem informatycznym, jeżeli podejmie decyzję, na mocy art. 4 protokołu nr 22, o wprowadzeniu do swojego prawa krajowego unijnego aktu prawnego regulującego rozwijanie, ustanawianie, funkcjonowanie i użytkowanie tego konkretnego systemu. W razie potrzeby grupy doradcze powinny ze sobą współpracować.

(36) Aby zagwarantować Agencji pełną autonomię i niezależność oraz umożliwić prawidłową realizację celów i zadań powierzonych jej na mocy niniejszego rozporządzenia, należy przyznać Agencji odpowiedni i autonomiczny budżet, którego dochody będą pochodzić z budżetu ogólnego Unii. Finansowanie Agencji powinno podlegać porozumieniu osiągniętemu przez Parlament Europejski i Radę, zgodnie z pkt 31 porozumienia międzyinstytu-

cjonalnego pomiędzy Parlamentem Europejskim, Radą i Komisją z dnia 2 grudnia 2013 r. w sprawie dyscypliny budżetowej, współpracy w kwestiach budżetowych i należytego zarządzania finansami ([1]). Zastosowanie powinny mieć unijne procedury budżetowe i procedury udzielania absolutorium. Kontrola sprawozdań finansowych oraz legalności i prawidłowości transakcji leżących u ich podstaw powinna być przeprowadzana przez Trybunał Obrachunkowy.

(37) Do celów wypełnienia swojej misji oraz w zakresie wymaganym do realizacji swoich zadań Agencja powinna mieć możliwość współpracy z instytucjami, organami i jednostkami organizacyjnymi Unii, zwłaszcza z tymi, które ustanowiono w przestrzeni wolności, bezpieczeństwa i sprawiedliwości, w zakresie kwestii objętych niniejszym rozporządzeniem oraz unijnymi aktami prawnymi regulującymi rozwijanie, ustanawianie, funkcjonowanie i użytkowanie systemów w ramach porozumień roboczych zawartych zgodnie z prawem i polityką Unii, a także w ramach ich odnośnych kompetencji. Jeśli jest to przewidziane w unijnym akcie prawnym, należy także zezwolić Agencji na prowadzenie współpracy z organizacjami międzynarodowymi i innymi właściwymi podmiotami oraz umożliwić jej zawieranie w tym celu porozumień roboczych. Takie porozumienia robocze powinny zostać wcześniej zatwierdzone przez Komisję i uzyskać zgodę zarządu. Agencja powinna również w stosownych przypadkach konsultować się z Agencją Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA), ustanowioną w rozporządzeniu Parlamentu Europejskiego i Rady (UE) nr 526/2013 ([2]), i stosować się do jej zaleceń dotyczących bezpieczeństwa sieci.

(38) Zapewniając rozwijanie systemów i zarządzanie operacyjne tymi systemami, Agencja powinna przestrzegać norm europejskich i międzynarodowych oraz uwzględniać najwyższe wymogi specjalistyczne, w szczególności strategię Unii Europejskiej w zakresie zarządzania informacjami.

(39) Do przetwarzania danych osobowych przez Agencję powinno mieć zastosowanie rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 ([3]), bez uszczerbku dla przepisów dotyczących ochrony danych, przewidzianych w unijnych aktach prawnych regulujących rozwijanie, tworzenie, funkcjonowanie i użytkowanie systemów, które to przepisy powinny być spójne z rozporządzeniem (UE) 2018/1725 . Aby utrzymać bezpieczeństwo i zapobiegać przetwarzaniu danych naruszającemu rozporządzenie (UE) 2018/1725 lub unijne akty prawne regulujące poszczególne systemy, Agencja dokonuje oceny ryzyka wynikającego z przetwarzania danych i wdraża środki mające na celu zmniejszenie tego ryzyka, jak np. szyfrowanie. Środki takie powinny zapewnić odpowiedni poziom bezpieczeństwa, w tym poufność, oraz uwzględniać stan wiedzy technicznej oraz koszty ich wdrożenia w stosunku do ryzyka i charakteru danych osobowych podlegających ochronie. Oceniając ryzyko w zakresie bezpieczeństwa danych, należy wziąć pod uwagę ryzyko związane z przetwarzaniem danych osobowych – takie jak przypadkowe lub niezgodne z prawem zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych – i mogące w szczególności prowadzić do uszczerbku fizycznego, szkód majątkowych i niemajątkowych. Europejski Inspektor Ochrony Danych powinien mieć możliwość uzyskiwania od Agencji dostępu do wszystkich informacji niezbędnych dla prowadzonych przez niego postępowań. Zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (WE) nr 45/2001 ([4]) Komisja skonsultowała się z Europejskim Inspektorem Ochrony Danych, który wydał opinię w dniu 10 października 2017 r.

(40) Aby zapewnić przejrzyste funkcjonowanie Agencji, powinno mieć do niej zastosowanie rozporządzenie (WE) nr 1049/2001 Parlamentu Europejskiego i Rady ([5]). Agencja powinna prowadzić działalność w możliwie najbardziej przejrzysty sposób, który nie utrudnia osiągania celu jej operacji. Agencja powinna podawać do wiadomości publicznej informacje dotyczące wszystkich jej działań. Powinna ona także zapewnić szybkie przekazywanie społeczeństwu i wszystkim zainteresowanym stronom informacji odnoszących się do jej pracy.

(41) Działania Agencji powinny podlegać kontroli Europejskiego Rzecznika Praw Obywatelskich zgodnie z art. 228 TFUE.

([1]) Dz.U. C 373 z 20.12.2013, s. 1.

([2]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 526/2013 z dnia 21 maja 2013 r. w sprawie Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA) oraz uchylające rozporządzenie (WE) nr 460/2004 (Dz.U. L 165 z 18.6.2013, s. 41).

([3]) 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 (zob. s. 39 niniejszego Dziennika Urzędowego).

([4]) Rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady 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).

([5]) 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).

(42) Do Agencji należy stosować rozporządzenie Parlamentu Europejskiego i Rady (UE, Euratom) nr 883/2013 ([1]); powinna ona przystąpić do Porozumienia międzyinstytucjonalnego z dnia 25 maja 1999 r. między Parlamentem Europejskim, Radą Unii Europejskiej i Komisją Wspólnot Europejskich dotyczącego dochodzeń wewnętrznych prowadzonych przez Europejski Urząd ds. Zwalczania Nadużyć Finansowych (OLAF) ([2]).

(43) Do Agencji powinno mieć zastosowanie rozporządzenie Rady (UE) 2017/1939 ([3]) dotyczące ustanowienia Prokuratury Europejskiej.

(44) Aby zapewnić otwarte i przejrzyste warunki zatrudnienia oraz równe traktowanie pracowników, do pracowników (w tym dyrektora wykonawczego Agencji i jego zastępcy) powinny mieć zastosowanie regulamin pracowniczy urzędników Unii Europejskiej (zwany dalej „regulaminem pracowniczym urzędników") i warunki zatrudnienia innych pracowników Unii Europejskiej (zwane dalej „warunkami zatrudnienia innych pracowników"), ustanowione w rozporządzeniu Rady (EWG, Euratom, EWWiS) nr 259/68 ([4]) (zwane łącznie „regulaminem pracowniczym"), w tym również przepisy dotyczące tajemnicy służbowej lub inne równoważne wymogi poufności.

(45) Ponieważ Agencja jest organem ustanowionym przez Unię w rozumieniu rozporządzenia (UE, Euratom) 2018/1046, powinna ona w związku z tym przyjąć swoje przepisy finansowe.

(46) Do Agencji powinno mieć zastosowanie rozporządzenie delegowane Komisji (UE) nr 1271/2013 ([5]).

(47) Agencja ustanowiona niniejszym rozporządzeniem zastępuje Europejską Agencję ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości ustanowioną rozporządzeniem (UE) nr 1077/2011 i jest jej następcą prawnym. Powinna ona zatem być jej następcą prawnym w odniesieniu do wszystkich umów zawartych przez Europejską Agencję ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości ustanowioną rozporządzeniem (UE) nr 1077/2011, ciążących na niej zobowiązań i nabytego przez nią majątku. Niniejsze rozporządzenie nie powinno wpływać na moc prawną umów, porozumień roboczych i protokołów ustaleń zawartych przez Agencję ustanowioną rozporządzeniem (UE) nr 1077/2011, bez uszczerbku dla wszelkich zmian wprowadzonych do tych umów, porozumień i protokołów na mocy niniejszego rozporządzenia.

(48) Aby Agencja mogła nadal jak najlepiej wypełniać zadania Europejskiej Agencji ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości ustanowionej rozporządzeniem (UE) nr 1077/2011, należy określić środki przejściowe, w szczególności odnośnie do zarządu, grup doradczych, dyrektora wykonawczego oraz regulaminu wewnętrznego przyjmowanego przez zarząd.

(49) Niniejsze rozporządzenie ma na celu zmianę i rozszerzenie przepisów rozporządzenia (UE) nr 1077/2011. Z uwagi na znaczną liczbę i istotny charakter zmian, które należy wprowadzić niniejszym rozporządzeniem, rozporządzenie to powinno w celu zapewnienia jasności zostać zastąpione w całości w odniesieniu do państw członkowskich związanych niniejszym rozporządzeniem. Agencja ustanowiona na mocy niniejszego rozporządzenia powinna zastąpić agencję ustanowioną rozporządzeniem (UE) nr 1077/2011 i przejąć jej funkcje, a rozporządzenie to należy w związku z tym uchylić.

(50) Ponieważ cele niniejszego rozporządzenia, a mianowicie ustanowienie na poziomie Unii agencji odpowiadającej za zarządzanie operacyjne wielkoskalowymi systemami informatycznymi w przestrzeni wolności, bezpieczeństwa i sprawiedliwości oraz, w stosownych przypadkach, za rozwijanie takich systemów, nie mogą zostać osiągnięte w sposób wystarczający przez państwa członkowskie, natomiast ze względu na rozmiary i skutki tych działań możliwe jest lepsze ich osiągnięcie na poziomie Unii, Unia może przyjąć środki zgodnie z zasadą pomocniczości określoną w art. 5 TUE. Zgodnie z zasadą proporcjonalności określoną w tym artykule niniejsze rozporządzenie nie wykracza poza to, co jest konieczne do osiągnięcia tych celów.

([1]) Rozporządzenie Parlamentu Europejskiego i Rady (UE, Euratom) nr 883/2013 z dnia 11 września 2013 r. dotyczące dochodzeń prowadzonych przez Europejski Urząd ds. Zwalczania Nadużyć Finansowych (OLAF) oraz uchylające rozporządzenie (WE) nr 1073/1999 Parlamentu Europejskiego i Rady, i rozporządzenie Rady (Euratom) nr 1074/1999 (Dz.U. L 248 z 18.9.2013, s. 1).

([2]) Dz.U. L 136 z 31.5.1999, s. 15.

([3]) 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).

([4]) Rozporządzenie Rady (EWG, Euratom, EWWiS) nr 259/68 z dnia 29 lutego 1968 r. ustanawiające regulamin pracowniczy urzędników i warunki zatrudnienia innych pracowników Wspólnot Europejskich oraz ustanawiające specjalne środki stosowane tymczasowo wobec urzędników Komisji (Dz.U. L 56 z 4.3.1968, s. 1).

([5]) Rozporządzenie delegowane Komisji (UE) nr 1271/2013 z dnia 30 września 2013 r. w sprawie ramowego rozporządzenia finansowego dotyczącego organów, o których mowa w art. 208 rozporządzenia Parlamentu Europejskiego i Rady (UE, Euratom) nr 966/2012 (Dz.U. L 328 z 7.12.2013, s. 42).

(51) Zgodnie z art. 1 i 2 protokołu nr 22 Dania nie uczestniczy w przyjęciu niniejszego rozporządzenia i nie jest nim związana ani go nie stosuje. Ponieważ niniejsze rozporządzenie – w zakresie, w jakim odnosi się do systemów SIS II, VIS, EES i ETIAS – stanowi rozwinięcie przepisów dorobku Schengen, zgodnie z art. 4 tego protokołu Dania – w terminie sześciu miesięcy po przyjęciu prze Radę niniejszego rozporządzenia – podejmuje decyzję, czy dokona jego włączenia do swojego prawa krajowego. Zgodnie z art. 3 umowy pomiędzy Wspólnotą Europejską i Królestwem Danii w sprawie kryteriów i mechanizmów określania państwa członkowskiego właściwego dla rozpatrywania wniosku o azyl, wniesionego w Danii lub innym państwie członkowskim Unii Europejskiej, i „Eurodac" do porównywania odcisków palców w celu skutecznego stosowania konwencji dublińskiej ([1]) Dania powiadomi Komisję o tym, czy wdroży niniejsze rozporządzenie w zakresie, w jakim odnosi się ono do Eurodac i DubliNet.

(52) W zakresie, w jakim przepisy niniejszego rozporządzenia odnoszą się do systemu SIS II regulowanego decyzją 2007/533/WSiSW, Zjednoczone Królestwo uczestniczy w niniejszym rozporządzeniu zgodnie z art. 5 ust. 1 Protokołu nr 19 w sprawie dorobku Schengen włączonego w ramy Unii Europejskiej, załączonego do TUE i TFUE, oraz art. 8 ust. 2 decyzji Rady 2000/365/WE ([2]). W zakresie, w jakim przepisy niniejszego rozporządzenia odnoszą się do systemu SIS II regulowanego rozporządzeniem (WE) nr 1987/2006 oraz do systemów VIS, EES oraz ETIAS, niniejsze rozporządzenie stanowi rozwinięcie przepisów dorobku Schengen, które nie mają zastosowania do Zjednoczonego Królestwa zgodnie z decyzją Rady 2000/365/WE; Zjednoczone Królestwo wystąpiło, pismem z dnia 19 lipca 2018 r. skierowanym do przewodniczącego Rady, z wnioskiem o zastosowanie wobec niego niniejszego rozporządzenia, zgodnie z art. 4 Protokołu nr 19. Na mocy art. 1 decyzji Rady (UE) 2018/1600 ([3]) Zjednoczone Królestwo uczestniczy w niniejszym rozporządzeniu. Ponadto w zakresie, w jakim przepisy niniejszego rozporządzenia odnoszą się do systemu Eurodac i DubliNet, Zjednoczone Królestwo notyfikowało, pismem z dnia 23 października 2017 r. skierowanym do przewodniczącego Rady, swoje życzenie uczestniczenia w przyjęciu i stosowaniu niniejszego rozporządzenia, zgodnie z art. 3 Protokołu nr 21 w sprawie stanowiska Zjednoczonego Królestwa i Irlandii w odniesieniu do przestrzeni wolności, bezpieczeństwa i sprawiedliwości, załączonego do TUE i do TFUE. W związku z tym Zjednoczone Królestwo uczestniczy w przyjęciu niniejszego rozporządzenia, jest nim związane i je stosuje.

(53) W zakresie, w jakim przepisy niniejszego rozporządzenia odnoszą się do systemu SIS II regulowanego decyzją 2007/533/WSiSW, Irlandia może, co do zasady, uczestniczyć w niniejszym rozporządzeniu zgodnie z art. 5 ust. 1 Protokołu nr 19 oraz art. 6 ust. 2 decyzji Rady 2002/192/WE ([4]). W zakresie, w jakim przepisy niniejszego rozporządzenia odnoszą się do systemu SIS II regulowanego rozporządzeniem (WE) nr 1987/2006 i do systemów VIS, EES oraz ETIAS, stanowi ono rozwinięcie przepisów dorobku Schengen, które nie mają zastosowania do Irlandii zgodnie z decyzją 2002/192/WE. Irlandia nie zwróciła się o uczestnictwo w przyjęciu niniejszego rozporządzenia zgodnie z art. 4 protokołu nr 19. Irlandia nie uczestniczy w związku z tym w jego przyjęciu i nie jest nim związana, ani go nie stosuje w zakresie, w jakim jego środki stanowią rozwinięcie dorobku Schengen w odniesieniu do systemu SIS II regulowanego rozporządzeniem (WE) nr 1987/2006 oraz do systemu VIS, do EEA oraz do ETIAS. Ponadto w zakresie, w jakim przepisy niniejszego rozporządzenia odnoszą się do systemu Eurodac i DubliNet, zgodnie z art. 1 i 2 oraz art. 4a ust. 1 Protokołu nr 21, Irlandia nie uczestniczy w przyjęciu niniejszego rozporządzenia i nie jest nim związana ani go nie stosuje. Ponieważ w tej sytuacji nie jest możliwe zapewnienie stosowania w całości niniejszego rozporządzenia w Irlandii, zgodnie z wymogiem określonym w art. 288 TFUE, Irlandia nie uczestniczy w przyjęciu niniejszego rozporządzenia, nie jest nim związana ani go nie stosuje, z zastrzeżeniem jej praw wynikających z Protokołu nr 19 i 21.

(54) W odniesieniu do Islandii i Norwegii niniejsze rozporządzenie stanowi – w zakresie, w jakim odnosi się ono do systemów SIS II i VIS, do EES oraz do ETIAS – rozwinięcie przepisów dorobku Schengen w rozumieniu Umowy zawartej przez Radę Unii Europejskiej i Republikę Islandii oraz Królestwo Norwegii dotyczącej włączenia tych dwóch państw we wprowadzanie w życie, stosowanie i rozwój dorobku Schengen ([5]) – które wchodzą w zakres obszaru, o którym mowa w art. 1 lit. A, B i G decyzji Rady 1999/437/WE ([6]). W odniesieniu do Eurodac i DubliNet

([1]) Dz.U. L 66 z 8.3.2006, s. 38.
([2]) Decyzja Rady 2000/365/WE z dnia 29 maja 2000 r. dotycząca wniosku Zjednoczonego Królestwa Wielkiej Brytanii i Irlandii Północnej o zastosowaniu wobec niego niektórych przepisów dorobku Schengen (Dz.U. L 131 z 1.6.2000, s. 43).
([3]) Decyzja Rady (UE) 2018/1600 z dnia 28 września 2018 r. w sprawie wniosku Zjednoczonego Królestwa Wielkiej Brytanii i Irlandii Północnej o zastosowanie wobec niego niektórych przepisów dorobku Schengen dotyczących Agencji Unii Europejskiej ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości (eu-LISA) (Dz.U. L 267 z 25.10.2018, s. 3).
([4]) Decyzja Rady 2002/192/WE z dnia 28 lutego 2002 r. dotycząca wniosku Irlandii o zastosowanie wobec niej niektórych przepisów dorobku Schengen (Dz.U. L 64 z 7.3.2002, s. 20).
([5]) Dz.U. L 176 z 10.7.1999, s. 36.
([6]) Decyzja Rady 1999/437/WE z dnia 17 maja 1999 r. w sprawie niektórych warunków stosowania Układu zawartego przez Radę Unii Europejskiej i Republikę Islandii oraz Królestwo Norwegii dotyczącego włączenia tych dwóch państw we wprowadzanie w życie, stosowanie i rozwój dorobku Schengen (Dz.U. L 176 z 10.7.1999, s. 31).

niniejsze rozporządzenie stanowi nowy środek w rozumieniu Umowy między Wspólnotą Europejską a Republiką Islandii i Królestwem Norwegii dotyczącej kryteriów i mechanizmów określania państwa właściwego dla rozpatrywania wniosku o azyl złożonego w państwie członkowskim lub w Islandii, lub Norwegii ([1]). W związku z tym, zależnie od decyzji Republiki Islandii i Królestwa Norwegii o włączeniu rozporządzenia do ich krajowych porządków prawnych, delegacje Republiki Islandii i Królestwa Norwegii powinny uczestniczyć w zarządzie Agencji. W celu określenia dalszych szczegółowych zasad pozwalających na uczestnictwo Republiki Islandii i Królestwa Norwegii w działaniach Agencji należy dokonać dalszych ustaleń między Unią a tymi państwami.

(55) W odniesieniu do Szwajcarii niniejsze rozporządzenie stanowi – w zakresie, w jakim odnosi się ono do systemów SIS II i VIS, do EES oraz do ETIAS – rozwinięcie przepisów dorobku Schengen w rozumieniu Umowy między Unią Europejską, Wspólnotą Europejską a Konfederacją Szwajcarską w sprawie włączenia Konfederacji Szwajcarskiej we wprowadzanie w życie, stosowanie i rozwój dorobku Schengen ([2]), które wchodzą w zakres obszaru, o którym mowa w art. 1 lit. A, B i G decyzji 1999/437/WE w związku z art. 3 decyzji Rady 2008/146/WE ([3]). W odniesieniu do Eurodac i DubliNet niniejsze rozporządzenie stanowi nowy środek dotyczący Eurodac w rozumieniu Umowy między Wspólnotą Europejską a Konfederacją Szwajcarską dotyczącej kryteriów i mechanizmów umożliwiających określanie państwa właściwego dla rozpatrywania wniosku o azyl złożonego w państwie członkowskim lub w Szwajcarii ([4]). W związku z tym, zależnie od decyzji Konfederacji Szwajcarskiej o włączeniu rozporządzenia do jej krajowego porządku prawnego, delegacja Konfederacji Szwajcarskiej powinna uczestniczyć w zarządzie Agencji. W celu określenia dalszych szczegółowych zasad pozwalających na uczestnictwo Konfederacji Szwajcarskiej w działaniach Agencji należy dokonać dalszych ustaleń między Unią a Konfederacją Szwajcarską.

(56) W odniesieniu do Liechtensteinu niniejsze rozporządzenie stanowi – w zakresie, w jakim odnosi się ono do systemów SIS II i VIS, do EES oraz do ETIAS – rozwinięcie przepisów dorobku Schengen w rozumieniu Protokołu między Unią Europejską, Wspólnotą Europejską, Konfederacją Szwajcarską i Księstwem Liechtensteinu o przystąpieniu Księstwa Liechtensteinu do Umowy między Unią Europejską, Wspólnotą Europejską a Konfederacją Szwajcarską w sprawie włączenia Konfederacji Szwajcarskiej we wprowadzanie w życie, stosowanie i rozwój dorobku Schengen ([5]), które wchodzą w zakres obszaru, o którym mowa w art. 1 lit. A, B i G decyzji 1999/437/WE w związku z art. 3 decyzji Rady 2011/350/UE ([6]).

W odniesieniu do Eurodac i DubliNet niniejsze rozporządzenie stanowi nowy środek w rozumieniu Protokołu między Wspólnotą Europejską, Konfederacją Szwajcarską i Księstwem Liechtensteinu o przystąpieniu Księstwa Liechtensteinu do Umowy między Wspólnotą Europejską a Konfederacją Szwajcarską dotyczącej kryteriów i mechanizmów określania państwa właściwego dla rozpatrywania wniosku o azyl złożonego w państwie członkowskim lub w Szwajcarii ([7]). W związku z tym, z zastrzeżeniem decyzji Księstwa Liechtensteinu o włączeniu rozporządzenia do jego krajowego porządku prawnego, delegacja Księstwa Liechtensteinu powinna uczestniczyć w zarządzie Agencji. W celu określenia dalszych szczegółowych zasad pozwalających na uczestnictwo Księstwa Liechtensteinu w działaniach Agencji należy dokonać dalszych ustaleń między Unią a Księstwem Liechtensteinu,

---

([1]) Dz.U. L 93 z 3.4.2001, s. 40.
([2]) Dz.U. L 53 z 27.2.2008, s. 52.
([3]) Decyzja Rady 2008/146/WE z dnia 28 stycznia 2008 r. w sprawie zawarcia w imieniu Wspólnoty Europejskiej Umowy między Unią Europejską, Wspólnotą Europejską i Konfederacją Szwajcarską dotyczącej włączenia tego państwa we wprowadzanie w życie, stosowanie i rozwój dorobku Schengen (Dz.U. L 53 z 27.2.2008, s. 1).
([4]) Dz.U. L 53 z 27.2.2008, s. 5.
([5]) Dz.U. L 160 z 18.6.2011, s. 21.
([6]) Decyzja Rady 2011/350/UE z dnia 7 marca 2011 r. w sprawie zawarcia w imieniu Unii Europejskiej Protokołu między Unią Europejską, Wspólnotą Europejską, Konfederacją Szwajcarską i Księstwem Liechtensteinu w sprawie przystąpienia Księstwa Liechtensteinu do Umowy między Unią Europejską, Wspólnotą Europejską i Konfederacją Szwajcarską dotyczącej włączenia Konfederacji Szwajcarskiej we wprowadzanie w życie, stosowanie i rozwój dorobku Schengen, odnoszącego się do zniesienia kontroli na granicach wewnętrznych i do przemieszczania się osób (Dz.U. L 160 z 18.6.2011, s. 19).
([7]) Dz.U. L 160 z 18.6.2011, s. 39.

PRZYJMUJĄ NINIEJSZE ROZPORZĄDZENIE:

ROZDZIAŁ I

PRZEDMIOT I CELE

Artykuł 1

Przedmiot

1. Niniejszym ustanawia się Agencję Unii Europejskiej ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości (zwaną dalej „Agencją").

2. Agencja ustanowiona niniejszym rozporządzeniem zastępuje Europejską Agencję ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości ustanowioną rozporządzeniem (UE) nr 1077/2011 i jest jej następcą prawnym.

3. Agencja odpowiada za zarządzanie operacyjne systemem informacyjnym Schengen (SIS), wizowym systemem informacyjnym (VIS) oraz Eurodac.

4. Agencja odpowiada za przygotowywanie i rozwijanie systemu wjazdu/wyjazdu (EES), DubliNet oraz europejskiego systemu informacji o podróży oraz zezwoleń na podróż (ETIAS) lub za zarządzanie operacyjne tymi systemami.

5. Agencji można powierzyć – tylko jeśli przewidują to stosowne unijne akty prawne regulujące te systemy przyjęte na podstawie art. 67–89 TFUE – przygotowywanie i rozwijanie wielkoskalowych systemów informatycznych w przestrzeni wolności, bezpieczeństwa i sprawiedliwości, innych niż te, o których mowa w ust. 3 i 4 niniejszego artykułu, lub zarządzanie operacyjne takimi systemami, włącznie z istniejącymi systemami, z uwzględnieniem, w stosownych przypadkach, rozwoju prac badawczych, o których mowa w art. 14 niniejszego rozporządzenia, a także wyników projektów pilotażowych i weryfikacji poprawności projektu, o których mowa w art. 15 niniejszego rozporządzenia.

6. Na zarządzanie operacyjne składają się wszystkie zadania niezbędne do tego, aby wielkoskalowe systemy informatyczne mogły funkcjonować zgodnie ze szczegółowymi przepisami mającymi zastosowanie do każdego z nich, włącznie z odpowiedzialnością za wykorzystywaną przez nie infrastrukturę łączności. Te wielkoskalowe systemy nie wymieniają danych ani nie pozwalają na wymianę informacji lub wiedzy, chyba że przewiduje to szczególny unijny akt prawny.

7. Agencja odpowiada również za realizację następujących zadań:

a) zapewnianie jakości danych zgodnie z art. 12;

b) prowadzenie działań koniecznych w celu zapewnienia interoperacyjności zgodnie z art. 13;

c) prowadzenie badań zgodnie z art. 14;

d) prowadzenie projektów pilotażowych, weryfikacji poprawności projektu oraz testowanie zgodnie z art. 15; oraz

e) zapewnianie wsparcia państwom członkowskim i Komisji zgodnie z art. 16.

Artykuł 2

Cele

Bez uszczerbku dla odpowiednich obowiązków przypadających Komisji i państwom członkowskim na mocy unijnych aktów prawnych regulujących wielkoskalowe systemy informatyczne, Agencja zapewnia:

a) rozwój wielkoskalowych systemów informatycznych z wykorzystaniem odpowiedniej struktury zarządzania projektami do skutecznego rozwijania takich systemów;

b) skuteczne, bezpieczne i nieprzerwane działanie wielkoskalowych systemów informatycznych;

c) efektywne i rozliczalne zarządzanie wielkoskalowymi systemami informatycznymi;

d) odpowiednio wysokiej jakości usługi oferowane użytkownikom wielkoskalowych systemów informatycznych;

e) ciągłość i nieprzerwane funkcjonowanie;

f) wysoki poziom ochrony danych zgodnie z unijnymi przepisami o ochronie danych, w tym przepisami szczególnymi odnoszącymi się do każdego z wielkoskalowych systemów informatycznych;

g) odpowiedni poziom bezpieczeństwa danych i bezpieczeństwa fizycznego, zgodnie z mającymi zastosowanie przepisami, w tym przepisami szczegółowymi odnoszącymi się do każdego z wielkoskalowych systemów informatycznych.

ROZDZIAŁ II

ZADANIA AGENCJI

Artykuł 3

Zadania w zakresie systemu SIS II

W odniesieniu do systemu SIS II Agencja wykonuje:

a) zadania powierzone organowi zarządzającemu w rozporządzeniu (WE) nr 1987/2006 i decyzji 2007/533/WSiSW; oraz

b) zadania związane ze szkoleniami w zakresie technicznego użytkowania systemu SIS II – zwłaszcza dla personelu SIRENE (SIRENE – wniosek o informacje uzupełniające wpisy krajowe) oraz ze szkoleniami dla ekspertów dotyczącymi technicznych aspektów systemu SIS II w ramach oceny Schengen.

Artykuł 4

Zadania związane z systemem VIS

W odniesieniu do systemu VIS Agencja wykonuje:

a) zadania powierzone organowi zarządzającemu na mocy rozporządzenia (WE) nr 767/2008 i decyzji 2008/633/WSiSW; oraz

b) zadania związane ze szkoleniami w zakresie technicznego użytkowania systemu VIS oraz szkoleniami dla ekspertów dotyczącymi technicznych aspektów systemu VIS w ramach oceny Schengen.

Artykuł 5

Zadania związane z systemem Eurodac

W odniesieniu do systemu Eurodac Agencja wykonuje:

a) zadania powierzone jej w rozporządzeniu (UE) nr 603/2013; oraz

b) zadania związane ze szkoleniami w zakresie technicznego użytkowania systemu Eurodac.

Artykuł 6

Zadania związane z systemem EES

W odniesieniu do systemu EES Agencja wykonuje:

a) zadania powierzone jej w rozporządzeniu (UE) 2017/2226; oraz

b) zadania związane ze szkoleniami w zakresie technicznego użytkowania systemu EES oraz szkoleniami dla ekspertów dotyczącymi technicznych aspektów tego systemu w ramach oceny Schengen.

Artykuł 7

Zadania związane z systemem ETIAS

W odniesieniu do systemu ETIAS Agencja wykonuje:

a) zadania powierzone jej w rozporządzeniu (UE) 2018/1240; oraz

b) zadania związane ze szkoleniami w zakresie technicznego użytkowania systemu ETIAS oraz szkoleniami dla ekspertów dotyczącymi technicznych aspektów systemu ETIAS w ramach oceny Schengen.

Artykuł 8

Zadania związane z systemem DubliNet

W odniesieniu do systemu DubliNet Agencja wykonuje:

a) zadania związane z zarządzaniem operacyjnym systemem DubliNet, osobnym bezpiecznym kanałem transmisji elektronicznej między organami państw członkowskich, ustanowionym na mocy art. 18 rozporządzenia (WE) nr 1560/2003 do celów art. 31, 32 i 34 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 604/2013 ([1]); oraz

([1]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 604/2013 z dnia 26 czerwca 2013 r. w sprawie ustanowienia kryteriów i mechanizmów ustalania państwa członkowskiego odpowiedzialnego za rozpatrzenie wniosku o udzielenie ochrony międzynarodowej złożonego w jednym z państw członkowskich przez obywatela państwa trzeciego lub bezpaństwowca (Dz.U. L 180 z 29.6.2013, s. 31).

b) zadania związane ze szkoleniami w zakresie technicznego użytkowania systemu DubliNet.

Artykuł 9

Zadania związane z przygotowywaniem i rozwijaniem innych wielkoskalowych systemów informatycznych oraz zarządzaniem operacyjnym tymi systemami

W przypadku powierzenia Agencji przygotowania i rozwijania innych wielkoskalowych systemów informatycznych, o których mowa w art. 1 ust. 5, a także zarządzania operacyjnego tymi systemami, Agencja wykonuje, w stosownych przypadkach, zadania związane ze szkoleniami w zakresie technicznego użytkowania tych systemów powierzone jej zgodnie z unijnym aktem prawnym regulującym dany system.

Artykuł 10

Rozwiązania techniczne wymagające szczególnych warunków przed wdrożeniem

W przypadku gdy unijne akty prawne regulujące systemy wymagają, by Agencja zapewniała działanie tych systemów w trybie całodobowym, 7 dni w tygodniu i bez uszczerbku dla tych unijnych aktów prawnych, Agencja wdraża rozwiązania techniczne, by spełnić te wymogi. W przypadku gdy te rozwiązania techniczne wymagają powielenia systemu lub powielenia elementów systemu, są one wdrażane dopiero po przeprowadzeniu niezależnej oceny skutków oraz analizy kosztów i korzyści zleconej przez Agencję, po zasięgnięciu opinii Komisji i po pozytywnej decyzji zarządu. Podczas oceny skutków analizuje się także obecne i przyszłe potrzeby istniejących centrów technicznych pod kątem potencjału hostingowego związane z rozwijaniem takich rozwiązań technicznych, a także ewentualne zagrożenia związane z aktualną konfiguracją operacyjną.

Artykuł 11

Zadania związane z infrastrukturą łączności

1. Agencja wykonuje zadania związane z infrastrukturą łączności systemów, które zostały jej powierzone w oparciu o unijne akty prawne regulujące systemy, z wyjątkiem tych systemów, które wykorzystują w ramach swojej infrastruktury łączności EuroDomain. W przypadku tych systemów, które wykorzystują w taki sposób EuroDomain, Komisja odpowiada za zadania związane z wdrożeniem budżetu, nabywaniem, odnawianiem oraz kwestiami dotyczącymi umów. Zgodnie z unijnymi aktami prawnymi regulującymi systemy wykorzystujące EuroDomain zadania dotyczące infrastruktury łączności, w tym zarządzania operacyjnego i bezpieczeństwa, są podzielone między Agencję a Komisję. W celu zapewnienia spójności pomiędzy wykonywanymi przez siebie odpowiednimi zadaniami Agencja i Komisja dokonują operacyjnych ustaleń roboczych, które zostają ujęte w protokole ustaleń.

2. W celu ochrony infrastruktury łączności przed zagrożeniami oraz zapewnienia bezpieczeństwa tej infrastruktury i systemów, w tym również bezpieczeństwa danych wymienianych przy użyciu infrastruktury łączności, jest ona odpowiednio zarządzana i podlega kontroli.

3. Agencja przyjmuje odpowiednie środki, w tym plany bezpieczeństwa, między innymi w celu zapobiegania nieupoważnionemu odczytywaniu, kopiowaniu, modyfikowaniu lub usuwaniu danych osobowych w czasie przekazywania danych osobowych lub transportu nośników danych, w szczególności poprzez zastosowanie odpowiednich technik szyfrowania. Wszelkie informacje operacyjne związane z systemem przekazywane przy użyciu infrastruktury łączności są szyfrowane.

4. Zadania związane z dostarczaniem, tworzeniem, utrzymywaniem i monitorowaniem infrastruktury łączności można powierzyć podmiotom zewnętrznym lub instytucjom z sektora prywatnego zgodnie z rozporządzeniem (UE, Euratom) 2018/1046. Zadania takie są przeprowadzane w ramach obowiązków Agencji i pod jej ścisłym nadzorem.

Przy realizacji zadań, o których mowa w akapicie pierwszym, wszystkie podmioty zewnętrzne lub instytucje z sektora prywatnego, w tym dostawcy sieci, są zobowiązane do stosowania środków bezpieczeństwa, o których mowa w ust. 3, i nie mają w żaden sposób dostępu do jakichkolwiek danych operacyjnych przechowywanych w systemach ani przesyłanych za pośrednictwem infrastruktury łączności czy na potrzeby wymiany wniosków SIRENE związanej z systemem SIS II.

5. Zarządzanie kluczami do szyfrowania pozostaje w gestii Agencji i nie może zostać przekazane żadnemu zewnętrznemu podmiotowi z sektora prywatnego. Powyższe pozostaje bez uszczerbku dla obowiązujących umów w sprawie infrastruktury łączności systemów SIS II, VIS i Eurodac.

Artykuł 12

Jakość danych

Niezależnie od odpowiedzialności państw członkowskich za dane wprowadzone do systemów, Agencja współpracuje z Komisją, angażując przy tym ściśle swoje grupy doradcze, w celu ustanowienia zautomatyzowanych mechanizmów kontroli jakości danych oraz wspólnych wskaźników jakości danych dla wszystkich systemów zarządzanych operacyjnie przez Agencję, a także opracowania centralnego repozytorium zawierającego wyłącznie zanonimizowane dane do celów sprawozdawczo-statystycznych, z zastrzeżeniem szczególnych przepisów w unijnych aktach prawnych regulujących rozwijanie, tworzenie, funkcjonowanie i użytkowanie systemów.

Artykuł 13

Interoperacyjność

Jeżeli interoperacyjność wielkoskalowych systemów informatycznych została przewidziana w odnośnym unijnym akcie prawnym, zadaniem Agencji jest prowadzenie działań niezbędnych do jej zapewnienia.

Artykuł 14

Monitorowanie prac badawczych

1. Agencja monitoruje rozwój prac badawczych istotnych dla zarządzania operacyjnego systemami SIS II, VIS, Eurodac, EES, ETIAS, DubliNet oraz innymi wielkoskalowymi systemami, o których mowa w art. 1 ust. 5.

2. Agencja może wnosić własny wkład we wdrażanie elementów programu ramowego Unii Europejskiej w zakresie badań naukowych i innowacji, które są związane z wielkoskalowymi systemami informatycznymi w przestrzeni wolności, bezpieczeństwa i sprawiedliwości. W tym celu, o ile Komisja przekazała Agencji odpowiednie uprawnienia, Agencja wykonuje następujące zadania:

a) zarządzanie niektórymi etapami wdrażania programu i niektórymi fazami w trakcie konkretnych projektów na podstawie właściwych programów prac przyjętych przez Komisję;

b) przyjmowanie wykonawczych aktów budżetowych w zakresie dochodów i wydatków oraz przeprowadzanie wszystkich operacji niezbędnych do zarządzania programem;

c) zapewnianie wsparcia we wdrażaniu programu.

3. Agencja regularnie i co najmniej raz w roku informuje Parlament Europejski, Radę, Komisję, a w przypadku, gdy dotyczy to przetwarzania danych osobowych, również Europejskiego Inspektora Ochrony Danych, o rozwoju prac badawczych, o których mowa w niniejszym artykule, niezależnie od wymogów sprawozdawczych w odniesieniu do wykonania elementów programu ramowego Unii Europejskiej w zakresie badań naukowych i innowacji, o którym mowa w ust. 2.

Artykuł 15

Projekty pilotażowe, weryfikacja poprawności projektu oraz testowanie

1. Na konkretny i precyzyjny wniosek Komisji – która z co najmniej trzymiesięcznym wyprzedzeniem informuje Parlament Europejski i Radę o złożeniu takiego wniosku – oraz po podjęciu pozytywnej decyzji przez zarząd, Agencji może zostać powierzone, zgodnie z art. 19 ust. 1 lit. u) niniejszego rozporządzenia oraz w drodze umowy o delegowaniu zadań, prowadzenie projektów pilotażowych, o których mowa w art. 58 ust. 2 lit. a) rozporządzenia (UE, Euratom) 2018/1046, w zakresie rozwijania wielkoskalowych systemów informatycznych lub zarządzania operacyjnego tymi systemami na podstawie art. 67–89 TFUE, zgodnie z art. 62 ust. 1 lit. c) rozporządzenia (UE, Euratom) 2018/1046.

Agencja regularnie informuje Parlament Europejski, Radę, a w przypadku gdy dotyczy to kwestii przetwarzania danych osobowych również Europejskiego Inspektora Ochrony Danych, o rozwoju projektów pilotażowych prowadzonych przez Agencję na podstawie akapitu pierwszego.

2. Środki finansowe na projekty pilotażowe, o których mowa w art. 58 ust. 2 lit. a) rozporządzenia (UE, Euratom) 2018/1046, będące przedmiotem wniosku Komisji na podstawie ust. 1 są ujmowane w budżecie na nie więcej niż dwa kolejne lata budżetowe.

3. Na wniosek Komisji lub Rady, po poinformowaniu Parlamentu Europejskiego, oraz po podjęciu pozytywnej decyzji przez zarząd, Agencji mogą dodatkowo zostać powierzone, w drodze umowy o delegowaniu zadań, zadania związane z wykonywaniem budżetu celem weryfikacji poprawności projektów finansowanych w ramach instrumentu na rzecz wsparcia finansowego w zakresie granic zewnętrznych i wiz ustanowionego w rozporządzeniu (UE) nr 515/2014, zgodnie z art. 62 ust. 1 lit. c) rozporządzenia (UE, Euratom) 2018/1046.

4. Na podstawie pozytywnej decyzji zarządu Agencja może również planować i realizować testy w sprawach objętych niniejszym rozporządzeniem oraz wszelkimi unijnymi aktami prawnymi regulującymi rozwijanie, tworzenie, funkcjonowanie i użytkowanie systemów.

Artykuł 16

Udzielanie wsparcia państwom członkowskim i Komisji

1. Każde państwo członkowskie może zwrócić się do Agencji o doradztwo w zakresie połączenia swoich systemów krajowych z systemami centralnymi wielkoskalowych systemów informatycznych zarządzanych przez Agencję.

2. Każde państwo członkowskie może wystąpić z wnioskiem o doraźne wsparcie do Komisji, która, o ile oceni, że takie wsparcie jest wymagane z powodów nadzwyczajnych związanych z bezpieczeństwem lub migracją, przekazuje wniosek niezwłocznie Agencji. Agencja informuje zarząd o takich wnioskach. Jeżeli ocena Komisji jest negatywna, państwo członkowskie jest o tym informowane.

Komisja kontroluje, czy Agencja zareagowała we właściwym czasie na wniosek państwa członkowskiego. Roczne sprawozdanie Agencji z działalności zawiera szczegółowe informacje o działaniach podjętych przez Agencję w celu udzielenia państwom członkowskim doraźnego wsparcia oraz o poniesionych w związku z tym kosztach.

3. Do Agencji może również zostać wystosowany wniosek o udzielenie Komisji porady lub wsparcia w kwestiach technicznych związanych z istniejącymi lub nowymi systemami, w tym w drodze przeprowadzenia badań i testów. Agencja informuje zarząd o takich wnioskach.

4. Grupa co najmniej pięciu państw członkowskich może powierzyć Agencji zadanie opracowania wspólnego elementu informatycznego, zarządzania nim lub hostingu takiego elementu, aby pomóc im we wdrażaniu technicznych aspektów obowiązków wynikających z prawa unijnego w zakresie zdecentralizowanych systemów w przestrzeni wolności, bezpieczeństwa i sprawiedliwości. Te wspólne rozwiązania informatyczne nie naruszają obowiązków państw członkowskich występujących z wnioskiem, które wynikają z mającego zastosowanie prawa unijnego, zwłaszcza w odniesieniu do struktury tych systemów.

W szczególności państwa członkowskie występujące z wnioskiem mogą powierzyć Agencji zadanie stworzenia wspólnego elementu lub routera do celów danych pasażera przekazywanych przed podróżą i danych o przelocie pasażera jako narzędzia wsparcia technicznego umożliwiającego zapewnienie łączności z przewoźnikami lotniczymi, aby pomóc państwom członkowskim we wdrażaniu dyrektywy Rady 2004/82/WE ([1]) i dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/681 ([2]). W takim przypadku Agencja gromadzi w sposób scentralizowany dane od przewoźników lotniczych i przekazuje je państwom członkowskim za pośrednictwem wspólnego elementu lub routera. Państwa członkowskie występujące z wnioskiem przyjmują środki niezbędne do zapewnienia, by przewoźnicy lotniczy przekazywali dane za pośrednictwem Agencji.

Agencji powierza się zadanie opracowania wspólnego elementu informatycznego, zarządzania nim lub jego hostingu jedynie po wcześniejszym zatwierdzeniu przez Komisję oraz po podjęciu pozytywnej decyzji przez zarząd.

Państwa członkowskie występujące z wnioskiem powierzają Agencji zadania, o których mowa w akapitach pierwszym i drugim, w drodze umowy o delegowaniu zadań określającej warunki delegowania zadań oraz sposoby wyliczania wszystkich powiązanych kosztów i metodę fakturowania. Wszystkie odnośne koszty pokrywają uczestniczące państwa członkowskie. Umowa o delegowaniu zadań musi być zgodna z unijnymi aktami prawnymi regulującymi dane systemy. Agencja informuje Parlament Europejski i Radę o zatwierdzonej umowie o delegowaniu zadań oraz o jej wszelkich modyfikacjach.

Inne państwa członkowskie mogą wystąpić o uczestniczenie we wspólnym rozwiązaniu informatycznym, jeśli taką możliwość przewiduje umowa o delegowaniu zadań określająca w szczególności finansowe skutki takiego uczestnictwa. Po wcześniejszym zatwierdzeniu przez Komisję i po podjęciu pozytywnej decyzji przez zarząd umowa o delegowaniu zadań zostaje odpowiednio zmieniona.

ROZDZIAŁ III

STRUKTURA I ORGANIZACJA

Artykuł 17

Status prawny i siedziba

1. Agencja jest organem Unii i ma osobowość prawną.

([1]) Dyrektywa Rady 2004/82/WE z dnia 29 kwietnia 2004 r. w sprawie zobowiązania przewoźników do przekazywania danych pasażerów (Dz.U. L 261 z 6.8.2004, s. 24).

([2]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/681 z dnia 27 kwietnia 2016 r. w sprawie wykorzystywania danych dotyczących przelotu pasażera (danych PNR) w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania (Dz.U. L 119 z 4.5.2016, s. 132).

2. Agencja posiada zdolność prawną i zdolność do czynności prawnych o najszerszym zakresie przyznanym przez prawo krajowe osobom prawnym w każdym państwie członkowskim. Może ona zwłaszcza nabywać i zbywać mienie ruchome i nieruchome oraz występować w charakterze strony w postępowaniach sądowych.

3. Siedzibą Agencji jest Tallin (Estonia).

Zadania związane z rozwojem i zarządzaniem operacyjnym, o których mowa w art. 1 ust. 4 i 5 oraz w art. 3, 4, 5, 6, 7, 8, 9 i 11 są wykonywane w centrum technicznym w Strasburgu we Francji.

Obiekt zapasowy, który umożliwia zapewnienie działania wielkoskalowego systemu informatycznego w przypadku awarii takiego systemu, jest zlokalizowany w Sankt Johann im Pongau w Austrii.

4. Oba centra techniczne mogą być użyte do celów jednoczesnej obsługi systemów, pod warunkiem że w przypadku awarii jednego lub większej liczby systemów obiekt zapasowy jest w stanie zapewnić ich obsługę.

5. Z uwagi na szczególny charakter systemów, jeżeli okazałoby się, że Agencja musi stworzyć drugie odrębne centrum techniczne w Strasburgu albo w Sankt Johann im Pongau albo, w razie potrzeby, w obu tych miejscach w celu zapewnienia hostingu systemów, konieczność taką należy uzasadnić w oparciu o niezależną ocenę skutków oraz analizę kosztów i korzyści. Zgodnie z art. 45 ust. 9 przed powiadomieniem władzy budżetowej o zamiarze zrealizowania jakiegokolwiek projektu związanego z nieruchomością zarząd konsultuje się z Komisją i uwzględnia jej opinię.

Artykuł 18

Struktura

1. Strukturę administracyjną i zarządczą Agencji tworzą:

a) zarząd;

b) dyrektor wykonawczy;

c) grupy doradcze.

2. Struktura Agencji obejmuje:

a) inspektora ochrony danych;

b) pracownika ds. bezpieczeństwa;

c) księgowego.

Artykuł 19

Funkcje zarządu

1. Zarząd:

a) wyznacza ogólne kierunki działań Agencji;

b) przyjmuje, większością dwóch trzecich głosów członków uprawnionych do głosowania, roczny budżet Agencji oraz pełni inne funkcje związane z budżetem Agencji na podstawie rozdziału V;

c) powołuje dyrektora wykonawczego i jego zastępcę oraz, w stosownych przypadkach, podejmuje decyzje odpowiednio o przedłużeniu ich mandatu lub usunięciu ich ze stanowiska zgodnie z art. 25 i 26;

d) sprawuje władzę dyscyplinarną nad dyrektorem wykonawczym i nadzoruje jego pracę, w tym wykonywanie decyzji zarządu, oraz sprawuje władzę dyscyplinarną nad zastępcą dyrektora wykonawczego w porozumieniu z dyrektorem wykonawczym;

e) podejmuje wszystkie decyzje dotyczące ustanowienia struktury organizacyjnej Agencji, a w razie potrzeby – jej modyfikacji, biorąc pod uwagę potrzeby w zakresie działań Agencji oraz mając na uwadze należyte zarządzanie budżetem;

f) przyjmuje politykę kadrową Agencji;

g) opracowuje regulamin wewnętrzny Agencji;

h) przyjmuje strategię zwalczania nadużyć finansowych, proporcjonalną do ryzyka nadużyć finansowych, uwzględniając koszty i korzyści środków planowanych do wdrożenia;

i) przyjmuje przepisy, których celem jest zapobieganie konfliktom interesów i zarządzanie nimi w odniesieniu do swoich członków, oraz publikuje je na stronie internetowej Agencji;

j) przyjmuje szczegółowe przepisy i procedury wewnętrzne w celu ochrony sygnalistów, w tym określa odpowiednie kanały komunikacji na potrzeby zgłaszania nieprawidłowości;

k) wydaje zgodę na zawieranie porozumień roboczych zgodnie z art. 41 i 43;

l) zatwierdza, na podstawie wniosku dyrektora wykonawczego, umowę w sprawie siedziby Agencji oraz umowy dotyczące centrum technicznego obiektu zapasowego, utworzonych zgodnie z art. 17 ust. 3, które to umowy podpisuje dyrektor wykonawczy z przyjmującymi państwami członkowskimi;

m) wykonuje w odniesieniu do pracowników Agencji, zgodnie z ust. 2, uprawnienia powierzone organowi powołującemu na mocy regulaminu pracowniczego urzędników oraz uprawnienia powierzone organowi uprawnionemu do zawierania umów o pracę na mocy warunków zatrudnienia innych pracowników („uprawnienia organu powołującego");

n) przyjmuje, w porozumieniu z Komisją, niezbędne przepisy wykonawcze w celu nadania skuteczności regulaminowi pracowniczemu zgodnie z art. 110 regulaminu pracowniczego urzędników;

o) przyjmuje niezbędne zasady dotyczące delegowania ekspertów krajowych do Agencji;

p) przyjmuje wstępny projekt preliminarza dochodów i wydatków Agencji, w tym projekt planu zatrudnienia, i przekazuje go Komisji do dnia 31 stycznia każdego roku;

q) przyjmuje projekt jednolitego dokumentu programowego zawierającego programowanie wieloletnie Agencji i jej program prac na następny rok oraz wstępny projekt preliminarza dochodów i wydatków Agencji, w tym projekt planu zatrudnienia, i do dnia 31 stycznia każdego roku przekazuje go, jak również wszelkie zaktualizowane wersje tego dokumentu, Parlamentowi Europejskiemu, Radzie i Komisji;

r) przyjmuje, przed dniem 30 listopada każdego roku, większością dwóch trzecich głosów członków z prawem głosu, zgodnie z roczną procedurą budżetową, jednolity dokument programowy uwzględniający opinię Komisji oraz zapewnia, że Parlamentowi Europejskiemu, Radzie i Komisji zostanie przekazana ostateczna wersja jednolitego dokumentu programowego, a także że taka wersja zostanie opublikowana;

s) przyjmuje, przed końcem sierpnia każdego roku, wstępne sprawozdanie z postępów we wdrażaniu działań zaplanowanych na rok bieżący oraz przekazuje je Parlamentowi Europejskiemu, Radzie i Komisji;

t) ocenia i przyjmuje skonsolidowane roczne sprawozdanie z działalności Agencji za poprzedni rok, w którym porównuje się w szczególności osiągnięte wyniki z celami wyznaczonymi w rocznym programie prac, i do dnia 1 lipca każdego roku wysyła sprawozdanie oraz jego ocenę Parlamentowi Europejskiemu, Radzie, Komisji i Trybunałowi Obrachunkowemu oraz zapewnia, aby roczne sprawozdanie z działalności zostało opublikowane;

u) realizuje swoje zadania związane z budżetem Agencji, w tym wdrażanie projektów pilotażowych oraz weryfikację poprawności projektów, o których mowa w art. 15;

v) przyjmuje przepisy finansowe mające zastosowanie do Agencji, zgodnie z art. 49;

w) powołuje księgowego, którym może być księgowy Komisji, zgodnie z regulaminem pracowniczym, który jest całkowicie niezależny w wykonywaniu swoich obowiązków;

x) zapewnia odpowiednie działania następcze w odniesieniu do ustaleń i zaleceń wynikających ze sprawozdań z różnych audytów wewnętrznych lub zewnętrznych oraz ocen, jak również uzyskanych w rezultacie dochodzeń przeprowadzonych przez Europejski Urząd ds. Zwalczania Nadużyć Finansowych (OLAF) oraz Prokuraturę Europejską (EPPO);

y) przyjmuje plany komunikacji i rozpowszechniania informacji, o których mowa w art. 34 ust. 4 oraz regularnie je aktualizuje;

z) przyjmuje niezbędne środki bezpieczeństwa, w tym plan bezpieczeństwa oraz plan ciągłości działania i plan przywrócenia gotowości do pracy po wystąpieniu sytuacji nadzwyczajnej, z uwzględnieniem ewentualnych zaleceń ekspertów ds. bezpieczeństwa wchodzących w skład grup doradczych;

aa) po zatwierdzeniu przez Komisję przyjmuje zasady bezpieczeństwa dotyczące ochrony informacji niejawnych oraz szczególnie chronionych informacji jawnych;

bb) wyznacza pracownika ds. bezpieczeństwa;

cc) wyznacza inspektora ochrony danych zgodnie z rozporządzeniem (UE) 2018/1725;

dd) przyjmuje szczegółowe zasady dotyczące wykonania rozporządzenia (WE) nr 1049/2001;

ee) przyjmuje sprawozdania dotyczące rozwoju systemu EES zgodnie z art. 72 ust. 2 rozporządzenia (UE) 2017/2226 oraz przyjmuje sprawozdania dotyczące rozwoju systemu ETIAS zgodnie z art. 92 ust. 2 rozporządzenia (UE) 2018/1240;

ff) przyjmuje sprawozdania na temat technicznych aspektów funkcjonowania systemu SIS II zgodnie z, odpowiednio, art. 50 ust. 4 rozporządzenia (WE) nr 1987/2006 oraz art. 66 ust. 4 decyzji 2007/533/WSiSW, systemu VIS zgodnie z art. 50 ust. 3 rozporządzenia (WE) 767/2008 i art. 17 ust. 3 decyzji 2008/633/WSiSW, jak i systemu EES zgodnie z art. 72 ust. 4 rozporządzenia (UE) 2017/2226 oraz systemu ETIAS zgodnie z art. 92 ust. 4 rozporządzenia (UE) 2018/1240;

gg) przyjmuje roczne sprawozdanie z działania centralnego systemu Eurodac zgodnie z art. 40 ust. 1 rozporządzenia (UE) nr 603/2013;

hh) przyjmuje oficjalne uwagi do sprawozdań Europejskiego Inspektora Ochrony Danych z przeprowadzanych audytów, na podstawie art. 45 ust. 2 rozporządzenia (WE) nr 1987/2006, art. 42 ust. 2 rozporządzenia (WE) nr 767/2008 i art. 31 ust. 2 rozporządzenia (UE) nr 603/2013, art. 56 ust. 2 rozporządzenia (UE) 2017/2226 i art. 67 rozporządzenia (UE) 2018/1240, a także zapewnia odpowiednie działania następcze w sprawie tych audytów;

ii) publikuje statystyki dotyczące systemu SIS II zgodnie z, odpowiednio, art. 50 ust. 3 rozporządzenia (WE) nr 1987/2006 i art. 66 ust. 3 decyzji 2007/533/WSiSW;

jj) przygotowuje oraz publikuje statystyki na temat funkcjonowania centralnego systemu Eurodac zgodnie z art. 8 ust. 2 rozporządzenia (UE) nr 603/2013;

kk) publikuje statystyki dotyczące systemu EES zgodnie z art. 63 rozporządzenia (UE) 2017/2226;

ll) publikuje statystyki dotyczące systemu ETIAS zgodnie z art. 84 rozporządzenia (UE) 2018/1240;

mm) zapewnia – zgodnie z art. 31 ust. 8 rozporządzenia (WE) nr 1987/2006 i art. 46 ust. 8 decyzji 2007/533/WSiSW – coroczną publikację wykazu właściwych organów upoważnionych do bezpośredniego wyszukiwania danych znajdujących się w systemie SIS II, o którym mowa w art. 31 ust. 8 rozporządzenia (WE) nr 1987/2006 i art. 46 ust. 8 decyzji 2007/533/WSiSW, wraz z wykazem urzędów krajowych systemów SIS II (urzędy N.SIS II) oraz biur SIRENE, zgodnie z art. 7 ust. 3 rozporządzenia (WE) nr 1987/2006 i art. 7 ust. 3 decyzji 2007/533/WSiSW, oraz wykazu właściwych organów zgodnie z art. 65 ust. 2 rozporządzenia (UE) 2017/2226, jak również wykazu właściwych organów zgodnie z art. 87 ust. 2 rozporządzenia (UE) 2018/1240;

nn) zapewnia coroczną publikację wykazu jednostek, zgodnie z art. 27 ust. 2 rozporządzenia (UE) nr 603/2013;

oo) zapewnia zgodność wszelkich decyzji i działań Agencji mających wpływ na wielkoskalowe systemy informatyczne w przestrzeni wolności, bezpieczeństwa i sprawiedliwości z zasadą niezawisłości sądownictwa;

pp) wykonuje wszelkie inne zadania powierzone mu zgodnie z niniejszym rozporządzeniem.

Bez uszczerbku dla przepisów dotyczących publikowania wykazów właściwych organów przewidzianych w unijnych aktach prawnych, o których mowa w lit. mm) akapitu pierwszego, oraz jeżeli w tych aktach prawnych nie przewiduje się obowiązku publikowania i stałego aktualizowania tych wykazów na stronie internetowej Agencji, zarząd odpowiada za zapewnienie tej publikacji i stałej aktualizacji.

2. Zgodnie z procedurą przewidzianą w art. 110 regulaminu pracowniczego urzędników, na podstawie art. 2 ust. 1 regulaminu pracowniczego urzędników i art. 6 warunków zatrudnienia innych pracowników zarząd przyjmuje decyzję przekazującą odpowiednie uprawnienia organu powołującego dyrektorowi wykonawczemu i określającą warunki, zgodnie z którymi możliwe jest zawieszenie przekazania tych uprawnień. Dyrektor wykonawczy jest uprawniony do dalszego przekazania tych uprawnień.

Jeżeli wymagają tego szczególne okoliczności, zarząd może w drodze decyzji tymczasowo zawiesić przekazanie uprawnień organu powołującego dyrektorowi wykonawczemu i uprawnienia dalej przez niego przekazane i wykonywać je samodzielnie lub przekazać je jednemu ze swoich członków lub też członkowi personelu innemu niż dyrektor wykonawczy.

3. Zarząd może doradzać dyrektorowi wykonawczemu w każdej sprawie ściśle związanej z rozwijaniem wielkoskalowych systemów informatycznych lub zarządzaniem operacyjnym tymi systemami oraz w kwestii działań związanych z badaniami, projektami pilotażowymi, weryfikacją poprawności projektu oraz testowaniem.

Artykuł 20

Skład zarządu

1. W skład zarządu wchodzi po jednym przedstawicielu każdego państwa członkowskiego oraz dwóch przedstawicieli Komisji. Każdy przedstawiciel posiada prawo głosu zgodnie z art. 23.

2. Każdy członek Zarządu ma zastępcę. Zastępca reprezentuje członka zarządu pod jego nieobecność lub w przypadku, gdy członek zostaje wybrany na przewodniczącego lub zastępcę przewodniczącego zarządu i przewodniczy posiedzeniu zarządu. Członkowie zarządu i ich zastępcy są powoływani w oparciu o wysoki poziom stosownego doświadczenia i fachowej wiedzy w dziedzinie wielkoskalowych systemów informatycznych w przestrzeni wolności, bezpieczeństwa i sprawiedliwości oraz ich wiedzy w odniesieniu do ochrony danych, z uwzględnieniem ich odpowiednich umiejętności zarządczych, administracyjnych i budżetowych. Wszystkie strony reprezentowane w zarządzie dokładają starań w celu ograniczenia rotacji swych przedstawicieli, aby zapewnić ciągłość prac zarządu. Wszystkie strony dążą do osiągnięcia równowagi pod względem liczby mężczyzn i kobiet w składzie zarządu.

3. Kadencja członków oraz ich zastępców trwa cztery lata, z możliwością przedłużenia. Po upływie ich kadencji lub w przypadku rezygnacji członkowie pełnią swoją funkcję do czasu ich ponownego powołania lub zastąpienia przez nowych członków.

4. W działaniach Agencji biorą udział państwa uczestniczące we wdrażaniu, stosowaniu i rozwijaniu dorobku Schengen oraz środków dotyczących rozporządzeń dublińskich i systemu Eurodac. Każde z tych państw powołuje do zarządu jednego przedstawiciela i jego zastępcę.

Artykuł 21

Przewodniczący zarządu

1. Zarząd wybiera przewodniczącego i zastępcę przewodniczącego spośród członków zarządu powołanych przez państwa członkowskie, które są w pełni związane na mocy prawa Unii wszystkimi unijnymi aktami prawnymi regulującymi rozwijanie, ustanawianie, funkcjonowanie i użytkowanie wszystkich zarządzanych przez Agencję wielkoskalowych systemów informatycznych. Przewodniczący i zastępca przewodniczącego wybierani są większością dwóch trzecich głosów członków zarządu z prawem głosu.

Zastępca przewodniczącego zastępuje z urzędu przewodniczącego w przypadku, gdy nie jest on w stanie wykonywać swoich obowiązków.

2. Kadencja przewodniczącego i zastępcy przewodniczącego trwa cztery lata. Ich kadencje mogą zostać jednokrotnie odnowione. Jeżeli w dowolnym momencie swojej kadencji stracą oni status członka zarządu, ich kadencja kończy się automatycznie w tym samym dniu.

Artykuł 22

Posiedzenia zarządu

1. Posiedzenia zarządu zwołuje przewodniczący.

2. Dyrektor wykonawczy bierze udział w obradach bez prawa głosu.

3. Zarząd zbiera się co najmniej dwa razy do roku na posiedzeniach zwyczajnych. Dodatkowo zarząd zbiera się z inicjatywy przewodniczącego, na wniosek Komisji, dyrektora wykonawczego lub co najmniej jednej trzeciej swoich członków zarządu z prawem głosu.

4. Europol i Eurojust mogą uczestniczyć w posiedzeniach zarządu jako obserwatorzy, gdy porządek obrad obejmuje kwestię dotyczącą systemu SIS II, w związku ze stosowaniem decyzji 2007/533/WSiSW. Europejska Agencja Straży Granicznej i Przybrzeżnej może uczestniczyć w posiedzeniach zarządu jako obserwator, gdy porządek obrad obejmuje kwestię dotyczącą systemu SIS II, z związku ze stosowaniem rozporządzenia (UE) 2016/1624.

Europol może uczestniczyć w posiedzeniach zarządu jako obserwator, gdy porządek obrad obejmuje kwestię dotyczącą systemu VIS, w związku ze stosowaniem decyzji 2008/633/WSiSW, lub kwestię dotyczącą systemu Eurodac, w związku ze stosowaniem rozporządzenia (UE) nr 603/2013.

Europol może uczestniczyć w posiedzeniach zarządu jako obserwator, gdy porządek obrad obejmuje kwestię dotyczącą systemu EES, w związku ze stosowaniem rozporządzenia (UE) 2017/2226, lub kwestię dotyczącą systemu ETIAS, w związku ze stosowaniem rozporządzenia (UE) 2018/1240. Europejska Agencja Straży Granicznej i Przybrzeżnej może również uczestniczyć w posiedzeniach zarządu jako obserwator, gdy porządek obrad obejmuje kwestię dotyczącą systemu ETIAS z związku ze stosowaniem rozporządzenia (UE) 2018/1240.

Zarząd może zaprosić na swoje posiedzenie w charakterze obserwatora każdą inną osobę, której opinia może mieć znaczenie.

5. Z zastrzeżeniem postanowień regulaminu wewnętrznego zarządu, członków zarządu i ich zastępców mogą wspierać doradcy lub eksperci, w szczególności ci, którzy wchodzą w skład grup doradczych.

6. Agencja zapewnia zarządowi obsługę sekretariatu.

Artykuł 23

Zasady głosowania zarządu

1. Bez uszczerbku dla ust. 5 niniejszego artykułu oraz art. 19 ust. 1 lit. b) i r), art. 21 ust. 1 i art. 25 ust. 8, zarząd podejmuje decyzje większością głosów swoich członków z prawem głosu.

2. Bez uszczerbku dla ust. 3 i 4, każdemu członkowi zarządu przysługuje jeden głos. W przypadku nieobecności członka z prawem głosu jego zastępca jest uprawniony do wykonywania jego prawa głosu.

3. Każdy z członków wyznaczonych przez państwo członkowskie, które jest związane na mocy prawa Unii unijnym aktem prawnym regulującym rozwijanie, ustanawianie, funkcjonowanie i użytkowanie zarządzanego przez Agencję wielkoskalowego systemu informatycznego, może głosować w sprawie kwestii dotyczących tego wielkoskalowego systemu informatycznego.

Dania może głosować w sprawie kwestii dotyczących wielkoskalowego systemu informatycznego, jeżeli podejmie decyzję – na mocy art. 4 Protokołu nr 22 w sprawie stanowiska Danii – o wprowadzeniu do swojego prawa krajowego unijnego aktu prawnego regulującego rozwijanie, ustanawianie, funkcjonowanie i użytkowanie tego konkretnego wielkoskalowego systemu informatycznego.

4. Artykuł 42 ma zastosowanie w odniesieniu do praw do głosowania przedstawicieli państw, które zawarły z Unią umowy dotyczące włączenia ich we wprowadzanie w życie, stosowanie i rozwój dorobku Schengen oraz środków dotyczących rozporządzeń dublińskich i systemu Eurodac.

5. W przypadku braku zgody między członkami co do tego, czy dane głosowanie dotyczy konkretnego wielkoskalowego systemu informatycznego, każda decyzja stwierdzająca, że głosowanie nie dotyczy tego konkretnego wielkoskalowego systemu informatycznego, podejmowana jest większością dwóch trzecich głosów członków zarządu, którym przysługuje prawo głosu.

6. Przewodniczący, lub zastępca przewodniczącego pełniący jego obowiązki pod jego nieobecność, nie głosuje. Przysługujące przewodniczącemu lub wiceprzewodniczącemu pełniącemu jego obowiązki pod jego nieobecność prawo głosu wykonuje jego zastępca.

7. Dyrektor wykonawczy nie głosuje.

8. Szczegółową procedurę głosowania określają przepisy regulaminu wewnętrznego zarządu, zwłaszcza co do warunków, na jakich jeden z członków może działać w imieniu innego członka, oraz, w stosownych przypadkach, wszelkie wymagania odnośnie do kworum.

Artykuł 24

Obowiązki dyrektora wykonawczego

1. Dyrektor wykonawczy zarządza Agencją. Dyrektor wykonawczy wspiera zarząd i przed nim odpowiada. Dyrektor wykonawczy składa sprawozdanie z wykonywania obowiązków Parlamentowi Europejskiemu na jego żądanie. Rada może wezwać dyrektora wykonawczego do złożenia sprawozdania z wykonywania obowiązków.

2. Dyrektor wykonawczy jest przedstawicielem prawnym Agencji.

3. Dyrektor wykonawczy odpowiada za wykonywanie zadań powierzonych Agencji na mocy niniejszego rozporządzenia. Dyrektor wykonawczy odpowiada w szczególności za:

a) bieżące kierowanie Agencją;

b) funkcjonowanie Agencji zgodne z niniejszym rozporządzeniem;

c) przygotowanie i wprowadzenie w życie – w granicach określonych niniejszym rozporządzeniem, przepisami wykonawczymi do niego oraz mającymi zastosowanie przepisami prawa unijnego – procedur, decyzji, strategii, programów oraz działań przyjętych przez zarząd;

d) opracowanie jednolitego dokumentu programowego oraz składanie go zarządowi po konsultacjach z Komisją i grupami doradczymi;

e) wdrożenie jednolitego dokumentu programowego i składanie sprawozdań z jego wykonania zarządowi;

f) przygotowanie wstępnego sprawozdania z postępów we wdrażaniu zaplanowanych działań obejmujących aktualny rok oraz, po konsultacjach z grupami doradczymi, przedkładanie go przed końcem sierpnia każdego roku zarządowi do przyjęcia;

g) opracowanie skonsolidowanego rocznego sprawozdania z działalności Agencji i, po konsultacjach z grupami doradczymi, przedkładanie go zarządowi do oceny i przyjęcia;

h) przygotowanie planu działań następczych w odniesieniu do ustaleń wynikających ze sprawozdań z audytu wewnętrznego lub zewnętrznego oraz ocen, jak również do postępowań przeprowadzonych przez Europejski Urząd ds. Zwalczania Nadużyć Finansowych (OLAF) i Prokuraturę Europejską oraz składanie – dwa razy w roku Komisji oraz regularnie zarządowi – sprawozdania z postępów;

i) ochronę interesów finansowych Unii poprzez stosowanie środków zapobiegawczych w stosunku do nadużyć finansowych, korupcji i wszelkiej innej nielegalnej działalności, z zastrzeżeniem kompetencji Prokuratury Europejskiej i OLAF-u w zakresie prowadzenia dochodzeń, poprzez skuteczne kontrole oraz – w przypadku stwierdzenia nieprawidłowości – odzyskiwanie nienależycie wydatkowanych kwot, a także w razie potrzeby stosowanie skutecznych, proporcjonalnych i odstraszających kar administracyjnych, w tym kar pieniężnych;

j) przygotowanie strategii Agencji na rzecz przeciwdziałania nadużyciom i przedstawienie jej zarządowi do zatwierdzenia, a także monitorowanie właściwego i terminowego wdrożenia tej strategii;

k) przygotowanie przepisów finansowych mających zastosowanie do Agencji i przedstawienie ich zarządowi do przyjęcia po konsultacji z Komisją;

l) przygotowanie projektu budżetu na kolejny rok, sporządzanego w oparciu o budżetowanie zadaniowe;

m) przygotowanie projektu preliminarza dochodów i wydatków Agencji;

n) wykonanie budżetu Agencji;

o) ustanowienie i wdrożenie skutecznego systemu w celu umożliwienia regularnego monitorowania i oceniania:

   (i) wielkoskalowych systemów informatycznych, w tym statystyk; oraz

   (ii) Agencji, w tym skutecznej i efektywnej realizacji jej celów;

p) określenie, bez uszczerbku dla art. 17 regulaminu pracowniczego urzędników, wymogów poufności w celu wykonania art. 17 rozporządzenia (WE) nr 1987/2006, art. 17 decyzji 2007/533/WSiSW, art. 26 ust. 9 rozporządzenia (WE) nr 767/2008, art. 4 ust. 4 rozporządzenia (UE) nr 603/2013, art. 37 ust. 4 rozporządzenia (UE) 2017/2226 i art. 74 ust. 2 rozporządzenia (UE) 2018/1240;

q) negocjowanie oraz – po zatwierdzeniu przez zarząd – podpisanie z przyjmującymi państwami członkowskimi umowy w sprawie siedziby Agencji oraz umów dotyczących centrum technicznego i obiektu zapasowego;

r) przygotowanie praktycznych ustaleń dotyczących wykonania rozporządzenia (WE) nr 1049/2001 oraz przedstawienie ich zarządowi do przyjęcia;

s) przygotowanie niezbędnych środków bezpieczeństwa, w tym planu bezpieczeństwa oraz planu ciągłości działania i planu przywrócenia gotowości do pracy po wystąpieniu sytuacji nadzwyczajnej oraz, po konsultacji ze stosowną grupą doradczą, przedstawienie ich zarządowi do przyjęcia;

t) przygotowanie sprawozdań z technicznego funkcjonowania każdego z wielkoskalowych systemów informatycznych, o których mowa w art. 19 ust. 1 lit. ff), oraz rocznego sprawozdania z działalności systemu centralnego Eurodac, o którym mowa w art. 19 ust. 1 lit. gg), na podstawie wyników monitorowania i oceny, oraz, po konsultacji ze stosowną grupą doradczą, przedstawienie ich zarządowi do przyjęcia;

u) przygotowanie sprawozdań dotyczących rozwoju systemu EES, o którym mowa w art. 72 ust. 2 rozporządzenia (UE) 2017/2226, oraz rozwoju systemu ETIAS, o którym mowa w art. 92 ust. 2 rozporządzenia (UE) 2018/1240;

v) przygotowanie, do celów publikacji, rocznego wykazu właściwych organów upoważnionych do bezpośredniego wyszukiwania danych znajdujących się w systemie SIS II wraz z wykazem urzędów N.SIS II oraz biur SIRENE oraz wykazu właściwych organów upoważnionych do bezpośredniego wyszukiwania danych znajdujących się w systemach EES i ETIAS, o których mowa w art. 19 ust. 1 lit. mm), oraz wykazów jednostek, o których mowa w art. 19 ust. 1 lit. nn), oraz przedstawienie ich zarządowi do przyjęcia.

4. Dyrektor wykonawczy wykonuje wszelkie inne zadania zgodnie z niniejszym rozporządzeniem.

5. Dyrektor wykonawczy podejmuje decyzję, czy do skutecznego i efektywnego wykonywania zadań Agencji konieczne jest umieszczenie jej pracownika lub pracowników w państwie członkowskim lub państwach członkowskich oraz utworzenie w tym celu biura lokalnego. Przed podjęciem takiej decyzji dyrektor wykonawczy musi otrzymać zgodę Komisji, zarządu i zainteresowanego państwa członkowskiego lub zainteresowanych państw członkowskich. W decyzji dyrektora wykonawczego określa się zakres działań prowadzonych w lokalnym biurze w sposób pozwalający uniknąć niepotrzebnych kosztów i powielania administracyjnych funkcji Agencji. Działania prowadzone w siedzibach technicznych nie mogą być prowadzone w biurze lokalnym.

Artykuł 25

Powoływanie dyrektora wykonawczego

1. Zarząd powołuje dyrektora wykonawczego z listy co najmniej trzech kandydatów zaproponowanych przez Komisję na podstawie otwartej i przejrzystej procedury naboru. Procedura naboru przewiduje publikację zaproszenia do wyrażenia zainteresowania w *Dzienniku Urzędowym Unii Europejskiej* oraz w innych właściwych środkach przekazu. Zarząd powołuje dyrektora wykonawczego w oparciu o kompetencje, udokumentowane doświadczenie w dziedzinie wielkoskalowych systemów informatycznych, umiejętności administracyjne, finansowe i w zakresie zarządzania oraz wiedzę w odniesieniu do ochrony danych.

2. Przed powołaniem zaproponowani przez Komisję kandydaci są wzywani do złożenia oświadczenia przed właściwą komisją lub właściwymi komisjami Parlamentu Europejskiego i do udzielenia odpowiedzi na pytania członków komisji. Po wysłuchaniu oświadczeń i odpowiedzi kandydatów Parlament Europejski przyjmuje opinię, w której przedstawia swoje uwagi i może wskazać preferowanego kandydata.

3. Zarząd powołuje dyrektora wykonawczego, uwzględniając wspomniane uwagi.

4. Jeżeli zarząd podejmie decyzję o powołaniu kandydata innego niż kandydat, którego Parlament Europejski wskazał jako preferowanego kandydata, informuje na piśmie Parlament Europejski i Radę o sposobie uwzględnienia opinii Parlamentu Europejskiego.

5. Kadencja dyrektora wykonawczego trwa pięć lat. Przed upływem tego okresu Komisja przeprowadza ocenę, w której uwzględnia wyniki swojej oceny pracy dyrektora wykonawczego oraz przyszłe zadania i wyzwania stojące przed Agencją.

6. Zarząd, działając na wniosek Komisji, w którym uwzględniono ocenę wspomnianą w ust. 5, może jednokrotnie przedłużyć kadencję dyrektora wykonawczego na okres nie dłuższy niż pięć lat.

7. Zarząd informuje Parlament Europejski o zamiarze przedłużenia kadencji dyrektora wykonawczego. W okresie miesiąca poprzedzającego każde takie przedłużenie kadencji dyrektor wykonawczy jest wzywany do złożenia oświadczenia przed właściwą komisją lub właściwymi komisjami Parlamentu Europejskiego i do udzielenia odpowiedzi na pytania członków komisji.

8. Dyrektor wykonawczy, którego kadencję przedłużono, nie może brać udziału w kolejnym postępowaniu rekrutacyjnym na to samo stanowisko pod koniec całego okresu urzędowania.

9. Dyrektor wykonawczy może zostać odwołany ze stanowiska jedynie na mocy decyzji zarządu działającego na wniosek większości swoich członków z prawem głosu lub na wniosek Komisji.

10. Zarząd podejmuje decyzje w sprawie powołania, przedłużenia kadencji lub odwołania ze stanowiska dyrektora wykonawczego większością dwóch trzecich głosów członków z prawem głosu.

11. Do celów zawarcia umowy o pracę z dyrektorem wykonawczym Agencję reprezentuje przewodniczący zarządu. Dyrektor wykonawczy zostaje zaangażowany jako pracownik Agencji zatrudniony na czas określony zgodnie z art. 2 lit. a) warunków zatrudnienia innych pracowników.

Artykuł 26

Zastępca dyrektora wykonawczego

1. Zastępca dyrektora wykonawczego wspiera dyrektora wykonawczego. Zastępca dyrektora wykonawczego zastępuje też dyrektora wykonawczego podczas jego nieobecności. Dyrektor wykonawczy określa obowiązki swojego zastępcy.

2. Zarząd powołuje zastępcę dyrektora wykonawczego na wniosek dyrektora wykonawczego. Zastępca dyrektora wykonawczego jest powoływany na podstawie osiągnięć i odpowiednich umiejętności w zakresie administracji i zarządzania, w tym odpowiedniego doświadczenia zawodowego. Dyrektor wykonawczy zgłasza co najmniej trzech kandydatów na stanowisko zastępcy dyrektora wykonawczego. Zarząd podejmuje decyzję większością dwóch trzecich głosów członków z prawem głosu. Zarząd jest uprawniony do zwolnienia zastępcy dyrektora wykonawczego decyzją przyjętą większością dwóch trzecich głosów członków z prawem głosu.

3. Kadencja zastępcy dyrektora wykonawczego trwa pięć lat. Zarząd może przedłużyć tę kadencję jednokrotnie o okres nieprzekraczający pięciu lat. Zarząd podejmuje taką decyzję większością dwóch trzecich głosów wszystkich członków z prawem głosu.

Artykuł 27

Grupy doradcze

1. Następujące grupy doradcze wspomagają zarząd, zapewniając wiedzę fachową w zakresie wielkoskalowych systemów informatycznych, w szczególności podczas przygotowywania rocznego programu prac oraz rocznego sprawozdania z działalności:

a) grupa doradcza ds. SIS II;

b) grupa doradcza ds. VIS;

c) grupa doradcza ds. Eurodac;

d) grupa doradcza ds. EES-ETIAS;

e) każda inna grupa doradcza do spraw wielkoskalowego systemu informatycznego, o ile tak stanowi unijny akt prawny regulujący rozwijanie, ustanowienie, funkcjonowanie i użytkowanie tego wielkoskalowego systemu informatycznego.

2. Każde z państw członkowskich, które na mocy prawa Unii jest związane unijnym aktem prawnym regulującym rozwijanie, ustanowienie, funkcjonowanie i użytkowanie określonego wielkoskalowego systemu informatycznego, oraz Komisja, wyznaczają na czteroletnią kadencję, z możliwością jej przedłużenia, jednego członka grupy doradczej zajmującej się tym wielkoskalowym systemem informatycznym.

Również Dania powinna wyznaczyć członka grupy doradczej zajmującej się wielkoskalowym systemem informatycznym, jeżeli podejmie decyzję – na mocy art. 4 Protokołu nr 22 – o wprowadzeniu do swojego prawa krajowego unijnego aktu prawnego regulującego rozwijanie, ustanawianie, funkcjonowanie i użytkowanie tego wielkoskalowego systemu informatycznego.

Każde z państw włączonych we wdrażanie, stosowanie i rozwijanie dorobku Schengen oraz środków dotyczących rozporządzeń dublińskich i systemu Eurodac, które uczestniczy w określonym wielkoskalowym systemie informatycznym, powołuje członka grupy doradczej zajmującej się tym wielkoskalowym systemem informatycznym.

3. Europol, Eurojust i Europejska Agencja Straży Granicznej i Przybrzeżnej mogą powołać po jednym przedstawicielu do grupy doradczej ds. SIS II. Europol może także powołać przedstawiciela do grup doradczych ds. VIS, Eurodac i EES-ETIAS. Europejska Agencja Straży Granicznej i Przybrzeżnej może także powołać przedstawiciela do grupy doradczej ds. EES-ETIAS.

4. Członkowie zarządu i ich zastępcy nie mogą być członkami jakichkolwiek grup doradczych. Dyrektor wykonawczy lub przedstawiciel dyrektora wykonawczego mają prawo uczestniczyć we wszystkich posiedzeniach grup doradczych w charakterze obserwatora.

5. W razie potrzeby grupy doradcze powinny ze sobą współpracować. Procedury działania i współpracy grup doradczych zostają ustanowione w regulaminie wewnętrznym Agencji.

6. Przygotowując opinię, członkowie każdej z grup doradczych dokładają wszelkich starań, aby osiągnąć porozumienie. Jeżeli nie osiągnięto porozumienia, za opinię uznaje się uzasadnione stanowisko większości członków. Odnotowuje się również uzasadnione stanowisko lub stanowiska mniejszości członków. Artykuł 23 ust. 3 i 5 stosuje się odpowiednio. Członkowie reprezentujący państwa włączone we wdrażanie, stosowanie i rozwijanie dorobku Schengen oraz środków dotyczących rozporządzeń dublińskich i systemu Eurodac mają prawo wyrażać opinie w sprawach, w których nie mają prawa głosu.

7. Każde z państw członkowskich oraz każde z państw włączonych we wdrażanie, stosowanie i rozwijanie dorobku Schengen oraz środków dotyczących rozporządzeń dublińskich i systemu Eurodac ułatwia działalność grup doradczych.

8. W odniesieniu do przewodniczących grup doradczych stosuje się odpowiednio art. 21.

ROZDZIAŁ IV

PRZEPISY OGÓLNE

Artykuł 28

Pracownicy

1. Do personelu Agencji, w tym dyrektora wykonawczego, mają zastosowanie regulamin pracowniczy oraz przepisy przyjęte w drodze porozumienia między instytucjami Unii w celu nadania skuteczności regulaminowi pracowniczemu.

2. Do celów wdrażania regulaminu pracowniczego Agencja uznawana jest za agencję w rozumieniu art. 1a ust. 2 regulaminu pracowniczego urzędników.

3. Personel Agencji składa się z urzędników, pracowników zatrudnionych na czas określony i personelu kontraktowego. Zarząd co roku wydaje zgodę w przypadku umów, które dyrektor wykonawczy zamierza przedłużyć, jeżeli w wyniku przedłużenia takie umowy stałyby się, zgodnie z warunkami zatrudnienia innych pracowników, umowami na czas nieokreślony.

4. Do wykonywania zadań finansowych uznawanych za szczególnie wrażliwe Agencja nie zatrudnia pracowników tymczasowych.

5. Komisja i państwa członkowskie mogą delegować do Agencji na czas określony urzędników lub ekspertów krajowych. Zarząd przyjmuje decyzję określającą zasady oddelegowania ekspertów krajowych do Agencji.

6. Bez uszczerbku dla art. 17 regulaminu pracowniczego urzędników Agencja stosuje odpowiednie zasady tajemnicy służbowej lub inne równoważne wymogi poufności.

7. W porozumieniu z Komisją zarząd przyjmuje niezbędne środki wykonawcze, o których mowa w art. 110 regulaminu pracowniczego urzędników.

Artykuł 29

Interes publiczny

Członkowie zarządu, dyrektor wykonawczy, zastępca dyrektora wykonawczego oraz członkowie grup doradczych zobowiązują się do działania w interesie publicznym. W tym celu wydają oni coroczne pisemne, publiczne zobowiązanie, które publikowane jest na stronie internetowej Agencji.

Lista członków zarządu i członków grup doradczych jest publikowana na stronie internetowej Agencji.

Artykuł 30

Umowa w sprawie siedziby oraz umowy dotyczące centrum technicznego

1. Niezbędne ustalenia dotyczące lokalizacji Agencji w przyjmujących państwach członkowskich oraz infrastruktury, jaką te państwa członkowskie mają udostępnić wraz ze szczególnymi zasadami mającymi zastosowanie w przyjmujących państwach członkowskich do członków zarządu, dyrektora wykonawczego, pracowników Agencji i członków ich rodzin są określane w umowie w sprawie siedziby dotyczącej siedziby Agencji oraz umowie w sprawie centrum technicznego. Taka umowa zawierana jest między Agencją a przyjmującymi państwami członkowskimi po uzyskaniu zgody zarządu.

2. Przyjmujące państwa członkowskie Agencji tworzą niezbędne warunki zapewniające między innymi prawidłowe funkcjonowanie Agencji, m.in. wielojęzyczne szkolnictwo o charakterze europejskim i odpowiednie połączenia transportowe.

Artykuł 31

Przywileje i immunitety

Do Agencji zastosowanie ma Protokół w sprawie przywilejów i immunitetów Unii Europejskiej.

Artykuł 32

Odpowiedzialność

1. Odpowiedzialność umowną Agencji reguluje prawo właściwe dla danej umowy.

2. Trybunał Sprawiedliwości Unii Europejskiej jest właściwy do rozpoznawania sporów na podstawie klauzuli arbitrażowej zamieszczonej w umowie zawartej przez Agencję.

3. W przypadku odpowiedzialności pozaumownej Agencja naprawia szkodę wyrządzoną przez jej jednostki lub jej pracowników przy wykonywaniu ich obowiązków zgodnie z zasadami ogólnymi wspólnymi dla ustawodawstw państw członkowskich.

4. Trybunał Sprawiedliwości Unii Europejskiej jest właściwy do orzekania w sporach dotyczących odszkodowania za szkody, o których mowa w ust. 3.

5. Odpowiedzialność osobista pracowników Agencji wobec Agencji uregulowana jest przepisami regulaminu pracowniczego urzędników lub mającymi do nich zastosowanie warunkami zatrudnienia innych pracowników.

Artykuł 33

Ustalenia językowe

1. Rozporządzenie Rady nr 1 ([1]) ma zastosowanie do Agencji.

2. Bez uszczerbku dla decyzji podjętych na podstawie art. 342 TFUE, jednolity dokument programowy, o którym mowa w art. 19 ust. 1 lit. r), i roczne sprawozdanie z działalności, o którym mowa w art. 19 ust. 1 lit. t), sporządzane są we wszystkich językach urzędowych instytucji Unii.

3. Zarząd może przyjąć decyzję w sprawie języków roboczych, pod warunkiem że pozostanie ona bez uszczerbku dla obowiązków określonych w ust. 1 i 2.

4. Tłumaczenia pisemne niezbędne do funkcjonowania Agencji zapewnia Centrum Tłumaczeń dla Organów Unii Europejskiej.

Artykuł 34

Przejrzystość i informowanie

1. Rozporządzenie (WE) nr 1049/2001 ma zastosowanie do dokumentów pozostających w posiadaniu Agencji.

2. Na wniosek dyrektora wykonawczego zarząd niezwłocznie przyjmuje szczegółowe zasady stosowania rozporządzenia (WE) nr 1049/2001.

3. Decyzje podjęte przez Agencję na mocy art. 8 rozporządzenia (WE) nr 1049/2001 mogą być przedmiotem skargi do Europejskiego Rzecznika Praw Obywatelskich lub może zostać przeciwko nim wniesiona skarga do Trybunału Sprawiedliwości Unii Europejskiej na warunkach określonych, odpowiednio, w art. 228 i 263 TFUE.

4. Agencja przekazuje informacje zgodnie z unijnymi aktami prawnymi regulującymi rozwijanie, tworzenie, funkcjonowanie i użytkowanie wielkoskalowych systemów informatycznych i może z własnej inicjatywy angażować się w działania komunikacyjne w zakresie swoich kompetencji. Agencja w szczególności zapewnia, aby poza publikowanymi informacjami określonymi w art. 19 ust. 1 lit. r), t), ii), jj), kk) i ll) oraz art. 47 ust. 9, opinii publicznej oraz każdej zainteresowanej stronie szybko przekazywane były obiektywne, dokładne, wiarygodne, kompleksowe i zrozumiałe informacje dotyczące pracy Agencji. Przydział zasobów na działania komunikacyjne nie może mieć niekorzystnego wpływu na skuteczne wykonywanie zadań Agencji, o których mowa w art. 3–16. Działania komunikacyjne są wykonywane zgodnie z przyjętymi przez zarząd właściwymi planami komunikacji i rozpowszechniania informacji.

5. Każda osoba fizyczna lub prawna może kierować do Agencji korespondencję w formie pisemnej w dowolnym języku urzędowym Unii. Dana osoba ma prawo do otrzymania odpowiedzi w tym samym języku.

Artykuł 35

Ochrona danych

1. Przetwarzanie danych osobowych przez Agencję podlega przepisom rozporządzenia (UE) 2018/1725.

2. Zarząd przyjmuje środki mające na celu umożliwienie stosowania przez Agencję rozporządzenia (UE) 2018/1725, w tym środki dotyczące inspektora ochrony danych. Środki te przyjmowane są po konsultacji z Europejskim Inspektorem Ochrony Danych.

([1]) Rozporządzenie Rady nr 1 z dnia 15 kwietnia 1958 r. w sprawie określenia systemu językowego Europejskiej Wspólnoty Gospodarczej (Dz.U. 17 z 6.10.1958, s. 385).

Artykuł 36

Cele przetwarzania danych osobowych

1. Agencja może przetwarzać dane osobowe jedynie do poniższych celów:

a) gdy jest to niezbędne do realizacji jej zadań związanych z zarządzaniem operacyjnym wielkoskalowymi systemami informatycznymi powierzonym jej na mocy prawa unijnego;

b) gdy jest to niezbędne do jej zadań administracyjnych.

2. Jeżeli Agencja przetwarza dane osobowe do celu, o którym mowa w ust. 1 lit. a) niniejszego artykułu, stosuje się rozporządzenie (UE)/2018/1725, bez uszczerbku dla określonych przepisów dotyczących ochrony i bezpieczeństwa danych pochodzących z unijnych aktów prawnych regulujących rozwijanie, tworzenie, funkcjonowanie i użytkowanie systemów.

Artykuł 37

Przepisy bezpieczeństwa w zakresie ochrony informacji niejawnych i szczególnie chronionych informacji jawnych

1. Agencja przyjmuje własne przepisy bezpieczeństwa w oparciu o zasady i przepisy bezpieczeństwa zawarte w przepisach bezpieczeństwa Komisji dotyczących ochrony informacji niejawnych UE (EUCI) oraz szczególnie chronionych informacji jawnych, m.in. w przepisach dotyczących wymiany z państwami trzecimi, przetwarzania i przechowywania tego rodzaju informacji, jak określono w decyzjach Komisji (UE, Euratom) 2015/443 ([1]) i 2015/444 ([2]). Wszelkie porozumienia administracyjne dotyczące wymiany informacji niejawnych z właściwymi organami państw trzecich lub, w przypadku braku takiego porozumienia, wszelkie wyjątkowe udostępnianie EUCI ad hoc tym organom wymagają wcześniejszego zatwierdzenia przez Komisję.

2. Zarząd przyjmuje przepisy bezpieczeństwa, o których mowa w ust. 1 niniejszego artykułu, po zatwierdzeniu przez Komisję. Agencja może podjąć wszelkie niezbędne środki w celu ułatwienia wymiany informacji istotnych dla jej zadań z Komisją i państwami członkowskimi oraz, w stosownych przypadkach, z właściwymi agencjami Unii. Agencja opracowuje i stosuje system informacyjny umożliwiający wymianę informacji niejawnych z Komisją, z państwami członkowskimi oraz z właściwymi agencjami unijnymi zgodnie z decyzją (UE, Euratom) 2015/444. Zarząd podejmuje decyzję – zgodnie z art. 2 i art. 19 ust. 1 lit. z) niniejszego rozporządzenia – w sprawie struktury wewnętrznej Agencji niezbędnej do przestrzegania przez nią odpowiednich zasad bezpieczeństwa.

Artykuł 38

Bezpieczeństwo Agencji

1. Agencja odpowiada za bezpieczeństwo i zachowanie porządku w budynkach, lokalach i na terenie, z których korzysta. Agencja stosuje zasady bezpieczeństwa i stosowne przepisy unijnych aktów prawnych regulujących rozwijanie, tworzenie, funkcjonowanie i użytkowanie wielkoskalowych systemów informatycznych.

2. Przyjmujące państwa członkowskie przyjmują wszystkie skuteczne i odpowiednie środki w celu zachowania porządku i bezpieczeństwa w najbliższym sąsiedztwie budynków, lokali i terenu, z których korzysta Agencja, i zapewniają Agencji odpowiednią ochronę, zgodnie z umową w sprawie siedziby dotyczącą siedziby Agencji i umowami dotyczącymi centrum technicznego i obiektu zapasowego, gwarantując jednocześnie osobom upoważnionym przez Agencję swobodny dostęp do tych budynków, lokali i terenu.

Artykuł 39

Ocena

1. Do dnia 12 grudnia 2023 r., a także co pięć lat po tej dacie, Komisja – po konsultacji z zarządem – ocenia wyniki prac Agencji w odniesieniu do jej celów, mandatu, lokalizacji i zadań, zgodnie z wytycznymi Komisji. Ocena ta obejmuje także analizę postępów we wdrażaniu niniejszego rozporządzenia oraz tego, w jaki sposób i w jakim zakresie Agencja skutecznie przyczynia się do zarządzania operacyjnego wielkoskalowymi systemami informatycznymi i do tworzenia skoordynowanego, efektywnego kosztowo i spójnego środowiska informatycznego na poziomie Unii w przestrzeni wolności, bezpieczeństwa i sprawiedliwości. Ocena ta dotyczy w szczególności ewentualnej potrzeby zmiany mandatu Agencji oraz skutków finansowych takiej zmiany. Zarząd może przedstawić Komisji zalecenia co do zmian w niniejszym rozporządzeniu.

([1]) Decyzja Komisji (UE, Euratom) 2015/443 z dnia 13 marca 2015 r. w sprawie bezpieczeństwa w Komisji (Dz.U. L 72 z 17.3.2015, s. 41).

([2]) Decyzja Komisji (UE, Euratom) 2015/444 z dnia 13 marca 2015 r. w sprawie przepisów bezpieczeństwa dotyczących ochrony informacji niejawnych UE (Dz.U. L 72 z 17.3.2015, s. 53).

2. Jeśli Komisja uzna, że dalsze działanie Agencji w odniesieniu do powierzonych jej celów, mandatu i zadań nie jest uzasadnione, może wnioskować o odpowiednią zmianę lub uchylenie niniejszego rozporządzenia.

3. Komisja zdaje sprawozdanie z wyników oceny, o której mowa w ust. 1, Parlamentowi Europejskiemu, Radzie i zarządowi. Wyniki oceny podawane są do wiadomości publicznej.

Artykuł 40

Dochodzenia administracyjne

Działania Agencji podlegają dochodzeniom prowadzonym przez Europejskiego Rzecznika Praw Obywatelskich zgodnie z postanowieniami art. 228 Traktatu.

Artykuł 41

Współpraca z instytucjami, organami i jednostkami organizacyjnymi Unii

1. W zakresie kwestii objętych niniejszym rozporządzeniem Agencja współpracuje z Komisją, innymi instytucjami, organami i jednostkami organizacyjnymi Unii, zwłaszcza z tymi, które ustanowiono w przestrzeni wolności, bezpieczeństwa i sprawiedliwości, a przede wszystkimi z Agencją Praw Podstawowych Unii Europejskiej w celu zapewnienia m.in. koordynacji i oszczędności finansowych, uniknięcia powielania i promowania synergii i komplementarności ich wzajemnych działań.

2. Agencja współpracuje z Komisją w ramach porozumienia roboczego, określającego operacyjne metody pracy.

3. W stosownych przypadkach Agencja konsultuje się z Europejską Agencją ds. Bezpieczeństwa Sieci i Informacji oraz stosuje się do jej zaleceń dotyczących bezpieczeństwa sieci i informacji.

4. Współpracę z organami i jednostkami organizacyjnymi Unii prowadzi się w ramach porozumień roboczych. Zarząd zatwierdza takie porozumienia robocze, biorąc pod uwagę opinię Komisji. Jeżeli Agencja nie zastosuje się do opinii Komisji, uzasadnia ona swoje stanowisko. W stosownych przypadkach takie porozumienia robocze mogą przewidywać wspólne korzystanie Agencji ze służb albo z uwagi na bliską lokalizację, albo pod kątem obszarów polityk w granicach odpowiednich mandatów oraz bez uszczerbku dla ich podstawowych zadań. Takie porozumienia robocze mogą ustanawiać mechanizm zwrotu kosztów.

5. Instytucje, organy i jednostki organizacyjne Unii wykorzystują informacje uzyskane od Agencji jedynie w ramach swoich kompetencji i z poszanowaniem praw podstawowych, w tym wymogów ochrony danych. Dalsze przekazywanie lub przekazywanie w inny sposób danych osobowych przetwarzanych przez Agencję instytucjom, organom i jednostkom organizacyjnym Unii odbywa się na podstawie specjalnych porozumień roboczych dotyczących wymiany danych osobowych oraz z zastrzeżeniem wcześniejszego zatwierdzenia przez Europejskiego Inspektora Ochrony Danych. Każdy przypadek przekazywania danych osobowych przez Agencję musi być zgodny z art. 35 i 36. W odniesieniu do postępowania z informacjami niejawnymi, w takich porozumieniach roboczych przewiduje się, że dana instytucja, organ lub jednostka organizacyjna Unii stosuje zasady i standardy bezpieczeństwa równoważne stosowanym przez Agencję.

Artykuł 42

Udział państw uczestniczących we wdrażaniu, stosowaniu i rozwijaniu dorobku Schengen oraz środków dotyczących rozporządzeń dublińskich i systemu Eurodac

1. Agencja jest otwarta na udział państw, które zawarły z Unią umowy dotyczące ich włączenia we wprowadzanie w życie, stosowanie i rozwój dorobku Schengen oraz środków dotyczących rozporządzeń dublińskich i systemu Eurodac.

2. Na mocy stosownych postanowień umów, o których mowa w ust. 1, dokonuje się ustaleń, w szczególności w odniesieniu do charakteru, zakresu i szczegółowych zasad udziału w pracy Agencji państw trzecich, zgodnie z ust. 1, w tym w odniesieniu do przepisów dotyczących wkładów finansowych, pracowników i prawa głosu.

Artykuł 43

Współpraca z organizacjami międzynarodowymi i innymi odpowiednimi podmiotami

1. Jeżeli tak przewidziano w akcie prawa unijnego oraz w zakresie, w jakim jest to niezbędne do realizacji jej zadań, Agencja może, w drodze zawarcia porozumień roboczych, nawiązać i utrzymywać stosunki z organizacjami międzynarodowymi i organami im podlegającymi będącymi podmiotami prawa międzynarodowego publicznego lub innymi właściwymi instytucjami lub organami utworzonymi w drodze lub na podstawie umowy między co najmniej dwoma państwami.

2. Zgodnie z ust. 1 mogą być zawierane porozumienia robocze dotyczące w szczególności zakresu, charakteru, celu i rozmiarów takiej współpracy. Takie porozumienia robocze mogą być zawierane wyłącznie za zgodą zarządu i po wcześniejszym zatwierdzeniu przez Komisję.

ROZDZIAŁ V

UCHWALANIE I STRUKTURA BUDŻETU

SEKCJA 1

Jednolity dokument programowy

Artykuł 44

Jednolity dokument programowy

1. Każdego roku dyrektor wykonawczy sporządza projekt jednolitego dokumentu programowego na następny rok, określonego w art. 32 rozporządzenia delegowanego (UE) nr 1271/2013 oraz w odpowiednich postanowieniach przepisów finansowych Agencji przyjętych na podstawie art. 49 niniejszego rozporządzenia, z uwzględnieniem wytycznych określonych przez Komisję.

Jednolity dokument programowy powinien zawierać program wieloletni, roczny program prac, a także budżet Agencji i informację o jej zasobach, jak szczegółowo określono w przepisach finansowych Agencji, przyjętych na podstawie art. 49.

2. Po konsultacjach z grupami doradczymi zarząd przyjmuje projekt jednolitego dokumentu programowego i przesyła go Parlamentowi Europejskiemu, Radzie i Komisji do dnia 31 stycznia każdego roku, oraz przekazuje im wszelkie późniejsze wersje tego dokumentu.

3. Przed dniem 30 listopada każdego roku zarząd, przy uwzględnieniu opinii Komisji, przyjmuje jednolity dokument programowy większością dwóch trzecich głosów swoich członków z prawem głosu i zgodnie z roczną procedurą budżetową. Zarząd zapewnia przekazanie ostatecznej wersji jednolitego dokumentu programowego Parlamentowi Europejskiemu, Radzie i Komisji oraz jego opublikowanie.

4. Jednolity dokument programowy staje się ostateczny po ostatecznym przyjęciu budżetu ogólnego Unii i w razie potrzeby jest odpowiednio korygowany. Przyjęty jednolity dokument programowy jest następnie przesyłany Parlamentowi Europejskiemu, Radzie i Komisji oraz publikowany.

5. Roczny program prac na następny rok zawiera szczegółowe cele oraz oczekiwane rezultaty, w tym wskaźniki wykonania. Zawiera również opis działań, które mają być finansowane, oraz określa zasoby finansowe i ludzkie przydzielone do każdego działania zgodnie z zasadami budżetowania zadaniowego i zarządzania kosztami działań. Roczny program prac musi być spójny z wieloletnim programem prac, o którym mowa w ust. 6. Roczny program prac jednoznacznie określa zadania, które zostały dodane, zmienione lub skreślone w stosunku do poprzedniego roku budżetowego. Zarząd dokonuje zmiany przyjętego rocznego programu prac w przypadku przekazania Agencji nowego zadania. Wszelkie merytoryczne zmiany w rocznym programie prac przyjmuje się w drodze tej samej procedury, co pierwotny roczny program prac. Zarząd może przekazać Dyrektorowi wykonawczemu uprawnienia do dokonywania zmian niemerytorycznych w rocznym programie prac.

6. Wieloletni program określa ogólne założenia strategiczne, w tym cele, oczekiwane rezultaty i wskaźniki wykonania. Wyznacza również programowanie w zakresie zasobów, w tym budżetu wieloletniego i personelu. Programowanie w zakresie zasobów jest aktualizowane co roku. Założenia strategiczne są uaktualniane w miarę potrzeb, w szczególności celem uwzględnienia wyników oceny, o której mowa w art. 39.

Artykuł 45

Ustanawianie budżetu

1. Dyrektor wykonawczy sporządza corocznie – przy uwzględnieniu działań prowadzonych przez Agencję – projekt preliminarza dochodów i wydatków Agencji na kolejny rok budżetowy, w tym projekt planu zatrudnienia, i przedstawia go zarządowi.

2. Zarząd przyjmuje corocznie – na podstawie projektu preliminarza sporządzonego przez dyrektora wykonawczego – projekt preliminarza dochodów i wydatków Agencji na kolejny rok budżetowy, w tym projekt planu zatrudnienia. Do dnia 31 stycznia każdego roku zarząd przesyła go Komisji oraz państwom włączonym we wprowadzanie w życie, stosowanie i rozwój dorobku Schengen oraz środków dotyczących rozporządzeń dublińskich i systemu Eurodac, jako część jednolitego dokumentu programowego.

3. Komisja przesyła projekt preliminarza władzy budżetowej wraz ze wstępnym projektem budżetu ogólnego Unii.

4. Na podstawie projektu preliminarza Komisja wprowadza do projektu budżetu ogólnego Unii oszacowania, które uważa za niezbędne dla planu zatrudnienia, oraz kwotę dotacji, która ma być ujęta w budżecie ogólnym przedkładanym przez Komisję władzy budżetowej zgodnie z art. 313 i 314 TFUE.

5. Władza budżetowa zatwierdza środki przewidziane na wkład dla Agencji.

6. Władza budżetowa przyjmuje plan zatrudnienia dla Agencji.

7. Zarząd przyjmuje budżet Agencji. Staje się on ostateczny po ostatecznym przyjęciu budżetu ogólnego Unii. W stosownych przypadkach budżet Agencji jest odpowiednio korygowany.

8. Wszelkich zmian w budżecie Agencji, w tym w planie zatrudnienia, dokonuje się według tej samej procedury, która ma zastosowanie do ustanawiania wstępnego budżetu.

9. Bez uszczerbku dla art. 17 ust. 5 zarząd niezwłocznie powiadamia władzę budżetową o swoim zamiarze realizacji wszelkich projektów, które mogą mieć znaczące konsekwencje finansowe dla środków budżetowych Agencji, w szczególności wszelkich projektów odnoszących się do nieruchomości, takich jak najem lub nabycie budynków. Zarząd informuje o nich Komisję. Jeżeli któryś z organów władzy budżetowej zamierza wydać opinię, powiadamia zarząd o tym zamiarze w terminie dwóch tygodni od otrzymania informacji o projekcie. W przypadku braku odpowiedzi Agencja może przystąpić do planowanego działania. Do wszelkich projektów budowlanych, które mogą mieć jakikolwiek znaczący wpływ na budżet Agencji, zastosowanie ma rozporządzenie delegowane (UE) nr 1271/2013.

SEKCJA 2

Przedstawianie, wykonywanie i kontrola budŻETU

Artykuł 46

Struktura budżetu

1. Preliminarz wszystkich dochodów i wydatków Agencji jest przygotowywany w każdym roku budżetowym odpowiadającym rokowi kalendarzowemu i jest wykazywany w budżecie Agencji.

2. Dochody i wydatki wykazane w budżecie Agencji muszą się równoważyć.

3. Bez uszczerbku dla innych rodzajów dochodów, struktura dochodów Agencji jest następująca:

a) wkład Unii zapisany w budżecie ogólnym Unii (dział Komisji);

b) wkład krajów włączonych we wdrażanie, stosowanie i rozwijanie dorobku Schengen oraz środków dotyczących rozporządzeń dublińskich i systemu Eurodac, które uczestniczą w pracach Agencji, ustalony w odpowiednich umowach o uczestnictwie oraz w uzgodnieniach, o jakich mowa w art. 42, określających ich wkład finansowy;

c) finansowanie Unii w formie umów o delegowaniu zadań zgodnie z przepisami finansowymi Agencji przyjętymi na podstawie art. 49 oraz postanowieniami stosownych instrumentów wspierających politykę Unii;

d) wkłady państw członkowskich za świadczone im usługi, zgodnie z umową o delegowaniu zadań, o której mowa w art. 16;

e) zwrot kosztów wnoszony przez organy i jednostki organizacyjne Unii w odniesieniu do usług świadczonych na ich rzecz zgodnie z porozumieniami roboczymi, o których mowa w art. 41; oraz

f) wszelkie dobrowolne wkłady finansowe państw członkowskich;

4. Wydatki Agencji obejmują wynagrodzenia pracowników, koszty administracyjne, koszty infrastruktury oraz koszty operacyjne.

Artykuł 47

Wykonywanie i kontrola budżetu

1. Dyrektor wykonawczy wykonuje budżet Agencji.

2. Co roku dyrektor wykonawczy przekazuje władzy budżetowej wszystkie informacje istotne z punktu widzenia wyników procedur oceny.

3. Do dnia 1 marca roku budżetowego N+1 księgowy Agencji przekazuje wstępne sprawozdania rachunkowe za rok budżetowy N księgowemu Komisji i Trybunałowi Obrachunkowemu. Księgowy Komisji konsoliduje sprawozdania rachunkowe instytucji i organów zdecentralizowanych zgodnie z art. 245 rozporządzenia (UE, Euratom) 2018/1046.

4. Do dnia 31 marca roku N+1 dyrektor wykonawczy przesyła sprawozdanie z zarządzania budżetem i finansami za rok N Parlamentowi Europejskiemu, Radzie, Komisji i Trybunałowi Obrachunkowemu.

5. Do dnia 31 marca roku N+1 księgowy Komisji przesyła wstępne sprawozdania rachunkowe Agencji za rok N, skonsolidowane ze sprawozdaniami Komisji, Trybunałowi Obrachunkowemu.

6. Po otrzymaniu uwag Trybunału Obrachunkowego dotyczących tymczasowego sprawozdania Agencji, zgodnie z art. 246 rozporządzenia (UE, Euratom) 2018/1046, dyrektor wykonawczy sporządza w zakresie swej odpowiedzialności ostateczne sprawozdanie finansowe Agencji i przekazuje je zarządowi do zaopiniowania.

7. Zarząd przedstawia opinię na temat końcowego sprawozdania rachunkowego Agencji za rok N.

8. Do dnia 1 lipca roku N+1 dyrektor wykonawczy przesyła Parlamentowi Europejskiemu, Radzie, Komisji i Trybunałowi Obrachunkowemu oraz państwom włączonym we wprowadzanie w życie, stosowanie i rozwój dorobku Schengen oraz środków dotyczących rozporządzeń dublińskich i systemu Eurodac ostateczne sprawozdanie rachunkowe wraz z opinią zarządu.

9. Końcowe sprawozdania rachunkowe za rok N są publikowane w *Dzienniku Urzędowym Unii Europejskiej* do dnia 15 listopada roku N+1.

10. Dyrektor wykonawczy przesyła Trybunałowi Obrachunkowemu odpowiedź na jego uwagi do dnia 30 września roku N+1. Dyrektor wykonawczy przesyła tę odpowiedź również zarządowi.

11. Dyrektor wykonawczy przesyła Parlamentowi Europejskiemu, na jego wniosek, wszelkie informacje niezbędne do sprawnego przeprowadzenia procedury udzielenia absolutorium za rok N, zgodnie z art. 261 ust. 3 rozporządzenia (UE, Euratom) 2018/1046.

12. Na zalecenie Rady, stanowiącej większością kwalifikowaną, do dnia 15 maja roku N+2 Parlament Europejski udziela dyrektorowi wykonawczemu absolutorium z wykonania budżetu za rok budżetowy N.

Artykuł 48

Zapobieganie konfliktom interesów

Agencja przyjmuje regulamin wewnętrzny wymagający, by członkowie jej zarządu oraz członkowie jej grup doradczych unikali sytuacji, które z dużym prawdopodobieństwem mogą spowodować konflikt interesów w trakcie okresu zatrudnienia lub kadencji, oraz by zgłaszali takie sytuacje. Ten regulamin wewnętrzny publikuje się na stronie internetowej Agencji.

Artykuł 49

Przepisy finansowe

Przepisy finansowe mające zastosowanie do Agencji przyjmuje zarząd po konsultacji z Komisją. Nie mogą one odbiegać od rozporządzenia delegowanego (UE) nr 1271/2013, chyba że takie odstępstwo jest niezbędne ze względu na szczególne wymogi działalności Agencji i uzyskano uprzednią zgodę Komisji.

Artykuł 50

Zwalczanie nadużyć finansowych

1. W celu zwalczania nadużyć finansowych, korupcji i innych bezprawnych działań zastosowanie ma rozporządzenie (UE, Euratom) nr 883/2013 i rozporządzenie (UE) 2017/1939.

2. Agencja przystępuje do Porozumienia międzyinstytucjonalnego z dnia 25 maja 1999 r. dotyczącego dochodzeń wewnętrznych prowadzonych przez Europejski Urząd ds. Zwalczania Nadużyć Finansowych (OLAF) oraz niezwłocznie przyjmuje odpowiednie przepisy mające zastosowanie do wszystkich pracowników Agencji, z wykorzystaniem wzoru określonego w załączniku do tego porozumienia.

3. Trybunał Obrachunkowy jest uprawniony do audytu, na podstawie dokumentów oraz na miejscu, wszystkich beneficjentów dotacji, wykonawców i podwykonawców, którzy otrzymali od Agencji unijne środki finansowe.

4. OLAF może przeprowadzać dochodzenia, w tym kontrole i inspekcje na miejscu, zgodnie z przepisami i procedurami określonymi w rozporządzeniu (UE, Euratom) nr 883/2013 i w rozporządzeniu Rady (Euratom, WE) nr 2185/96 ([1]) w celu ustalenia, czy miało miejsce nadużycie finansowe, korupcja lub jakiekolwiek inne działanie niezgodne z prawem, wpływające na interesy finansowe Unii w związku z dotacją lub zamówieniem finansowanym przez Agencję.

5. Bez uszczerbku dla ust. 1, 2, 3 i 4, zamówienia, umowy o udzielenie dotacji i decyzje Agencji o udzieleniu dotacji zawierają postanowienia wyraźnie upoważniające Trybunał Obrachunkowy, OLAF i Prokuraturę Europejską do prowadzenia audytów i dochodzeń, zgodnie z kompetencjami każdego z nich.

ROZDZIAŁ VI

ZMIANY W INNYCH UNIJNYCH AKTACH PRAWNYCH

Artykuł 51

Zmiana w rozporządzeniu (WE) nr 1987/2006

W rozporządzeniu (WE) nr 1987/2006 art. 15 ust. 2 i 3 otrzymują brzmienie:

„2. Organ zarządzający jest odpowiedzialny za realizację wszystkich zadań związanych z infrastrukturą łączności, w szczególności za:

a) nadzór;

b) bezpieczeństwo;

c) koordynację stosunków między państwami członkowskimi a dostawcą usług;

d) zadania związane z wykonywaniem budżetu;

e) nabywanie i odnawianie;

f) kwestie dotyczące umów.”.

Artykuł 52

Zmiana w decyzji Rady 2007/533/WSiSW

W decyzji Rady 2007/533/WSiSW art. 15 ust. 2 i 3 otrzymują brzmienie:

„2. Organ zarządzający jest także odpowiedzialny za realizację wszystkich zadań związanych z infrastrukturą łączności, w szczególności za:

a) nadzór;

b) bezpieczeństwo;

c) koordynację stosunków między państwami członkowskimi a dostawcą usług;

d) zadania związane z wykonywaniem budżetu;

e) nabywanie i odnawianie;

f) kwestie dotyczące umów.”.

ROZDZIAŁ VII

PRZEPISY PRZEJŚCIOWE

Artykuł 53

Następstwo prawne

1. Agencja ustanowiona niniejszym rozporządzeniem jest następcą prawnym w odniesieniu do wszystkich umów zawartych przez Europejską Agencję ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości ustanowioną rozporządzeniem (UE) nr 1077/2011, ciążących na niej zobowiązań i nabytego przez nią majątku.

([1]) Rozporządzenie Rady (Euratom, WE) nr 2185/96 z dnia 11 listopada 1996 r. w sprawie kontroli na miejscu oraz inspekcji przeprowadzanych przez Komisję w celu ochrony interesów finansowych Wspólnot Europejskich przed nadużyciami finansowymi i innymi nieprawidłowościami (Dz.U. L 292 z 15.11.1996, s. 2).

2. Niniejsze rozporządzenie nie wpływa na moc prawną umów, porozumień roboczych i protokołów ustaleń zawartych przez agencję ustanowioną rozporządzeniem (UE) nr 1077/2011, z zastrzeżeniem wszelkich zmian wprowadzonych do tych umów, porozumień roboczych i protokołów na mocy niniejszego rozporządzenia.

Artykuł 54

Przepisy przejściowe dotyczące zarządu i grup doradczych

1. Członkowie oraz przewodniczący i zastępca przewodniczącego zarządu, powołani na podstawie odpowiednio art. 13 i 14 rozporządzenia (UE) nr 1077/2011, pełnią nadal obowiązki przez pozostały okres swoich kadencji.

2. Członkowie, przewodniczący i zastępcy przewodniczących grup doradczych, powołani na podstawie art. 19 rozporządzenia (UE) nr 1077/2011, pełnią nadal obowiązki przez pozostały okres swoich kadencji.

Artykuł 55

Utrzymanie w mocy przepisów wewnętrznych przyjętych przez zarząd

Wewnętrzne przepisy i środki przyjęte przez zarząd na podstawie rozporządzenia (UE) nr 1077/2011 pozostają w mocy po dniu 11 grudnia 2018 r., z zastrzeżeniem wszelkich wprowadzonych do nich zmian wymaganych na mocy niniejszego rozporządzenia.

Artykuł 56

Przepisy przejściowe dotyczące dyrektora wykonawczego

Dyrektor wykonawczy Europejskiej Agencji ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości, powołany na podstawie art. 18 rozporządzenia (UE) nr 1077/2011, przez pozostały okres swojej kadencji wykonuje obowiązki dyrektora wykonawczego Agencji, jak przewidziano w art. 24 niniejszego rozporządzenia. Pozostałe warunki zawartej z nim umowy pozostają bez zmian. Jeżeli decyzja w sprawie przedłużenia mandatu dyrektora wykonawczego zgodnie z art. 18 ust. 4 rozporządzenia (UE) nr 1077/2011 zostanie przyjęta przed 11 grudnia 2018 r., mandat zostaje automatycznie przedłużony do dnia 31 października 2022 r.

ROZDZIAŁ VIII

PRZEPISY KOŃCOWE

Artykuł 57

Zastąpienie i uchylenie

Rozporządzenie (UE) nr 1077/2011 zostaje niniejszym zastąpione w odniesieniu do państw członkowskich związanych niniejszym rozporządzeniem.

Niniejszym uchyla się rozporządzenie (UE) nr 1077/2011.

W odniesieniu do państw członkowskich związanych niniejszym rozporządzeniem odesłania do uchylonego rozporządzenia traktuje się jako odesłania do niniejszego rozporządzenia i odczytuje się zgodnie z tabelą korelacji zawartą w załączniku do niniejszego rozporządzenia.

Artykuł 58

Wejście w życie i stosowanie

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

Niniejsze rozporządzenie stosuje się od dnia 11 grudnia 2018 r. Jednakże art. 19 ust. 1 lit. x), art. 24 ust. 3 lit. h) i i) oraz art. 50 ust. 5 niniejszego rozporządzenia, o ile odnoszą się one do Prokuratury Europejskiej, oraz art. 50 ust. 1 niniejszego rozporządzenia, o ile odnosi się on do rozporządzenia (UE) 2017/1939, stosuje się od daty wyznaczonej w decyzji Komisji, przewidzianej w art. 120 ust. 2 akapit drugi rozporządzenia 2017/1939.

Niniejsze rozporządzenie wiąże w całości i jest bezpośrednio stosowane w państwach członkowskich zgodnie z Traktatami.

Sporządzono w Strasburgu dnia 14 listopada 2018 r.

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

ZAŁĄCZNIK

TABELA KORELACJI

Rozporządzenie (UE) nr 1077/2011	Niniejsze rozporządzenie
art. 1 ust. 1	art. 1 ust. 1
—	art. 1 ust. 2
art. 1 ust. 2	art. 1 ust. 3 i 4
art. 1 ust. 3	art. 1 ust. 5
art. 1 ust. 4	art. 1 ust. 6
art. 2	art. 2
art. 3	art. 3
art. 4	art. 4
art. 5	art. 5
art. 5a	art. 6
—	art. 7
—	art. 8
art. 6	art. 9
—	art. 10
art. 7 ust. 1 i 2	art. 11 ust. 1
art. 7 ust. 3	art. 11 ust. 2
art. 7 ust. 4	art. 11 ust. 3
art. 7 ust. 5	art. 11 ust. 4
art. 7 ust. 6	art. 11 ust. 5
—	art. 12
—	art. 13
art. 8 ust. 1	art. 14 ust. 1
—	art. 14 ust. 2
art. 8 ust. 2	art. 14 ust. 3
art. 9 ust. 1 i 2	art. 15 ust. 1 i 2
—	art. 15 ust. 3
—	art. 15 ust. 4
—	art. 16
art. 10 ust. 1 i 2	art. 17 ust. 1 i 2
art. 10 ust. 3	art. 24 ust. 2
art. 10 ust. 4	art. 17 ust. 3
—	art. 17 ust. 4
—	art. 17 ust. 5
art. 11	art. 18
art. 12 ust. 1	art. 19 ust. 1
—	art. 19 ust. 1 lit. a)

Rozporządzenie (UE) nr 1077/2011	Niniejsze rozporządzenie
—	art. 19 ust. 1 lit. b)
art. 12 ust. 1 lit. a)	art. 19 ust. 1 lit. c)
art. 12 ust. 1 lit. b)	art. 19 ust. 1 lit. d)
art. 12 ust. 1 lit. c)	art. 19 ust. 1 lit. e)
—	art. 19 ust. 1 lit. f)
art. 12 ust. 1 lit. d)	art. 19 ust. 1 lit. g)
—	art. 19 ust. 1 lit. h)
—	art. 19 ust. 1 lit. i)
—	art. 19 ust. 1 lit. j)
—	art. 19 ust. 1 lit. k)
art. 12 ust. 1 lit. e)	art. 19 ust. 1 lit. l)
—	art. 19 ust. 1 lit. m)
art. 12 ust. 1 lit. f)	art. 19 ust. 1 lit. n)
art. 12 ust. 1 lit. g)	art. 19 ust. 1 lit. o)
—	art. 19 ust. 1 lit. p)
art. 12 ust. 1 lit. h)	art. 19 ust. 1 lit. q)
art. 12 ust. 1 lit. i)	art. 19 ust. 1 lit. q)
art. 12 ust. 1 lit. j)	art. 19 ust. 1 lit. r)
—	art. 19 ust. 1 lit. s)
art. 12 ust. 1 lit. k)	art. 19 ust. 1 lit. t)
art. 12 ust. 1 lit. l)	art. 19 ust. 1 lit. u)
art. 12 ust. 1 lit. m)	art. 19 ust. 1 lit. v)
art. 12 ust. 1 lit. n)	art. 19 ust. 1 lit. w)
art. 12 ust. 1 lit. o)	art. 19 ust. 1 lit. x)
—	art. 19 ust. 1 lit. y)
art. 12 ust. 1 lit. p)	art. 19 ust. 1 lit. z)
art. 12 ust. 1 lit. q)	art. 19 ust. 1 lit. bb)
art. 12 ust. 1 lit. r)	art. 19 ust. 1 lit. cc)
art. 12 ust. 1 lit. s)	art. 19 ust. 1 lit. dd)
art. 12 ust. 1 lit. t)	art. 19 ust. 1 lit. ff)
art. 12 ust. 1 lit. u)	art. 19 ust. 1 lit. gg)
art. 12 ust. 1 lit. v)	art. 19 ust. 1 lit. hh)
art. 12 ust. 1 lit. w)	art. 19 ust. 1 lit. ii)
art. 12 ust. 1 lit. x)	art. 19 ust. 1 lit. jj)
—	art. 19 ust. 1 lit. ll)
art. 12 ust. 1 lit. y)	art. 19 ust. 1 lit. mm)
art. 12 ust. 1 lit. z)	art. 19 ust. 1 lit. nn)
—	art. 19 ust. 1 lit. oo)
art. 12 ust. 1 lit. aa)	art. 19 ust. 1 lit. pp)
art. 12 ust. 1 lit. sa)	art. 19 ust. 1 lit. ee)

Rozporządzenie (UE) nr 1077/2011	Niniejsze rozporządzenie
art. 12 ust. 1 lit. xa)	art. 19 ust. 1 lit. kk)
art. 12 ust. 1 lit. za)	art. 19 ust. 1 lit. mm)
—	art. 19 ust. 1) akapit drugi
—	art. 19 ust. 2
art. 12 ust. 2	art. 19 ust. 3
art. 13 ust. 1	art. 20 ust. 1
art. 13 ust. 2 i 3	art. 20 ust. 2
art. 13 ust. 4	art. 20 ust. 3
art. 13 ust. 5	art. 20 ust. 4
art. 14 ust. 1 i 3	art. 21 ust. 1
art. 14 ust. 2	art. 21 ust. 2
art. 15 ust. 1	art. 22 ust. 1 i 3
art. 15 ust. 2	art. 22 ust. 2
art. 15 ust. 3	art. 22 ust. 5
art. 15 ust. 4 i 5	art. 22 ust. 4
art. 15 ust. 6	art. 22 ust. 6
art. 16 ust. 1–5	art. 23 ust. 1– 5
—	art. 23 ust. 6
art. 16 ust. 6	art. 23 ust. 7
art. 16 ust. 7	art. 23 ust. 8
art. 17 ust. 1–4	art. 24 ust. 1
art. 17 ust. 2	—
art. 17 ust. 3	—
art. 17 ust. 5 i 6	art. 24 ust. 3
art. 17 ust. 5 lit. a)	art. 24 ust. 3 lit. a)
art. 17 ust. 5 lit. b)	art. 24 ust. 3 lit. b)
art. 17 ust. 5 lit. c)	art. 24 ust. 3 lit. c)
art. 17 ust. 5 lit. d)	art. 24 ust. 3 lit. o)
art. 17 ust. 5 lit. e)	art. 22 ust. 2
art. 17 ust. 5 ust. f)	art. 19 ust. 2
art. 17 ust. 5 lit. g)	art. 24 ust. 3 lit. p)
art. 17 ust. 5 lit. h)	art. 24 ust. 3 lit. q)
art. 17 ust. 6 lit. a)	art. 24 ust. 3 lit. d) i g)
art. 17 ust. 6 lit. b)	art. 24 ust. 3 lit. k)
art. 17 ust. 6 lit. c)	art. 24 ust. 3 lit. d)
art. 17 ust. 6 lit. d)	art. 24 ust. 3 lit. l)
art. 17 ust. 6 lit. e)	—
art. 17 ust. 6 lit. f)	—
art. 17 ust. 6 lit. g)	art. 24 ust. 3 lit. r)
art. 17 ust. 6 lit. h)	art. 24 ust. 3 lit. s)

Rozporządzenie (UE) nr 1077/2011	Niniejsze rozporządzenie
art. 17 ust. 6 lit. i)	art. 24 ust. 3 lit. t)
art. 17 ust. 6 lit. j)	art. 24 ust. 3 lit. v)
art. 17 ust. 6 lit. k)	art. 24 ust. 3 lit. u)
art. 17 ust. 7	art. 24 ust. 4
—	art. 24 ust. 5
art. 18	art. 25
art. 18 ust. 1	art. 25 ust. 1 i 10
art. 18 ust. 2	art. 25 ust. 2, 3 i 4
art. 18 ust. 3	art. 25 ust. 5
art. 18 ust. 4	art. 25 ust. 6
art. 18 ust. 5	art. 25 ust. 7
art. 18 ust. 6	art. 24 ust. 1
—	art. 25 ust. 8
art. 18 ust. 7	art. 25 ust. 9 i 10
—	art. 25 ust. 11
—	art. 26
art. 19	art. 27
art. 20	art. 28
art. 20 ust. 1 i 2	art. 28 ust. 1 i 2
art. 20 ust. 3	—
art. 20 ust. 4	art. 28 ust. 3
art. 20 ust. 5	art. 28 ust. 4
art. 20 ust. 6	art. 28 ust. 5
art. 20 ust. 7	art. 28 ust. 6
art. 20 ust. 8	art. 28 ust. 7
art. 21	art. 29
art. 22	art. 30
art. 23	art. 31
art. 24	art. 32
art. 25 ust. 1 i 2	art. 33 ust. 1 i 2
—	art. 33 ust. 3
art. 25 ust. 3	art. 33 ust. 4
art. 26 i 27	art. 34
art. 28 ust. 1	art. 35 ust. 1 i art. 36 ust. 2
art. 28 ust. 2	art. 35 ust. 2
—	art. 36 ust. 1
art. 29 ust. 1 i 2	art. 37 ust. 1
art. 29 ust. 3	art. 37 ust. 2
art. 30	art. 38

Rozporządzenie (UE) nr 1077/2011	Niniejsze rozporządzenie
art. 31 ust. 1	art. 39 ust. 1
art. 31 ust. 2	art. 39 ust. 1 i 3
—	art. 39 ust. 2
—	art. 40
—	art. 41
—	art. 43
—	art. 44
art. 32 ust. 1	art. 46 ust. 3
art. 32 ust. 2	art. 46 ust. 4
art. 32 ust. 3	art. 46 ust. 2
art. 32 ust. 4	art. 45 ust. 2
art. 32 ust. 5	art. 45 ust. 2
art. 32 ust. 6	art. 44 ust. 2
art. 32 ust. 7	art. 45 ust. 3
art. 32 ust. 8	art. 45 ust. 4
art. 32 ust. 9	art. 45 ust. 5 i 6
art. 32 ust. 10	art. 45 ust. 7
art. 32 ust. 11	art. 45 ust. 8
art. 32 ust. 12	art. 45 ust. 9
art. 33 ust. 1–4	art. 47 ust. 1–4
—	art. 47 ust. 5
art. 33 ust. 5	art. 47 ust. 6
art. 33 ust. 6	art. 47 ust. 7
art. 33 ust. 7	art. 47 ust. 8
art. 33 ust. 8	art. 47 ust. 9
art. 33 ust. 9	art. 47 ust. 10
art. 33 ust. 10	art. 47 ust. 11
art. 33 ust. 11	art. 47 ust. 12
—	art. 48
art. 34	art. 49
art. 35 ust. 1 i 2	art. 50 ust. 1 i 2
—	art. 50 ust. 3
art. 35 ust. 3	art. 50 ust. 4 i 5
art. 36	—
art. 37	art. 42
—	art. 51
—	art. 52
—	art. 53
—	art. 54

Rozporządzenie (UE) nr 1077/2011	Niniejsze rozporządzenie
—	art. 55
—	art. 56
—	art. 57
art. 38	art. 58
—	załącznik

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2018/1727

z dnia 14 listopada 2018 r.

w sprawie Agencji Unii Europejskiej ds. Współpracy Wymiarów Sprawiedliwości w Sprawach Karnych (Eurojust) oraz zastąpienia i uchylenia decyzji Rady 2002/187/WSiSW

PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 85,

uwzględniając wniosek Komisji Europejskiej,

po przekazaniu projektu aktu ustawodawczego parlamentom narodowym,

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą ([1]),

a także mając na uwadze, co następuje:

(1) Eurojust został ustanowiony decyzją Rady 2002/187/WSiSW ([2]) jako organ Unii mający osobowość prawną, którego zadaniem jest stymulowanie i poprawa koordynacji i współpracy między właściwymi organami sądowymi państw członkowskich, szczególnie w odniesieniu do poważnej przestępczości zorganizowanej. Ramy prawne Eurojustu zmieniono decyzjami Rady 2003/659/WSiSW ([3]) i 2009/426/WSiSW ([4]).

(2) Art. 85 Traktatu o funkcjonowaniu Unii Europejskiej („TFUE") stanowi, że Eurojust działa na podstawie rozporządzenia przyjmowanego zgodnie ze zwykłą procedurą ustawodawczą. Artykuł ten wymaga także określenia warunków uczestnictwa Parlamentu Europejskiego i parlamentów narodowych w ocenie działalności Eurojustu.

(3) Artykuł 85 TFUE stanowi również, że zadaniem Eurojustu jest wspieranie oraz wzmacnianie koordynacji i współpracy między krajowymi organami śledczymi i organami ścigania w odniesieniu do poważnej przestępczości, która dotyka dwóch lub więcej państw członkowskich lub która wymaga wspólnego ścigania, w oparciu o operacje przeprowadzane i informacje dostarczane przez organy państw członkowskich i Agencję Unii Europejskiej ds. Współpracy Organów Ścigania (Europol).

(4) Celem niniejszego rozporządzenia jest zmiana i rozszerzenie przepisów decyzji 2002/187/WSiSW. Biorąc pod uwagę znaczną liczbę i istotny charakter zmian, które należy wprowadzić, decyzja 2009/426/WSiSW powinna przez wzgląd na jasność zostać zastąpiona w całości w odniesieniu do państw członkowskich związanych niniejszym rozporządzeniem.

(5) Ponieważ Prokuratura Europejska została utworzona w drodze wzmocnionej współpracy, rozporządzenie Rady (UE) 2017/1939 ([5]) jest wiążące w całości dla państw członkowskich biorących udział we wzmocnionej współpracy i tylko w nich jest bezpośrednio stosowane. W związku z tym dla państw członkowskich, które nie uczestniczą w Prokuraturze Europejskiej, Eurojust pozostaje w pełni właściwy w sprawach dotyczących form poważnej przestępczości wymienionych w załączniku I do niniejszego rozporządzenia.

(6) Artykuł 4 ust. 3 Traktatu o Unii Europejskiej (TUE) przywołuje zasadę lojalnej współpracy, zgodnie z którą Unia i państwa członkowskie wzajemnie się szanują i udzielają sobie wzajemnego wsparcia w wykonywaniu zadań wynikających z TUE i TFUE.

(7) W celu ułatwienia współpracy między Eurojustem i Prokuraturą Europejską Eurojust powinien w razie konieczności rozpatrywać sprawy istotne dla Prokuratury Europejskiej.

(8) Mając na uwadze ustanowienie Prokuratury Europejskiej w drodze wzmocnionej współpracy, należy jasno określić podział właściwości między Prokuraturą Europejską a Eurojustem w odniesieniu do przestępstw mających wpływ na interesy finansowe Unii. Począwszy od dnia rozpoczęcia wykonywania obowiązków przez Prokuraturę Europejską Eurojust powinien być w stanie wykonywać swoją właściwość w sprawach dotyczących przestępstw, w przypadku których właściwa jest Prokuratura Europejska, jeżeli przestępstwa te dotyczą zarówno państw członkowskich, które uczestniczą we wzmocnionej współpracy w zakresie ustanowienia Prokuratury Europejskiej, jak i państw

([1]) Stanowisko Parlamentu Europejskiego z dnia 4 października 2018 r. (dotychczas nieopublikowane w Dzienniku Urzędowym) oraz decyzja Rady z dnia 6 listopada 2018 r.

([2]) Decyzja Rady 2002/187/WSiSW z dnia 28 lutego 2002 r. ustanawiająca Eurojust w celu zintensyfikowania walki z poważną przestępczością (Dz.U. L 63 z 6.3.2002, s. 1).

([3]) Decyzja Rady 2003/659/WSiSW z dnia 18 czerwca 2003 r. zmieniająca decyzję 2002/187/WSiSW ustanawiającą Eurojust w celu zintensyfikowania walki z poważną przestępczością (Dz.U. L 245 z 29.9.2003, s. 44.)

([4]) Decyzja Rady 2009/426/WSiSW z dnia 16 grudnia 2008 r. w sprawie wzmocnienia Eurojustu i w sprawie zmiany decyzji 2002/187/WSiSW ustanawiającej Eurojust w celu zintensyfikowania walki z poważną przestępczością (Dz.U. L 138 z 4.6.2009, s. 14).

([5]) 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).

członkowskich, które w takiej współpracy nie uczestniczą. W takich przypadkach Eurojust powinien działać na wniosek nieuczestniczących państw członkowskich lub na wniosek Prokuratury Europejskiej. W każdym przypadku Eurojust powinien pozostać właściwy w sprawach dotyczących przestępstw mających wpływ na interesy finansowe Unii, które pozostają poza zakresem właściwości Prokuratury Europejskiej, lub gdy Prokuratura Europejska jest wprawdzie właściwa, lecz nie wykonuje swojej właściwości. Państwa członkowskie, które nie uczestniczą we wzmocnionej współpracy w zakresie ustanowienia Prokuratury Europejskiej, mogą nadal zwracać się do Eurojustu o wsparcie we wszystkich sprawach związanych z przestępstwami mającymi wpływ na interesy finansowe Unii. Prokuratura Europejska i Eurojust powinny rozwijać ścisłą współpracę operacyjną zgodnie z ich zakresami działania.

(9) Aby Eurojust mógł wypełniać swoją misję i rozwijać pełny potencjał w walce z poważną przestępczością transgraniczną, należy wzmocnić jego funkcje operacyjne poprzez zmniejszenie obciążeń administracyjnych przedstawicieli krajowych oraz rozszerzyć jego wymiar europejski poprzez udział Komisji w zarządzie i zwiększone uczestnictwo Parlamentu Europejskiego i parlamentów narodowych w ocenie jego działalności.

(10) W związku z tym niniejsze rozporządzenie powinno określać warunki uczestnictwa parlamentów, przewidując modernizację struktury i uproszczenie obecnych ram prawnych Eurojustu, przy jednoczesnym zachowaniu tych elementów, które okazały się skuteczne w jego funkcjonowaniu.

(11) Należy jasno określić wchodzące w zakres właściwości Eurojustu formy poważnej przestępczości, która dotyka co najmniej dwóch państw członkowskich. Ponadto należy zdefiniować sprawy, które nie dotyczą co najmniej dwóch państw członkowskich, ale które wymagają wspólnego ścigania. Takie przypadki mogą obejmować postępowania przygotowawcze oraz wnoszenie i popieranie oskarżeń dotyczące tylko jednego państwa członkowskiego i państwa trzeciego, w przypadku gdy została zawarta umowa z państwem trzecim lub gdy może istnieć szczególna potrzeba zaangażowania się Eurojustu. Takie ściganie może również dotyczyć przypadków, które dotyczą jednego państwa członkowskiego i mają następstwa na poziomie Unii.

(12) W ramach wykonywania swoich funkcji operacyjnych w odniesieniu do konkretnych spraw karnych Eurojust powinien działać, na wniosek właściwych organów państw członkowskich lub z własnej inicjatywy, za pośrednictwem co najmniej jednego przedstawiciela krajowego albo jako kolegium. Działając z własnej inicjatywy, Eurojust może przyjąć bardziej proaktywną rolę w koordynowaniu spraw, na przykład przez wspieranie organów krajowych w prowadzonych przez nie postępowaniach przygotowawczych oraz wnoszonych i popieranych oskarżeniach. Może to obejmować angażowanie państw członkowskich, które mogły początkowo nie zostać włączone w daną sprawę, oraz odkrywanie powiązań między sprawami na podstawie informacji otrzymanych od Europolu, Europejskiego Urzędu ds. Zwalczania Nadużyć finansowych (OLAF), Prokuratury Europejskiej i organów krajowych. Ponadto pozwala to Eurojustowi opracowywać w ramach jego prac strategicznych wytyczne, dokumenty strategiczne i analizy dotyczące prowadzonych przez niego spraw.

(13) Na wniosek właściwego organu danego państwa członkowskiego lub na wniosek Komisji Eurojust powinien także móc udzielać pomocy w postępowaniach przygotowawczych dotyczących tylko tego państwa członkowskiego, lecz mających następstwa na poziomie Unii. Takie postępowania przygotowawcze obejmują przykładowo sprawy, które dotyczą pracownika instytucji lub organu Unii. Obejmują one także sprawy, które dotyczą znacznej liczby państw członkowskich i mogłyby ewentualnie wymagać skoordynowanej reakcji na poziomie europejskim.

(14) Pisemne opinie Eurojustu nie są wiążące dla państw członkowskich, ale powinno się udzielić na nie odpowiedzi zgodnie z niniejszym rozporządzeniem.

(15) W celu zapewnienia, że Eurojust może odpowiednio wspierać i koordynować transgraniczne postępowania przygotowawcze, konieczne jest zapewnienie wszystkim przedstawicielom krajowym niezbędnych uprawnień operacyjnych w odniesieniu do ich państw członkowskich i zgodnie z prawem tych państw członkowskich, by mogli w sposób bardziej spójny i efektywny współpracować między sobą oraz z organami krajowymi. Przedstawicielom krajowym należy przyznać takie uprawnienia, które umożliwią Eurojustowi właściwe realizowanie jego misji. Uprawnienia te powinny obejmować dostęp do istotnych informacji znajdujących się w krajowych rejestrach publicznych, bezpośrednie kontaktowanie się z właściwymi organami i wymianę informacji z nimi oraz udział we wspólnych zespołach dochodzeniowo-śledczych. Przedstawiciele krajowi mogą, zgodnie ze swoim prawem krajowym, zachować uprawnienia przysługujące im jako organom krajowym. W porozumieniu z właściwym organem krajowym lub w nagłych przypadkach przedstawiciele krajowi mogą również nakazywać podjęcie czynności dochodzeniowo-śledczych i zastosowanie przesyłek niejawnie nadzorowanych, a także wydawać i wykonywać wnioski o wzajemną pomoc prawną lub wnioski o wzajemne uznanie. Ponieważ uprawnienia te mają być wykonywane zgodnie z prawem krajowym, sądy państw członkowskich są właściwe do kontroli sądowej tych środków, zgodnie z wymogami i procedurami ustanowionymi w prawie krajowym.

(16) Konieczne jest zapewnienie Eurojustowi struktury administracyjnej i kierowniczej, która umożliwi mu skuteczniejszą realizację zadań, będzie zgodna z zasadami mającymi zastosowanie do agencji Unii oraz będzie w pełni zgodna z podstawowymi prawami i wolnościami, przy jednoczesnym zachowaniu specyfiki Eurojustu i zagwarantowaniu jego niezależności w wykonywaniu funkcji operacyjnych. W tym celu należy sprecyzować funkcje przedstawicieli krajowych, kolegium i dyrektora administracyjnego oraz ustanowić zarząd.

(17) Należy ustanowić przepisy w celu wyraźnego rozróżnienia wykonywanych przez kolegium funkcji operacyjnych i kierowniczych, co przyczyni się do ograniczenia do minimum obciążenia administracyjnego przedstawicieli krajowych, tak aby położyć nacisk na pracę operacyjną Eurojustu. Zadania kolegium w zakresie zarządzania

powinny obejmować w szczególności przyjmowanie programów prac Eurojustu, budżetu, rocznego sprawozdania z działalności oraz uzgodnień roboczych z partnerami. Kolegium powinno wykonywać uprawnienia organu powołującego w odniesieniu do dyrektora administracyjnego. Ponadto kolegium powinno przyjąć regulamin wewnętrzny Eurojustu. Ponieważ regulamin ten może mieć wpływ na działanie wymiarów sprawiedliwości w państwach członkowskich, należy powierzyć Radzie uprawnienia wykonawcze do jego zatwierdzania.

(18) W celu usprawnienia zarządzania Eurojustem i procedur należy ustanowić zarząd, który będzie wspierać kolegium w jego funkcjach kierowniczych i umożliwiać sprawniejsze podejmowanie decyzji w kwestiach nieoperacyjnych i strategicznych.

(19) Komisja powinna być reprezentowana w kolegium podczas wykonywania przez kolegium funkcji kierowniczych. Aby zapewnić nieoperacyjny nadzór nad Eurojustem i strategiczne kierowanie tą agencją, przedstawiciel Komisji w kolegium powinien być także jej przedstawicielem w zarządzie.

(20) W celu zapewnienia skutecznego bieżącego zarządzania Eurojustem dyrektor administracyjny powinien być jego przedstawicielem prawnym i kierownikiem, odpowiadającym przed kolegium. Dyrektor administracyjny powinien przygotowywać i wdrażać decyzje kolegium i zarządu. Dyrektora administracyjnego powinno się powoływać w oparciu o osiągnięcia i udokumentowane umiejętności w zakresie administracji i zarządzania, a także odpowiednie kompetencje i doświadczenie.

(21) Kolegium powinno wybrać spośród przedstawicieli krajowych przewodniczącego i dwóch wiceprzewodniczących Eurojustu na czteroletnią kadencję. Gdy przedstawiciel krajowy zostaje wybrany na stanowisko przewodniczącego, dane państwo członkowskie powinno mieć możliwość oddelegowania do biura krajowego innej odpowiednio wykwalifikowanej osoby i złożenia wniosku o rekompensatę z budżetu Eurojustu.

(22) Osoby odpowiednio wykwalifikowane to osoby posiadające kwalifikacje i doświadczenie niezbędne do wykonywania zadań wymaganych do zapewnienia skutecznego działania biura krajowego. Osoby takie mogą mieć status zastępcy lub asystenta przedstawiciela krajowego wybranego na przewodniczącego lub mogą pełnić funkcję o charakterze bardziej administracyjnym lub technicznym. Każde państwo członkowskie powinno mieć możliwość decydowania o własnych wymogach w tym względzie.

(23) W regulaminie Eurojustu należy uregulować kwestie kworum i procedury głosowania. W wyjątkowych sytuacjach, w przypadku nieobecności przedstawiciela krajowego lub jego zastępcy, asystent danego przedstawiciela krajowego powinien być uprawniony do głosowania w kolegium, jeżeli asystent taki ma status funkcjonariusza wymiaru sprawiedliwości, tj. prokuratora, sędziego lub przedstawiciela organu sądowego.

(24) Ponieważ mechanizm rekompensaty wywołuje skutki dla budżetu, niniejsze rozporządzenie powinno powierzyć Radzie uprawnienia wykonawcze do określenia tego mechanizmu.

(25) W strukturach Eurojustu należy utworzyć dyżurny mechanizm koordynacyjny, by zapewnić większą skuteczność Eurojustu oraz możliwość interwencji Eurojustu w nagłych przypadkach przez całą dobę. Każde państwo członkowskie powinno zapewnić, aby jego przedstawiciele w ramach dyżurnego mechanizmu koordynacyjnego byli gotowi do działania przez całą dobę we wszystkie dni tygodnia.

(26) W państwach członkowskich powinny zostać utworzone krajowe systemy koordynacyjne Eurojustu, które będą koordynować działania krajowych korespondentów Eurojustu, krajowego korespondenta Eurojustu do spraw terroryzmu, każdego krajowego korespondenta do spraw kwestii związanych z właściwością Prokuratury Europejskiej, krajowego korespondenta Europejskiej Sieci Sądowej oraz maksymalnie trzech innych punktów kontaktowych, a także przedstawicieli sieci wspólnych zespołów dochodzeniowo-śledczych oraz przedstawicieli sieci utworzonych decyzjami Rady 2002/494/WSiSW ([1]), 2007/845/WSiSW ([2]) oraz 2008/852/WSiSW ([3]). Państwa członkowskie mogą zadecydować, że co najmniej jedno z tych zadań jest wykonywane przez tego samego krajowego korespondenta.

(27) Do celów stymulowania i wzmacniania koordynacji i współpracy między krajowymi organami prowadzącymi postępowania przygotowawcze i organami właściwymi w zakresie wnoszenia i popierania oskarżeń niezwykle istotne jest, aby Eurojust otrzymywał od organów krajowych informacje niezbędne do wykonywania jego zadań.

([1]) Decyzja Rady 2002/494/WSiSW z dnia 13 czerwca 2002 r. ustanawiająca europejską sieć punktów kontaktowych dotyczących osób odpowiedzialnych za ludobójstwo, zbrodnie przeciw ludzkości oraz zbrodnie wojenne (Dz.U. L 167 z 26.6.2002, s. 1).

([2]) Decyzja Rady 2007/845/WSiSW z dnia 6 grudnia 2007 r. dotyczącą współpracy pomiędzy biurami ds. odzyskiwania mienia w państwach członkowskich w dziedzinie wykrywania i identyfikacji korzyści pochodzących z przestępstwa lub innego mienia związanego z przestępstwem (Dz.U. L 332 z 18.12.2007, s. 103).

([3]) Decyzja Rady 2008/852/WSiSW z dnia 24 października 2008 r. w sprawie sieci punktów kontaktowych służącej zwalczaniu korupcji (Dz.U. L 301 z 12.11.2008, s. 38).

W tym celu właściwe organy krajowe powinny bez zbędnej zwłoki informować swoich przedstawicieli krajowych o utworzeniu wspólnych zespołów dochodzeniowo-śledczych i osiąganych przez nie wynikach. Właściwe organy krajowe powinny również bez zbędnej zwłoki informować przedstawicieli krajowych o wchodzących w zakres właściwości Eurojustu sprawach, które dotyczą bezpośrednio co najmniej trzech państw członkowskich i w odniesieniu do których wnioski lub decyzje dotyczące współpracy wymiarów sprawiedliwości zostały przekazane do co najmniej dwóch państw członkowskich. W niektórych okolicznościach powinny one również informować przedstawicieli krajowych o konfliktach jurysdykcji, przesyłkach niejawnie nadzorowanych oraz powtarzających się trudnościach we współpracy wymiarów sprawiedliwości.

(28) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 ([1]) zawiera zharmonizowane zasady ochrony i swobodnego przepływu danych osobowych przetwarzanych do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w tym do ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom. Aby zapewnić identyczny stopień ochrony osób fizycznych w całej Unii za pomocą praw możliwych do wyegzekwowania na drodze prawnej oraz zapobiegać rozbieżnościom utrudniającym wymianę danych osobowych między Eurojustem i właściwymi organami w państwach członkowskich, przepisy dotyczące ochrony i swobodnego przepływu operacyjnych danych osobowych przetwarzanych przez Eurojust powinny być spójne z dyrektywą (UE) 2016/680.

(29) Przepisy ogólne odrębnego rozdziału rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725 ([2]) dotyczące przetwarzania operacyjnych danych osobowych powinny mieć zastosowanie z zastrzeżeniem przepisów szczegółowych dotyczących ochrony danych, zawartych w niniejszym rozporządzeniu. Te przepisy szczegółowe należy postrzegać jako *lex specialis* w stosunku do przepisów zawartych w rozdziale rozporządzenia (UE) 2018/1725 (*lex specialis derogat legi generali*). Aby zmniejszyć fragmentaryzację przepisów, szczegółowe przepisy dotyczące ochrony danych zawarte w niniejszym rozporządzeniu powinny być spójne z zasadami leżącymi u podstaw tego rozdziału rozporządzenia (UE) 2018/1725, a także z przepisami tego rozporządzenia odnoszącymi się do niezależnego nadzoru, środków ochrony prawnej, odpowiedzialności i sankcji.

(30) Ochrona praw i wolności osób, których dane dotyczą, wymaga wprowadzenia jasnego podziału odpowiedzialności za ochronę danych osobowych na mocy niniejszego rozporządzenia. Państwa członkowskie powinny być odpowiedzialne za prawidłowość i aktualizację danych przekazanych przez nie do Eurojustu i przetworzonych przez Eurojust w niezmienionej postaci oraz za zgodność z prawem takiego przekazania danych do Eurojustu. Eurojust powinien być odpowiedzialny za prawidłowość i aktualizację danych dostarczanych przez inne podmioty dostarczające danych lub danych pochodzących z własnych analiz lub gromadzonych przez Eurojust. Eurojust powinien zapewniać, by dane były przetwarzane rzetelnie i zgodnie z prawem oraz by były gromadzone i przetwarzane w konkretnym celu. Eurojust powinien również zapewniać, by dane były prawidłowe, odpowiednie, proporcjonalne w stosunku do celu, w jakim są przetwarzane, przechowywane przez czas nie dłuższy niż jest to niezbędne do tego celu, a także by były przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych oraz poufność przetwarzania danych.

(31) Regulamin wewnętrzny Eurojustu powinien zawierać odpowiednie zabezpieczenia w odniesieniu do przechowywania operacyjnych danych osobowych do celów archiwalnych w interesie publicznym lub do celów statystycznych.

(32) Osoba, której dane dotyczą, powinna mieć możliwość skorzystania z prawa do dostępu, o którym mowa w rozporządzeniu (UE) 2018/1725, do swoich operacyjnych danych osobowych przetwarzanych przez Eurojust. Osoba, której dane dotyczą, może bezpłatnie składać w tej sprawie wnioski w rozsądnych odstępach czasu do Eurojustu lub do krajowego organu nadzorczego w wybranym przez siebie państwie członkowskim.

(33) Zawarte w niniejszym rozporządzeniu przepisy o ochronie danych mają zastosowanie z zastrzeżeniem obowiązujących przepisów dotyczących dopuszczalności danych osobowych w charakterze dowodów w postępowaniach przygotowawczych i postępowaniach sądowych w sprawach karnych.

(34) Wszelkie przetwarzanie danych osobowych przez Eurojust w zakresie jego właściwości w celu wykonywania spoczywających na nim zadań powinno być uważane za przetwarzanie operacyjnych danych osobowych.

(35) Ponieważ Eurojust przetwarza również dane administracyjne, niezwiązane z postępowaniami przygotowawczymi, przetwarzanie takich danych powinno podlegać przepisom ogólnym rozporządzenia (UE) 2018/1725.

([1]) 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).

([2]) 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 (zob. s. 39 niniejszego Dziennika Urzędowego).

(36) Jeżeli operacyjne dane osobowe są przekazywane lub dostarczane Eurojustowi przez państwo członkowskie, właściwy organ, przedstawiciel krajowy lub korespondent krajowy Eurojustu powinni mieć prawo żądania sprostowania lub usunięcia takich operacyjnych danych osobowych.

(37) Dla zachowanie zgodności z niniejszym rozporządzeniem, Eurojust lub upoważniony podmiot przetwarzający powinni prowadzić wykazy wszystkich kategorii czynności przetwarzania danych osobowych, za które są odpowiedzialni. Eurojust i każdy upoważniony podmiot przetwarzający powinni mieć obowiązek współpracy z Europejskim Inspektorem Ochrony Danych („EIOD") i udostępniania na jego żądanie takich wykazów w celu monitorowania tych operacji przetwarzania. Eurojust lub jego upoważniony podmiot przetwarzający dane osobowe w niezautomatyzowanych systemach przetwarzania powinni dysponować skutecznymi metodami, takimi jak ewidencja lub inne formy zapisu, pozwalającymi wykazać zgodność przetwarzania danych z prawem, monitorować własną działalność i zapewniać integralność i bezpieczeństwo danych.

(38) Zarząd Eurojustu powinien wyznaczyć inspektora ochrony danych spośród członków dotychczasowego personelu. Osoba wyznaczona na stanowisko inspektora ochrony danych w Eurojuście powinna być po odbyciu specjalnego szkolenia z zakresu prawa ochrony danych oraz praktyki w zdobywaniu wiedzy fachowej w tej dziedzinie. Niezbędny poziom wiedzy fachowej należy ustalić w świetle prowadzonych operacji przetwarzania danych oraz ochrony, której wymagają dane osobowe przetwarzane przez Eurojust.

(39) EIOD jest odpowiedzialny za monitorowanie i zapewnienie pełnego stosowania przepisów niniejszego rozporządzenia odnoszących się do przetwarzania operacyjnych danych osobowych przez Eurojust. Należy przyznać EIOD uprawnienia pozwalające mu na skuteczne wykonywanie swych obowiązków. EIOD powinien mieć prawo konsultowania się z Eurojustem w związku ze złożonymi wnioskami, przekazywania spraw do Eurojustu w celu rozwiązania problemów wynikłych podczas przetwarzania przezeń operacyjnych danych osobowych, występowania z propozycjami poprawy ochrony osób, których dane dotyczą oraz nakazywania Eurojustowi przeprowadzania specjalnych czynności dotyczących przetwarzania operacyjnych danych osobowych. W rezultacie EIOD potrzebuje środków zapewniających wykonanie tych nakazów i ich egzekwowanie. EIOD powinien w związku z tym mieć uprawnienia do ostrzegania Eurojustu. Przez ostrzeżenie należy rozumieć ustne lub pisemne przypomnienie o obowiązku Eurojustu wykonania nakazów EIOD lub podporządkowania się propozycjom EIOD oraz przypomnienie dotyczące środków, jakie zostaną zastosowane w razie niepodporządkowania się lub odmowy ze strony Eurojustu.

(40) Obowiązki i uprawnienia EIOD, w tym uprawnienie do nakazania Eurojustowi sprostowania, ograniczenia przetwarzania lub usunięcia operacyjnych danych osobowych, które zostały przetworzone z naruszeniem przepisów niniejszego rozporządzenia dotyczących ochrony danych, nie powinny obejmować danych osobowych zawartych w krajowych aktach sprawy.

(41) W celu ułatwienia współpracy między EIOD a krajowymi organami nadzorczymi, lecz bez uszczerbku dla niezależności EIOD i jego odpowiedzialności za nadzór nad Eurojustem w zakresie ochrony danych, EIOD i krajowe organy nadzorcze powinny odbywać regularne spotkania w ramach Europejskiej Rady Ochrony Danych, zgodnie z przepisami w sprawie skoordynowanego nadzoru zawartymi w rozporządzeniu (UE) 2018/1725.

(42) Będąc pierwszym na terytorium Unii odbiorcą danych dostarczonych przez państwa trzecie lub organizacje międzynarodowe bądź uzyskanych od nich, Eurojust powinien być odpowiedzialny za prawidłowość tych danych. Eurojust powinien podjąć środki do możliwie najdogłębniejszego sprawdzania prawidłowości danych w momencie ich otrzymywania lub udostępniania innym organom.

(43) Eurojust powinien podlegać przepisom ogólnym dotyczącym odpowiedzialności umownej i pozaumownej, obowiązującym instytucje, organy i jednostki organizacyjne Unii.

(44) Eurojust powinien mieć możliwość wymiany odpowiednich danych osobowych i prowadzenia współpracy z innymi instytucjami, organami i jednostkami organizacyjnymi Unii w zakresie koniecznym do wykonywania jego lub ich zadań.

(45) Z myślą o zagwarantowaniu przestrzegania zasady celowości ważne jest zapewnienie, by Eurojust mógł przekazywać dane osobowe państwom trzecim i organizacjom międzynarodowym tylko wtedy, gdy jest to niezbędne do zapobiegania przestępczości objętej zadaniami Eurojustu i zwalczania jej. W tym celu należy zapewnić, by w przypadku przekazywania danych osobowych odbiorca zobowiązywał się do wykorzystywania tych danych lub ich dalszego przekazywania właściwemu organowi państwa trzeciego wyłącznie w celu, w jakim zostały pierwotnie przekazane. Dalsze przekazywanie danych powinno odbywać się w sposób zgodny z niniejszym rozporządzeniem.

(46) Wszystkie państwa członkowskie należą do Międzynarodowej Organizacji Policji Kryminalnej (Interpol). Aby wypełniać swoją misję, Interpol otrzymuje, przechowuje i przekazuje dane osobowe w celu wspierania właściwych organów w zapobieganiu przestępczości międzynarodowej i w jej zwalczaniu. W związku z tym należy wzmocnić współpracę między Unią a Interpolem poprzez promowanie sprawnej wymiany danych osobowych z jednoczesnym zapewnieniem poszanowania podstawowych praw i wolności w przypadku automatycznego przetwarzania danych osobowych. Gdy operacyjne dane osobowe są przekazywane przez Eurojust Interpolowi oraz państwom, które oddelegowały swoich przedstawicieli do Interpolu, zastosowanie powinno mieć niniejsze rozporządzenie, w szczególności przepisy o międzynarodowym przekazywaniu danych. Niniejsze rozporządzenie powinno być stosowane z zastrzeżeniem przepisów szczegółowych określonych we wspólnym stanowisku Rady 2005/69/WSiSW ([1]) i w decyzji Rady 2007/533/WSiSW ([2]).

(47) W przypadku gdy Eurojust przekazuje operacyjne dane osobowe organowi państwa trzeciego lub organizacji międzynarodowej na mocy umowy międzynarodowej zawartej na podstawie art. 218 TFUE, w umowie takiej powinny zostać przewidziane odpowiednie zabezpieczenia w odniesieniu do ochrony prywatności oraz podstawowych praw i wolności osób fizycznych, aby zapewnić przestrzeganie mających zastosowanie przepisów dotyczących danych osobowych.

(48) Państwa członkowskie powinny zapewnić, by dane były przekazywane do państwa trzeciego lub organizacji międzynarodowej tylko wtedy, gdy jest to konieczne do zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w tym do ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom, oraz gdy administrator w państwie trzecim lub w organizacji międzynarodowej jest organem właściwym w rozumieniu niniejszego rozporządzenia. Przekazania powinien dokonywać wyłącznie Eurojust występujący jako administrator. Przekazanie takie może nastąpić w przypadkach, w których Komisja zdecydowała, że dane państwo trzecie lub organizacja międzynarodowa zapewniają odpowiedni stopień ochrony, gdy przewidziano odpowiednie zabezpieczenia lub gdy mają zastosowanie odstępstwa w szczególnych sytuacjach.

(49) Eurojust powinien mieć możliwość przekazywania danych osobowych organowi państwa trzeciego lub organizacji międzynarodowej na podstawie decyzji Komisji stwierdzającej, że dane państwo lub organizacja międzynarodowa zapewniają odpowiedni poziom ochrony danych (zwanej dalej „decyzją stwierdzającą odpowiedni poziom ochrony"), lub – w przypadku braku decyzji stwierdzającej odpowiedni stopień ochrony – na podstawie umowy międzynarodowej zawartej przez Unię zgodnie z art. 218 TFUE lub umowy o współpracy umożliwiającej wymianę danych osobowych, zawartej między Eurojustem a tym państwem trzecim przed datą rozpoczęcia stosowania niniejszego rozporządzenia.

(50) W przypadku gdy kolegium stwierdzi, że ze względów operacyjnych istnieje potrzeba współpracy z państwem trzecim lub organizacją międzynarodową, powinno mieć możliwość zaproponowania Radzie, by zwróciła uwagę Komisji na potrzebę wydania decyzji stwierdzającej odpowiedni poziom ochrony lub na potrzebę wydania zalecenia w sprawie otwarcia negocjacji dotyczących umowy międzynarodowej zgodnie z art. 218 TFUE.

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

(52) Jeżeli nie wydano decyzji stwierdzającej odpowiedni poziom ochrony lub nie ma odpowiednich zabezpieczeń, przekazanie lub określona kategoria przekazań może nastąpić tylko w szczególnych sytuacjach, gdy jest to konieczne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby, bądź do zabezpieczenia uzasadnionych prawnie interesów osoby, której dane dotyczą, zgodnie z wymogami prawa państwa członkowskiego

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

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

przekazującego dane osobowe; do zapobieżenia bezpośredniemu i poważnemu zagrożeniu dla bezpieczeństwa publicznego państwa członkowskiego lub państwa trzeciego; w indywidualnym przypadku do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kary, w tym do ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom; lub w indywidualnym przypadku do celów ustalenia, dochodzenia lub obrony roszczenia przed sądem. Wyjątki te należy interpretować wąsko i nie powinny one umożliwiać częstego, masowego i zorganizowanego przekazywania danych osobowych ani przekazywania danych na dużą skalę; powinny też być ograniczone do danych ściśle niezbędnych. Takie operacje przekazania powinny być udokumentowane, a dokumentacja ta powinna być udostępniana na wniosek EIOD w celu monitorowania zgodności przekazania z prawem.

(53) W wyjątkowych przypadkach Eurojust powinien mieć możliwość przedłużania terminów przechowywania operacyjnych danych osobowych na potrzeby realizacji swych celów, pod warunkiem przestrzegania zasady celowości mającej zastosowanie do przetwarzania danych osobowych w kontekście wszystkich swych działań. Decyzje takie powinny być podejmowane po dokładnym rozważeniu wszystkich interesów, w tym interesów osób, których dane dotyczą. Decyzja o jakimkolwiek przedłużeniu terminu przetwarzania danych osobowych po upływie terminu przedawnienia ścigania we wszystkich zainteresowanych państwach członkowskich powinna być podejmowana tylko w przypadkach, gdy istnieje szczególna potrzeba udzielenia wsparcia na podstawie niniejszego rozporządzenia.

(54) Eurojust powinien utrzymywać uprzywilejowane stosunki z Europejską Siecią Sądową, oparte na konsultacjach i komplementarności. Niniejsze rozporządzenie powinno pomóc doprecyzować role, jakie Eurojust i Europejska Sieć Sądownicza będą odgrywały w swoich wzajemnych stosunkach, a przy tym utrzymać swoisty charakter Europejskiej Sieci Sądowej.

(55) W zakresie, w jakim jest to konieczne do wykonywania zadań, Eurojust powinien prowadzić współpracę z innymi instytucjami, organami i jednostkami organizacyjnymi Unii, Prokuraturą Europejską, właściwymi organami państw trzecich, a także z organizacjami międzynarodowymi.

(56) Aby wzmocnić współpracę operacyjną między Eurojustem a Europolem, a zwłaszcza w celu ustanowienia powiązań między danymi już posiadanymi przez te agencje, Eurojust powinien zapewnić Europolowi dostęp – w oparciu o system trafieniowy (figuruje/nie figuruje) – do danych będących w posiadaniu Eurojustu. Eurojust i Europol powinny zapewnić dokonanie niezbędnych uzgodnień służących optymalizacji współpracy operacyjnej między nimi, z należytym uwzględnieniem ich zakresów działania oraz wszelkich ograniczeń ze strony państw członkowskich. Takie uzgodnienia robocze powinny zapewniać dostęp do wszelkich informacji, które zostały dostarczone Europolowi i możliwość ich wyszukiwania na potrzeby kontroli krzyżowej, zgodnie ze szczególnymi zabezpieczeniami oraz gwarancjami ochrony danych przewidzianymi w niniejszym rozporządzaniu. Jakikolwiek dostęp przez Europol do danych będących w posiadaniu Eurojustu powinien być ograniczony – za pomocą środków technicznych – do informacji objętych zakresami działania tych agencji Unii.

(57) Eurojust i Europol powinny informować się nawzajem o działaniach pociągających za sobą finansowanie wspólnych zespołów dochodzeniowo-śledczych.

(58) Eurojust powinien mieć możliwość wymiany danych osobowych z instytucjami, organami i jednostkami organizacyjnymi Unii w zakresie niezbędnym do wykonywania jego zadań, przy zachowaniu pełnej ochrony prywatności oraz innych podstawowych praw i wolności.

(59) Eurojust powinien zacieśnić współpracę z właściwymi organami państw trzecich oraz z organizacjami międzynarodowymi na podstawie strategii opracowanej w porozumieniu z Komisją. W tym celu Eurojust powinien mieć możliwość oddelegowywania sędziów łącznikowych do państw trzecich, by mogli oni pełnić funkcje podobne do tych, które są pełnione przez sędziów łącznikowych oddelegowywanych przez państwa członkowskie na podstawie wspólnego działania Rady 96/277/WSiSW ([1]).

(60) Eurojust powinien mieć możliwość koordynacji wykonywania wniosków państwa trzeciego o współpracę wymiarów sprawiedliwości, w przypadku gdy wnioski te wymagają wykonania w co najmniej dwóch państwach członkowskich w ramach tego samego postępowania przygotowawczego. Eurojust powinien podejmować się takiej koordynacji wyłącznie za zgodą zainteresowanego państwa członkowskiego.

(61) W celu zagwarantowania pełnej autonomii i niezależności Eurojustu należy mu przyznać autonomiczny budżet, wystarczający do prawidłowego wykonywania jego pracy, którego dochody pochodzą zasadniczo z wkładu z budżetu Unii, poza kosztami wynagrodzeń i poborów przedstawicieli krajowych, zastępców i asystentów, ponoszonymi przez ich państwa członkowskie. Procedura budżetowa Unii powinna mieć zastosowanie w zakresie dotyczącym wkładu Unii oraz innych dotacji pochodzących z ogólnego budżetu Unii. Kontrolę sprawozdań finansowych powinien przeprowadzać Trybunał Obrachunkowy, a decyzję o ich zatwierdzeniu powinna podejmować Komisja Kontroli Budżetowej Parlamentu Europejskiego.

([1]) Wspólne działanie Rady 96/277/WSiSW z dnia 22 kwietnia 1996 r. dotyczące podstaw dla wymiany sędziów łącznikowych w celu poprawy współpracy sądowej między Państwami Członkowskimi Unii Europejskiej (Dz.U. L 105 z 27.4.1996, s. 1).

(62) W celu zwiększenia przejrzystości działań Eurojustu i wzmocnienia demokratycznego nadzoru nad tą agencją konieczne jest zapewnienie, zgodnie z art. 85 ust. 1 TFUE, mechanizmu wspólnej oceny działalności Eurojustu przez Parlament Europejski i parlamenty narodowe. Ocena powinna mieć miejsce w ramach międzyparlamentarnego posiedzenia komisji w pomieszczeniach Parlamentu Europejskiego w Brukseli, z udziałem członków właściwych komisji Parlamentu Europejskiego i parlamentów narodowych. Międzyparlamentarne posiedzenie komisji powinno się odbywać z pełnym poszanowaniem niezależności Eurojustu w odniesieniu do działań podejmowanych w konkretnych sprawach operacyjnych oraz w odniesieniu do obowiązku zachowania dyskrecji i poufności.

(63) Należy regularnie przeprowadzać ocenę stosowania niniejszego rozporządzenia.

(64) Działania Eurojustu powinny być przejrzyste zgodnie z art. 15 ust. 3 TFUE. Kolegium powinno przyjąć przepisy szczegółowe dotyczące sposobu zapewniania prawa do publicznego dostępu do dokumentów. Żaden z przepisów niniejszego rozporządzenia nie ma na celu ograniczenia prawa do publicznego dostępu do dokumentów, w zakresie w jakim jest ono zagwarantowane w Unii i w państwach członkowskich, w szczególności na mocy art. 42 Karty praw podstawowych Unii Europejskiej (zwanej dalej „Kartą"). Przepisy ogólne w zakresie przejrzystości, które mają zastosowanie do agencji Unii, powinny również mieć zastosowanie do Eurojustu w sposób w żadnym razie nie naruszając obowiązku zachowania poufności w jego działalności operacyjnej. W dochodzeniach administracyjnych prowadzonych przez Europejskiego Rzecznika Praw Obywatelskich powinno się przestrzegać obowiązku zachowania poufności obowiązującego Eurojust.

(65) Z myślą o zwiększeniu przejrzystości Eurojustu względem obywateli Unii i poprawie jego rozliczalności Eurojust powinien publikować na swojej stronie internetowej wykaz członków zarządu oraz w stosownych przypadkach podsumowania wyników posiedzeń zarządu, z poszanowaniem wymogów dotyczących ochrony danych.

(66) Do Eurojustu powinno mieć zastosowanie rozporządzenie Parlamentu Europejskiego i Rady (UE, Euratom) 2018/1046 ([1]).

(67) Do Eurojustu powinno mieć zastosowanie rozporządzenie Parlamentu Europejskiego i Rady (UE, Euratom) nr 883/2013 ([2]).

(68) Niezbędne przepisy dotyczące obiektów dla Eurojustu w państwie członkowskim, w którym ma on siedzibę – tj. w Niderlandach – a także szczególne przepisy mające zastosowanie do wszystkich pracowników Eurojustu i członków ich rodzin powinny zostać określone w umowie w sprawie siedziby. Przyjmujące państwo członkowskie powinno zapewnić najlepsze możliwe warunki w celu zagwarantowania funkcjonowania Eurojustu, w tym wielojęzyczne szkolnictwo o nastawieniu europejskim i odpowiednie połączenia transportowe, aby był on atrakcyjnym miejscem zatrudnienia dla wysoko wykwalifikowanych pracowników z jak największego obszaru geograficznego.

(69) Eurojust ustanowiony na mocy niniejszego rozporządzenia powinien być następcą prawnym Eurojustu ustanowionego na mocy decyzji 2002/187/WSiSW w odniesieniu do wszystkich zawartych przez niego umów, w tym umów o pracę, zaciągniętych zobowiązań i nabytego mienia. Umowy międzynarodowe zawarte przez Eurojust ustanowiony na mocy tą decyzją powinny dalej obowiązywać.

(70) Ponieważ cel niniejszego rozporządzenia, mianowicie stworzenie jednostki odpowiedzialnej za wspieranie i wzmacnianie koordynacji i współpracy między organami sądowymi państw członkowskich w odniesieniu do poważnej przestępczości, która dotyka co najmniej dwóch państw członkowskich lub która wymaga wspólnego ścigania, nie może zostać osiągnięty w sposób wystarczający przez państwa członkowskie, natomiast ze względu na zakres i skutki działań, możliwe jest jego lepsze osiągnięcie na poziomie Unii, może ona podjąć działania zgodnie z zasadą pomocniczości określoną w art. 5 TUE. Zgodnie z zasadą proporcjonalności, określoną w tym artykule, niniejsze rozporządzenie nie wykracza poza to, co jest konieczne do osiągnięcia tego celu.

(71) Zgodnie z art. 1, 2 i art. 4a ust. 1 Protokołu nr 21 w sprawie stanowiska Zjednoczonego Królestwa i Irlandii w odniesieniu do przestrzeni wolności, bezpieczeństwa i sprawiedliwości, załączonego do TUE i do TFUE oraz z zastrzeżeniem art. 4 tego protokołu, wspomniane państwa członkowskie nie uczestniczą w przyjęciu niniejszego rozporządzenia i nie są nim związane, ani go nie stosują.

([1]) Rozporządzenie Parlamentu Europejskiego i Rady (UE, Euratom) 2018/1046 z dnia 18 lipca 2018 r. w sprawie zasad finansowych mających zastosowanie do budżetu ogólnego Unii, zmieniające rozporządzenia (UE) nr 1296/2013, (UE) nr 1301/2013, (UE) nr 1303/2013, (UE) nr 1304/2013, (UE) nr 1309/2013, (UE) nr 1316/2013, (UE) nr 223/2014 i (UE) nr 283/2014 oraz decyzję nr 541/2014/UE, a także uchylające rozporządzenie (UE, Euratom) nr 966/2012 (Dz.U. L 193 z 30.7.2018, s. 1).

([2]) Rozporządzenie Parlamentu Europejskiego i Rady (UE, Euratom) nr 883/2013 z dnia 11 września 2013 r. dotyczące dochodzeń prowadzonych przez Europejski Urząd ds. Zwalczania Nadużyć Finansowych (OLAF) oraz uchylające rozporządzenie (WE) nr 1073/1999 Parlamentu Europejskiego i Rady i rozporządzenie Rady (Euratom) nr 1074/1999 (Dz.U. L 248 z 18.9.2013, s. 1).

(72) Zgodnie z art. 1 i 2 Protokołu nr 22 w sprawie stanowiska Danii, załączonego do TUE i do TFUE, Dania nie uczestniczy w przyjęciu niniejszego rozporządzenia i nie jest nim związana ani go nie stosuje.

(73) Zgodnie z art. 28 ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 45/2001 ([1]) skonsultowano się z EIOD, który wydał opinię w dniu 5 marca 2014 r.

(74) Niniejsze rozporządzenie nie narusza podstawowych praw i gwarancji oraz przestrzega zasad uznanych w szczególności w Karcie,

PRZYJMUJĄ NINIEJSZE ROZPORZĄDZENIE:

ROZDZIAŁ I

CELE I ZADANIA

Artykuł 1

Ustanowienie Agencji Unii Europejskiej ds. Współpracy Wymiarów Sprawiedliwości w Sprawach Karnych

1. Niniejszym ustanawia się Agencję Unii Europejskiej ds. Współpracy Wymiarów Sprawiedliwości w Sprawach Karnych (Eurojust).

2. Eurojust ustanowiony na mocy niniejszego rozporządzenia zastępuje Eurojust ustanowiony na mocy decyzji Rady 2002/187/WSiSW i jest jego następcą prawnym.

3. Eurojust ma osobowość prawną.

Artykuł 2

Zadania

1. Eurojust wspiera i wzmacnia koordynację i współpracę między krajowymi organami prowadzącymi postępowania przygotowawcze i organami właściwymi w zakresie wnoszenia i popierania oskarżeń w związku z poważną przestępczością, która zgodnie z art. 3 ust. 1 i 3 wchodzi w zakres właściwości Eurojustu, jeżeli przestępczość ta dotyka co najmniej dwóch państw członkowskich lub wymaga wspólnego ścigania, w oparciu o operacje przeprowadzane i informacje dostarczane przez organy państw członkowskich, Europol, Prokuraturę Europejską i OLAF.

2. Wykonując swoje zadania, Eurojust:

a) uwzględnia wszelkie wnioski składane przez właściwe organy państwa członkowskiego, wszelkie informacje dostarczone przez władze, instytucje, organy i jednostki organizacyjne Unii właściwe na podstawie przepisów przyjętych w ramach Traktatów oraz wszelkie informacje zgromadzone przez sam Eurojust;

b) ułatwia wykonywanie wniosków i decyzji dotyczących współpracy wymiarów sprawiedliwości, w tym wniosków i decyzji opartych na instrumentach służących wdrożeniu zasady wzajemnego uznawania.

3. Eurojust wykonuje swoje zadania na wniosek właściwych organów państw członkowskich, z własnej inicjatywy lub na wniosek Prokuratury Europejskiej w granicach właściwości Prokuratury Europejskiej.

Artykuł 3

Właściwość Eurojustu

1. Eurojust jest właściwy w sprawach dotyczących form poważnej przestępczości, które wymienione są w załączniku I. Jednakże od daty podjęcia przez Prokuraturę Europejską zadań związanych z prowadzeniem postępowań przygotowawczych oraz z wnoszeniem i popieraniem oskarżeń zgodnie z art. 120 ust. 2 rozporządzenia (UE) 2017/1939 Eurojust nie będzie wykonywać swojej właściwości w sprawach dotyczących przestępstw, w przypadku których Prokuratura Europejska wykonuje swoją właściwość, z wyjątkiem spraw dotyczących również państw członkowskich, które nie uczestniczą we wzmocnionej współpracy w zakresie ustanowienia Prokuratury Europejskiej, a także na wniosek tych państw członkowskich lub na wniosek Prokuratury Europejskiej.

2. Eurojust wykonuje swoją właściwość w sprawach dotyczących przestępstw mających wpływ na interesy finansowe Unii w przypadkach dotyczących państw członkowskich uczestniczących we wzmocnionej współpracy dotyczącej ustanowienia Prokuratury Europejskiej, w odniesieniu do których Prokuratura Europejska nie jest jednak właściwa lub podejmuje decyzję o niewykonywaniu swojej właściwości.

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

Eurojust, Prokuratura Europejska i zainteresowane państwa członkowskie konsultują się i współpracują ze sobą w celu ułatwienia Eurojustowi wykonywania jego właściwości wynikającej z niniejszego ustępu. Praktyczne szczegóły wykonywania przez Eurojust właściwości zgodnie z niniejszym ustępem są regulowane uzgodnieniem roboczym, o którym mowa w art. 47 ust. 3.

3. W odniesieniu do form przestępczości innych niż wymienione w załączniku I Eurojust może ponadto, zgodnie ze swoimi zadaniami, udzielać pomocy w postępowaniach przygotowawczych oraz wnoszeniu i popieraniu oskarżeń w sprawach tego rodzaju przestępczości, na wniosek właściwego organu danego państwa członkowskiego.

4. Eurojust jest właściwy w sprawach dotyczących przestępstw powiązanych z przestępstwami wymienionymi w załączniku I. Za przestępstwa powiązane uważa się następujące kategorie przestępstw:

a) przestępstwa mające służyć uzyskaniu środków do popełniania poważnych przestępstw wymienionych w załączniku I;

b) przestępstwa mające ułatwić lub umożliwić popełnienie poważnych przestępstw wymienionych w załączniku I;

c) przestępstwa popełnione w celu uniknięcia kary za popełnienie poważnych przestępstw wymienionych w załączniku I.

5. Na wniosek właściwego organu państwa członkowskiego Eurojust może także udzielać pomocy w postępowaniach przygotowawczych oraz wnoszeniu i popieraniu oskarżeń w sprawach dotyczących tylko tego państwa członkowskiego i państwa trzeciego, jeżeli z przedmiotowym państwem trzecim została zawarta umowa o współpracy lub porozumienie ustanawiające współpracę na podstawie art. 52 lub jeżeli w konkretnym przypadku istnieją szczególne powody do udzielenia takiej pomocy.

6. Na wniosek właściwego organu państwa członkowskiego albo Komisji, Eurojust może także udzielać pomocy w postępowaniach przygotowawczych oraz wnoszeniu i popieraniu oskarżeń w sprawach dotyczących tylko tego państwa członkowskiego, lecz mających następstwa na poziomie Unii. Przed podjęciem działania na wniosek Komisji Eurojust zasięga stosownej opinii właściwego organu zainteresowanego państwa członkowskiego.

Właściwy organ może w terminie określonym przez Eurojust sprzeciwić się wykonaniu wniosku przez Eurojust, uzasadniając w każdym przypadku swoje stanowisko.

Artykuł 4

Funkcje operacyjne Eurojustu

1. Eurojust:

a) udziela właściwym organom państw członkowskich informacji na temat postępowań przygotowawczych oraz wniesienia i popierania oskarżeń, o których został poinformowany, które mają następstwa na poziomie Unii lub które mogą mieć wpływ na państwa członkowskie inne niż te, które są bezpośrednio zainteresowane;

b) pomaga właściwym organom państw członkowskich zapewnić najlepszą możliwą koordynację postępowań przygotowawczych oraz wnoszenia i popierania oskarżeń;

c) pomaga w poprawie współpracy między właściwymi organami państw członkowskich, w szczególności na podstawie analiz Europolu;

d) współpracuje i konsultuje się z Europejską Siecią Sądową w sprawach karnych, w tym wykorzystuje jej bazę dokumentów i przyczynia się do jej udoskonalenia;

e) ściśle współpracuje z Prokuraturą Europejską w sprawach związanych z jej właściwością;

f) zapewnia wsparcie operacyjne, techniczne i finansowe na potrzeby transgranicznych operacji i postępowań przygotowawczych państw członkowskich, w tym na potrzeby wspólnych zespołów dochodzeniowo-śledczych;

g) wspiera unijne ośrodki wiedzy specjalistycznej, rozwijane przez Europol oraz instytucje, organy i jednostki organizacyjne Unii, a w stosownych przypadkach uczestniczy w ich działaniach;

h) współpracuje z instytucjami, organami i jednostkami organizacyjnymi Unii, jak również z sieciami utworzonymi w przestrzeni wolności, bezpieczeństwa i sprawiedliwości regulowanej tytułem V TFUE;

i) wspomaga działania państw członkowskich związane ze zwalczaniem form poważnej przestępczości, o których mowa w załączniku I.

2. W ramach wykonywania swoich zadań Eurojust może, podając powody swojego działania, występować do właściwych organów zainteresowanych państw członkowskich o:

a) wszczęcie postępowania przygotowawczego lub wniesienie i popieranie oskarżenia w związku z określonymi czynami;

b) uznanie, iż jeden z nich może mieć lepsze możliwości wszczęcia postępowania przygotowawczego lub wniesienia i popierania oskarżenia w związku z określonymi czynami;

c) koordynowanie działań między właściwymi organami zainteresowanych państw członkowskich;

d) ustanowienie wspólnego zespołu dochodzeniowo-śledczego, zgodnie z odpowiednimi instrumentami współpracy;

e) dostarczenie wszelkich informacji niezbędnych do wykonywania jego zadań;

f) dokonanie specjalnych czynności dochodzeniowo-śledczych;

g) podjęcie jakichkolwiek innych działań uzasadnionych potrzebami postępowania przygotowawczego lub wniesienia i popierania oskarżenia.

3. Eurojust może także:

a) wydawać opinie dla Europolu oparte na analizach przeprowadzonych przez Europol;

b) udzielać wsparcia logistycznego, w tym w zakresie tłumaczeń pisemnych i ustnych oraz organizacji spotkań koordynacyjnych.

4. W przypadku gdy co najmniej dwa państwa członkowskie nie mogą porozumieć się co do tego, które z nich powinno wszcząć postępowanie przygotowawcze lub wnieść i popierać oskarżenie w wyniku wniosku złożonego na podstawie ust. 2 lit. a) i b), Eurojust wydaje pisemną opinię w tej sprawie. Eurojust przesyła niezwłocznie tę opinię zainteresowanym państwom członkowskim.

5. Na wniosek właściwego organu lub z własnej inicjatywy Eurojust wydaje pisemną opinię w sprawie powtarzających się przypadków odmowy lub trudności związanych z wykonaniem wniosków i decyzji dotyczących współpracy wymiarów sprawiedliwości, w tym wniosków i decyzji opartych na instrumentach służących wdrożeniu zasady wzajemnego uznawania, pod warunkiem że nie można rozwiązać takich spraw za obopólnym porozumieniem właściwych organów krajowych lub przy udziale zainteresowanych przedstawicieli krajowych. Eurojust przesyła niezwłocznie tę opinię zainteresowanym państwom członkowskim.

6. Właściwe organy zainteresowanych państw członkowskich są zobowiązane udzielić odpowiedzi na wnioski Eurojustu, o których mowa w ust. 2, oraz na pisemne opinie, o których mowa w ust. 4 lub 5, bez zbędnej zwłoki. Właściwe organy państw członkowskich mogą odmówić zastosowania się do tych wniosków lub pisemnych opinii, jeżeli szkodziłoby to żywotnym interesom bezpieczeństwa narodowego lub groziło pomyślnemu prowadzeniu toczącego się postępowania przygotowawczego lub bezpieczeństwu osób.

Artykuł 5

Wykonywanie funkcji operacyjnych i innych funkcji

1. Przy podejmowaniu działań, o których mowa w art. 4 ust. 1 lub 2, Eurojust działa za pośrednictwem co najmniej jednego zainteresowanego przedstawiciela krajowego. Z zastrzeżeniem ust. 2 kolegium skupia się na kwestiach operacyjnych i wszelkich innych kwestiach, które są bezpośrednio powiązane ze sprawami operacyjnymi. Kolegium angażowane jest w sprawy administracyjne wyłącznie w zakresie, jaki jest niezbędny do zapewnienia realizacji jego funkcji operacyjnych.

2. Eurojust działa jako kolegium:

a) przy podejmowaniu wszelkich działań, o których mowa w art. 4 ust. 1 lub 2:

   (i) na wniosek co najmniej jednego przedstawiciela krajowego, którego dotyczy sprawa objęta działaniem Eurojust; lub

   (ii) gdy sprawa wymaga postępowania przygotowawczego lub wniesienia i popierania oskarżenia, które mają następstwa na poziomie Unii lub które mogą dotyczyć innych państw członkowskich niż te, które są bezpośrednio zainteresowane;

b) przy podejmowaniu jakichkolwiek działań, o których mowa w art. 4 ust. 3, 4 lub 5;

c) w przypadku kwestii o charakterze ogólnym dotyczącej osiągnięcia jego celów operacyjnych;

d) przy przyjmowaniu rocznego budżetu Eurojustu; w takim przypadku Eurojust podejmuje decyzje większością dwóch trzecich głosów swoich członków;

e) przy przyjmowaniu dokumentu programowego, o którym mowa w art. 15, lub sprawozdania rocznego z działalności Eurojustu; w takim przypadku Eurojust podejmuje decyzję większością dwóch trzecich głosów swoich członków;

f) przy wyborze lub odwołaniu przewodniczącego i wiceprzewodniczących zgodnie z art. 11;

g) przy powoływaniu dyrektora administracyjnego lub, w stosownych przypadkach, przedłużaniu jego kadencji lub odwoływaniu go ze stanowiska zgodnie z art. 17;

h) przy przyjmowaniu uzgodnień roboczych na mocy art. 47 ust. 3 i art. 52;

i) przy przyjmowaniu przepisów, których celem jest zapobieganie konfliktom interesów i zarządzanie nimi, w odniesieniu do jego członków, w tym dotyczących deklaracji interesów jego członków;

j) przy przyjmowaniu sprawozdań, dokumentów kierunkowych, wytycznych dla organów krajowych oraz opinii wchodzących w zakres działań operacyjnych Eurojustu, o ile dokumenty te mają charakter strategiczny;

k) przy powoływaniu sędziów łącznikowych zgodnie z art. 53;

l) przy podejmowaniu wszelkich decyzji, które nie są wyraźnie przypisane zarządowi w niniejszym rozporządzeniu lub nie należą do obowiązków dyrektora administracyjnego zgodnie z art. 18;

m) gdy inne przepisy niniejszego rozporządzenia tak stanowią.

3. W ramach wypełniania zadań Eurojust wskazuje, czy działa za pośrednictwem co najmniej jednego zainteresowanego przedstawiciela krajowego, czy jako kolegium.

4. Kolegium może powierzać dyrektorowi administracyjnemu i zarządowi dodatkowe zadania administracyjne wykraczające poza zadania, o których mowa w art. 16 i 18, zgodnie ze swoimi potrzebami operacyjnymi.

Jeżeli wymagają tego szczególne okoliczności, kolegium może zawiesić tymczasowo przekazanie uprawnień organu powołującego dyrektorowi administracyjnemu i uprawnień przekazanych dalej przez dyrektora administracyjnego oraz wykonywać je samodzielnie lub przekazać je jednemu ze swoich członków lub też członkowi personelu innemu niż dyrektor administracyjny.

5. Kolegium przyjmuje regulamin wewnętrzny Eurojustu większością dwóch trzecich głosów swoich członków. W przypadku niemożności osiągnięcia porozumienia większością dwóch trzecich głosów decyzja podejmowana jest zwykłą większością głosów. Regulamin wewnętrzny Eurojustu jest zatwierdzany przez Radę w drodze aktów wykonawczych.

ROZDZIAŁ II

STRUKTURA I ORGANIZACJA EUROJUSTU

SEKCJA I

Struktura

Artykuł 6

Struktura Eurojustu

Eurojustu składa się z:

a) przedstawicieli krajowych;

b) kolegium;

c) zarząd;

d) dyrektora administracyjnego.

SEKCJA II

Przedstawiciele krajowi

Artykuł 7

Status przedstawicieli krajowych

1. W skład Eurojustu wchodzi po jednym przedstawicielu krajowym oddelegowanym przez każde państwo członkowskie zgodnie z systemem prawnym tego państwa. Stałym miejscem pracy przedstawiciela krajowego jest siedziba Eurojustu.

2. Każdy przedstawiciel krajowy korzysta ze wsparcia jednego zastępcy i jednego asystenta. Zastępca i asystent co do zasady mają stałe miejsce pracy w siedzibie Eurojustu. Każde państwo członkowskie może zadecydować, że zastępca lub asystent mają stałe miejsce pracy w swoim państwie członkowskim. Jeżeli państwo członkowskie podejmie taką decyzję, powiadamia o tym kolegium. Jeżeli jest to wymagane ze względu na potrzeby operacyjne Eurojustu, kolegium może zażądać od państwa członkowskiego oddelegowania zastępcy lub asystenta na wskazany okres do siedziby Eurojustu. Państwo członkowskie zastosowuje się do takiego żądania kolegium bez zbędnej zwłoki.

3. Przedstawicielowi krajowemu mogą pomagać dodatkowi zastępcy lub asystenci, którzy mogą mieć – w razie konieczności i za zgodą kolegium – stałe miejsce pracy w siedzibie Eurojustu. Państwo członkowskie powiadamia Eurojust i Komisję o powołaniu przedstawicieli krajowych, zastępców i asystentów.

4. Przedstawiciele krajowi i ich zastępcy mają status prokuratora, sędziego lub przedstawiciela organu sądowego o kompetencjach równoważnych kompetencjom prokuratora lub sędziego zgodnie z prawem krajowym. Państwa członkowskie przyznają im co najmniej uprawnienia, o których mowa w niniejszym rozporządzeniu, aby mogli oni wykonywać swoje zadania.

5. Kadencja przedstawicieli krajowych i ich zastępców trwa pięć lat i jest odnawialna jednokrotnie. Jeżeli zastępca nie może działać w imieniu przedstawiciela krajowego lub go zastępować, przedstawiciel krajowy w momencie wygaśnięcia kadencji pozostaje na stanowisku – za zgodą swojego państwa członkowskiego – do momentu odnowienia kadencji lub zastąpienia go.

6. Państwa członkowskie powołują przedstawicieli krajowych i ich zastępców, kierując się ich odpowiednim poświadczonym doświadczeniem praktycznym na wysokim poziomie w dziedzinie wymiaru sprawiedliwości w sprawach karnych.

7. Zastępca może działać w imieniu przedstawiciela krajowego lub go zastępować. Asystent może również działać w imieniu przedstawiciela krajowego lub go zastępować, jeżeli posiada status, o którym mowa w ust. 4.

8. Wymiana informacji operacyjnych między Eurojustem a państwami członkowskimi odbywa się za pośrednictwem przedstawicieli krajowych.

9. Koszty wynagrodzeń i poborów przedstawicieli krajowych, ich zastępców i asystentów są ponoszone przez ich państwa członkowskie, z zastrzeżeniem art. 12.

10. Jeżeli przedstawiciele krajowi, ich zastępcy i asystenci wykonują zadania Eurojustu, stosowne wydatki związane z tymi działaniami uznaje się za wydatki operacyjne.

Artykuł 8

Uprawnienia przedstawicieli krajowych

1. Przedstawiciele krajowi są uprawnieni do:

a) ułatwiania lub wspierania w inny sposób wydawania lub wykonywania wniosków o wzajemną pomoc prawną lub o wzajemne uznanie;

b) bezpośredniego kontaktowania się z dowolnym właściwym organem krajowym państwa członkowskiego lub z jakimkolwiek innym właściwym organem lub jednostką organizacyjną Unii, w tym z Prokuraturą Europejską, oraz do wymiany z nimi informacji;

c) bezpośredniego kontaktowania się z dowolnym właściwym organem międzynarodowym zgodnie z międzynarodowymi zobowiązaniami swojego państwa członkowskiego oraz do wymiany z nim informacji organem;

d) udziału we wspólnych zespołach dochodzeniowo-śledczych, w tym w ich tworzeniu.

2. Z zastrzeżeniem ust. 1 państwa członkowskie mogą przyznać przedstawicielom krajowym dodatkowe uprawnienia zgodnie z prawem krajowym. Te państwa członkowskie powiadamiają Komisję i kolegium o tych uprawnieniach.

3. W porozumieniu z właściwym organem krajowym przedstawiciele krajowi mogą, zgodnie z prawem krajowym:

a) wydawać lub wykonywać wszelkie wnioski o wzajemną pomoc prawną lub o wzajemne uznanie;

b) nakazywać lub wnosić o podjęcie czynności dochodzeniowych przewidzianych w dyrektywie Parlamentu Europejskiego i Rady nr 2014/41/UE ([1]).

4. W nagłych przypadkach, gdy nie jest możliwe w odpowiednim czasie wskazanie właściwego organu krajowego lub skontaktowanie się z nim, przedstawiciele krajowi są uprawnieni do podjęcia środków, o których mowa w ust. 3, zgodnie z prawem krajowym, pod warunkiem że jak najszybciej poinformują o tym fakcie właściwy organ krajowy.

5. Przedstawiciel krajowy może wystąpić z wnioskiem do właściwego organu krajowego o podjęcie czynności, o których mowa w ust. 3 i 4, w przypadku gdy wykonywanie przez tego przedstawiciela krajowego uprawnień, o których mowa w ust. 3 i 4, byłoby sprzeczne z:

a) przepisami konstytucyjnymi państwa członkowskiego;

lub

b) zasadniczymi aspektami krajowych systemów wymiaru sprawiedliwości w sprawach karnych tego państwa członkowskiego dotyczącymi:

(i) podziału uprawnień między policję, prokuratorów i sędziów;

([1]) Dyrektywa Parlamentu Europejskiego i Rady nr 2014/41/UE z dnia 3 kwietnia 2014 r. w sprawie europejskiego nakazu dochodzeniowego w sprawach karnych (Dz.U. L 130 z 1.5.2014, s. 1).

(ii) funkcjonalnego podziału zadań między organy ścigania;

lub

(iii) struktury federalnej danego państwa członkowskiego.

6. Państwa członkowskie zapewniają, by w przypadkach, o których mowa w ust. 5, wniosek złożony przez ich przedstawiciela krajowego został rozpatrzony bez zbędnej zwłoki przez właściwy organ krajowy.

Artykuł 9

Dostęp do rejestrów krajowych

Przedstawiciele krajowi mają dostęp do informacji zawartych w wymienionych poniżej rodzajach rejestrów w swoich państwach członkowskich lub co najmniej mają możliwość uzyskania takich informacji, zgodnie ze swoim prawem krajowym:

a) rejestry karne;

b) rejestry osób aresztowanych;

c) rejestry postępowań przygotowawczych;

d) rejestry DNA;

e) inne rodzaje rejestrów prowadzonych przez organy publiczne ich państwa członkowskiego, w przypadku gdy takie informacje są niezbędne do wykonywania przez przedstawicieli krajowych ich zadań.

SEKCJA III

Kolegium

Artykuł 10

Skład kolegium

1. W skład kolegium wchodzą:

a) wszyscy przedstawiciele krajowi; oraz

b) jeden przedstawiciel Komisji, w przypadku gdy kolegium wykonuje swoje funkcje kierownicze.

Przedstawicielem Komisji powołanym na podstawie akapitu pierwszego lit. b) powinna być osoba pełniąca funkcję przedstawiciela Komisji w zarządzie na mocy art. 16 ust. 4.

2. Dyrektor administracyjny bierze udział w posiedzeniach kolegium związanych z zarządzaniem bez prawa głosu.

3. Kolegium może zaprosić do udziału w swoich posiedzeniach w charakterze obserwatora każdą osobę, której opinia może mieć znaczenie.

4. Z zastrzeżeniem przepisów regulaminu wewnętrznego Eurojustu, członkowie kolegium mogą korzystać z pomocy doradców lub ekspertów.

Artykuł 11

Przewodniczący i wiceprzewodniczący Eurojustu

1. Kolegium wybiera przewodniczącego i dwóch wiceprzewodniczących spośród przedstawicieli krajowych większością dwóch trzecich głosów swoich członków. W przypadku gdy nie można osiągnąć większości dwóch trzecich głosów w drugiej turze wyborów, wiceprzewodniczący wybierany jest zwykłą większością głosów członków kolegium, przy czym w przypadku wyboru przewodniczącego nadal wymagana jest większość dwóch trzecich głosów.

2. Przewodniczący wykonuje swoje funkcje w imieniu kolegium. Przewodniczący:

a) reprezentuje Eurojust;

b) zwołuje posiedzenia kolegium i zarządu oraz przewodniczy im, a także informuje kolegium o wszelkich sprawach będących przedmiotem jego zainteresowania;

c) kieruje pracą kolegium i nadzoruje bieżące kierowanie Eurojustem przez dyrektora administracyjnego;

d) wykonuje wszelkie inne funkcje określone w regulaminie wewnętrznym Eurojustu.

3. Wiceprzewodniczący wykonują funkcje określone w ust. 2 powierzone im przez przewodniczącego. Zastępują oni przewodniczącego, jeśli ten nie może wykonywać swoich obowiązków. Przewodniczącego i wiceprzewodniczących w wykonywaniu ich konkretnych obowiązków wspomaga personel administracyjny Eurojustu.

4. Kadencja przewodniczącego i wiceprzewodniczących trwa cztery lata. Mogą oni zostać jednokrotnie wybrani ponownie.

5. Jeżeli przedstawiciel krajowy zostaje wybrany na przewodniczącego lub wiceprzewodniczącego Eurojustu, jego kadencja ulega przedłużeniu w celu zapewnienia, aby mógł on pełnić swoją funkcję jako przewodniczący lub wiceprzewodniczący.

6. Jeżeli przewodniczący lub wiceprzewodniczący przestaje spełniać warunki wymagane do wykonywania swoich obowiązków, może zostać odwołany przez kolegium działające na wniosek jednej trzeciej członków. Decyzję przyjmuje się większością dwóch trzecich głosów członków kolegium, z wyłączeniem przewodniczącego lub wiceprzewodniczącego, którego decyzja ta dotyczy.

7. Jeżeli przedstawiciel krajowy zostaje wybrany na przewodniczącego Eurojustu, dane państwo członkowskie może oddelegować inną odpowiednio wykwalifikowaną osobę, aby wzmocnić biuro krajowe na czas sprawowania przez tego przedstawiciela krajowego kadencji przewodniczącego.

Państwo członkowskie, które postanowi oddelegować taką osobę, jest uprawnione do złożenia wniosku o rekompensatę zgodnie z art. 12.

Artykuł 12

Mechanizm rekompensat związany z wyborem na stanowisko przewodniczącego

1. Do dnia 12 grudnia 2019 r. Rada, działając na wniosek Komisji, określi w drodze aktów wykonawczych mechanizm rekompensaty do celów art. 11 ust. 7, przyznawanej państwom członkowskim, których przedstawiciel krajowy został wybrany na przewodniczącego.

2. Rekompensatę przyznaje się każdemu państwu członkowskiemu, jeżeli:

a) jego przedstawiciel krajowy został wybrany na przewodniczącego; oraz

b) złożyło ono do kolegium wniosek o rekompensatę i uzasadniło potrzebę wzmocnienia biura krajowego w związku ze zwiększonym obciążeniem pracą.

3. Rekompensata jest równoważna 50 % wynagrodzenia krajowego osoby oddelegowanej. Rekompensatę kosztów utrzymania i inne powiązane wydatki oblicza się w oparciu o podstawę porównywalną do tej, jaką stosuje się w przypadku urzędników Unii lub innych urzędników oddelegowanych za granicę.

4. Koszty mechanizmu rekompensat są pokrywane z budżetu Eurojustu.

Artykuł 13

Posiedzenia kolegium

1. Posiedzenia kolegium są zwoływane przez przewodniczącego.

2. Kolegium odbywa co najmniej jedno posiedzenie w miesiącu. Ponadto kolegium zbiera się z inicjatywy przewodniczącego, na wniosek Komisji w celu przedyskutowania zadań administracyjnych kolegium lub na wniosek co najmniej jednej trzeciej jego członków.

3. Eurojust przekazuje Prokuratorze Europejskiej porządek obrad posiedzeń kolegium w każdym przypadku, gdy omawiane są zagadnienia, które są istotne dla wykonywania zadań Prokuratury Europejskiej. Eurojust zaprasza Prokuraturę Europejską do udziału w takich posiedzeniach bez prawa głosu. W przypadku zaproszenia Prokuratury Europejskiej na posiedzenie kolegium, Eurojust przekazuje Prokuraturze Europejskiej dokumenty związane z porządkiem obrad.

Artykuł 14

Zasady głosowania kolegium

1. O ile nie wskazano inaczej oraz jeżeli osiągnięcie konsensusu nie jest możliwe, kolegium podejmuje decyzje większością głosów swoich członków.

2. Każdy członek ma jeden głos. W przypadku nieobecności członka uprawnionego do głosowania jego zastępca jest uprawniony do wykonywania prawa głosu na warunkach określonych w art. 7 ust. 7. W przypadku nieobecności zastępcy członka również asystent jest uprawniony do wykonywania prawa głosu na warunkach określonych w art. 7 ust. 7.

Artykuł 15

Programowanie roczne i wieloletnie

1. Do dnia 30 listopada każdego roku kolegium przyjmuje dokument programowy zawierający założenia programu rocznego i wieloletniego w oparciu o projekt przygotowany przez dyrektora administracyjnego, biorąc pod uwagę opinię Komisji. Kolegium przekazuje dokument programowy Parlamentowi Europejskiemu, Radzie, Komisji oraz Prokuraturze Europejskiej. Dokument programowy staje się ostateczny po końcowym uchwaleniu budżetu ogólnego Unii Europejskiej i w razie potrzeby podlega odpowiednim dostosowaniom.

2. Roczny program prac zawiera szczegółowe cele oraz oczekiwane wyniki, a także wskaźniki skuteczności. Roczny program prac zawiera również opis działań, które mają być finansowane, oraz określenie zasobów finansowych i kadrowych przydzielonych na każde działanie, zgodnie z zasadami budżetowania i zarządzania zadaniowego. Roczny program prac jest spójny z wieloletnim programem prac, o którym mowa w ust. 4. Jednoznacznie określone są w nim zadania, które zostały dodane, zmienione lub skreślone w stosunku do poprzedniego roku budżetowego.

3. Kolegium zmienia przyjęty roczny program prac w sytuacji, gdy Eurojustowi zostało powierzone nowe zadanie. Wszelkie znaczące zmiany w rocznym programie prac przyjmuje się w drodze tej samej procedury, co pierwotny roczny program prac. Kolegium może przekazać dyrektorowi administracyjnemu uprawnienia do dokonywania nieznacznych zmian w rocznym programie prac.

4. W wieloletnim programie prac określa się ogólne założenia strategiczne, w tym cele, strategię współpracy z organami państw trzecich i organizacjami międzynarodowymi, o której mowa w art. 52, oczekiwane wyniki i wskaźniki skuteczności. Obejmuje on również programowanie w zakresie zasobów, w tym budżetu wieloletniego i personelu. Program w zakresie zasobów jest aktualizowany co roku. Założenia strategiczne są uaktualniane w miarę potrzeb, a w szczególności w celu uwzględnienia wyników oceny, o której mowa w art. 69.

SEKCJA IV

Zarząd

Artykuł 16

Funkcjonowanie zarządu

1. Kolegium jest wspierane przez zarząd. Zarząd jest odpowiedzialny za podejmowanie decyzji administracyjnych w celu zapewnienia właściwego funkcjonowania Eurojustu. Nadzoruje on również niezbędne prace przygotowawcze prowadzone przez dyrektora administracyjnego dotyczące innych kwestii administracyjnych, które ma przyjąć kolegium. Nie angażuje się on **w** funkcje operacyjne Eurojustu, o których mowa w art. 4 i 5.

2. Wykonując swoje zadania zarząd może konsultować się z kolegium.

3. Ponadto zarząd:

a) dokonuje przeglądu dokumentu programowego Eurojustu, o którym mowa w art. 15, opracowanego w oparciu o projekt przygotowany przez dyrektora administracyjnego, i przekazuje go kolegium do przyjęcia;

b) przyjmuje strategię zwalczania nadużyć finansowych dla Eurojustu proporcjonalną do zagrożeń takimi nadużyciami, przy uwzględnieniu kosztów i korzyści wynikających ze środków, które mają zostać wdrożone, i w oparciu o projekt przygotowany przez dyrektora administracyjnego;

c) przyjmuje odpowiednie przepisy wykonawcze do regulaminu pracowniczego urzędników Unii Europejskiej (zwanego dalej „regulaminem pracowniczym urzędników") i do warunków zatrudnienia innych pracowników Unii Europejskiej (zwanych dalej „warunkami zatrudnienia innych pracowników"), ustanowionych w rozporządzeniu Rady (EWG, Euratom, EWWiS) nr 259/68 ([1]), zgodnie z art. 110 regulaminu pracowniczego urzędników;

d) zapewnia odpowiednie działania następcze w odpowiedzi na ustalenia i zalecenia wynikające z wewnętrznych lub zewnętrznych sprawozdań z kontroli, ocen i dochodzeń, w tym tych przeprowadzonych przez EIOD i OLAF;

e) podejmuje wszelkie decyzje dotyczące utworzenia i w stosownych przypadkach zmiany wewnętrznych struktur administracyjnych Eurojustu;

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

f) z zastrzeżeniem obowiązków dyrektora administracyjnego określonych w art. 18, służy mu pomocą i doradztwem w zakresie wykonywania decyzji kolegium, mając na względzie wzmocnienie nadzoru nad zarządzaniem administracyjnym i budżetowym;

g) realizuje wszelkie dodatkowe zadania administracyjne powierzone mu przez kolegium na mocy art. 5 ust. 4;

h) przyjmuje przepisy finansowe mające zastosowanie do Eurojustu zgodnie z art. 64;

i) zgodnie z art. 110 regulaminu pracowniczego urzędników przyjmuje –na podstawie art. 2 ust. 1 regulaminu pracowniczego urzędników i art. 6 warunków zatrudnienia innych pracowników – decyzję, zgodnie z którą dyrektorowi administracyjnemu przekazuje się odpowiednie uprawnienia organu powołującego i w której określa się warunki, na jakich można zawiesić przekazanie tych uprawnień; dyrektor administracyjny jest upoważniony do dalszego przekazywania tych uprawnień;

j) dokonuje przeglądu budżetu rocznego Eurojustu do przyjęcia przez kolegium;

k) dokonuje przeglądu sprawozdania rocznego z działalności Eurojustu i przekazuje je kolegium do przyjęcia;

l) powołuje księgowego i inspektora ochrony danych, którzy są funkcjonalnie niezależni w wykonywaniu swoich obowiązków.

4. W skład zarządu wchodzą przewodniczący i wiceprzewodniczący Eurojustu, jeden przedstawiciel Komisji i dwóch innych członków kolegium wyznaczonych w systemie dwuletniej rotacji zgodnie z regulaminem wewnętrznym Eurojustu. Dyrektor administracyjny bierze udział w posiedzeniach zarządu bez prawa głosu.

5. Przewodniczącym zarządu jest przewodniczący Eurojustu. Zarząd podejmuje decyzje większością głosów swoich członków. Każdy członek ma jeden głos. W przypadku równego rozkładu głosów przewodniczący Eurojustu ma głos decydujący.

6. Kadencja członków zarządu kończy się z chwilą zakończenia ich kadencji jako przedstawicieli krajowych, przewodniczącego lub wiceprzewodniczącego.

7. Zarząd zbiera się co najmniej raz w miesiącu. Ponadto zarząd zbiera się z inicjatywy przewodniczącego, na wniosek Komisji lub na wniosek przynajmniej dwóch jego członków.

8. Eurojust przekazuje Prokuraturze Europejskiej porządek obrad wszystkich posiedzeń zarządu i konsultuje się z nią w sprawie konieczności udziału w tych posiedzeniach. Eurojust zaprasza Prokuraturę Europejską do udziału w posiedzeniach, bez prawa głosu, w każdym przypadku gdy omawiane są zagadnienia, które są istotne dla funkcjonowania Prokuratury Europejskiej.

W przypadku zaproszenia Prokuratury Europejskiej na posiedzenie zarządu, Eurojust przekazuje Prokuraturze Europejskiej dokumenty związane z porządkiem obrad.

SEKCJA V

Dyrektor administracyjny

Artykuł 17

Status dyrektora administracyjnego

1. Dyrektor administracyjny jest zatrudniony w Eurojuście na czas określony zgodnie z art. 2 lit. a) warunków zatrudnienia.

2. Dyrektor administracyjny jest powoływany przez kolegium z listy kandydatów zaproponowanej przez zarząd na podstawie otwartej i przejrzystej procedury naboru zgodnie z regulaminem wewnętrznym Eurojustu. Przy zawarciu umowy o pracę z dyrektorem administracyjnym Eurojust jest reprezentowany przez przewodniczącego Eurojustu.

3. Kadencja dyrektora administracyjnego trwa cztery lata. Przed upływem tego okresu zarząd przeprowadza ocenę, w której uwzględnia się ocenę pracy dyrektora administracyjnego.

4. Kolegium, działając na wniosek zarządu, który uwzględnia ocenę wskazaną w ust. 3, może przedłużyć kadencję dyrektora administracyjnego jeden raz, na okres nie dłuższy niż cztery lata.

5. Dyrektor administracyjny, którego kadencja została przedłużona, nie może uczestniczyć w kolejnej procedurze naboru na to samo stanowisko po upływie swojej przedłużonej kadencji.

6. Dyrektor administracyjny odpowiada przed kolegium.

7. Dyrektor administracyjny może zostać odwołany ze stanowiska jedynie na mocy decyzji kolegium działającego na wniosek zarządu.

Artykuł 18

Obowiązki dyrektora administracyjnego

1. Do celów administracyjnych Eurojustem kieruje jego dyrektor administracyjny.

2. Z zastrzeżeniem uprawnień kolegium lub zarządu, dyrektor administracyjny jest niezależny w wykonywaniu swoich obowiązków i nie zwraca się o instrukcje do żadnego rządu ani jakiegokolwiek innego podmiotu ani też nie przyjmuje od nich takich instrukcji.

3. Dyrektor administracyjny jest przedstawicielem prawnym Eurojustu.

4. Dyrektor administracyjny odpowiada za realizację zadań administracyjnych powierzonych Eurojustowi, w szczególności za:

a) bieżące zarządzanie Eurojustem i jego personelem;

b) wdrażanie decyzji przyjętych przez kolegium i zarząd;

c) opracowywanie dokumentu programowego, o którym mowa w art. 15, oraz przekazywanie go zarządowi do dokonania przeglądu;

d) realizację dokumentu programowego, o którym mowa w art. 15, oraz przekazywanie zarządowi i kolegium sprawozdań z jego realizacji;

e) opracowywanie rocznego sprawozdania z działalności Eurojustu i przedstawianie go zarządowi do dokonania przeglądu i kolegium do przyjęcia;

f) opracowywanie planu działania w następstwie wniosków z wewnętrznych lub zewnętrznych sprawozdań z kontroli, ocen i dochodzeń, w tym tych przeprowadzonych przez EIOD i OLAF, oraz przekazywanie kolegium, zarządowi, Komisji i EIOD dwa razy w roku sprawozdań z postępów w realizacji tego planu;

g) opracowywanie strategii zwalczania nadużyć finansowych dla Eurojustu i przedstawianie jej zarządowi do przyjęcia;

h) przygotowanie projektu przepisów finansowych mających zastosowanie do Eurojustu;

i) sporządzanie projektu zestawienia przewidywanych dochodów i wydatków Eurojustu i realizacja jego budżetu;

j) wykonywanie w odniesieniu do pracowników Agencji uprawnień przyznanych organowi powołującemu na mocy regulaminu pracowniczego urzędników oraz uprawnień przyznanych organowi uprawnionemu do zawierania umów o pracę na mocy warunków zatrudnienia innych pracowników („uprawnienia organu powołującego”);

k) zapewnianie niezbędnego wsparcia administracyjnego w celu ułatwienia działalności operacyjnej Eurojustu;

l) zapewnianie wsparcia dla przewodniczącego i wiceprzewodniczących w wykonywaniu ich obowiązków;

m) przygotowanie wstępnego projektu rocznego budżetu Eurojustu, który należy przedstawić zarządowi do przeglądu przed przyjęciem przez kolegium.

ROZDZIAŁ III

KWESTIE OPERACYJNE

Artykuł 19

Dyżurny mechanizm koordynacyjny

1. W celu realizacji swoich zadań w nagłych przypadkach Eurojust prowadzi dyżurny mechanizm koordynacyjny („DMK”), który w każdym momencie jest w stanie przyjmować i rozpatrywać kierowane do niego wnioski. Kontakt z DMK musi być możliwy przez całą dobę, siedem dni w tygodniu.

2. DMK składa się z jednego przedstawiciela DMK na każde państwo członkowskie, którym może być przedstawiciel krajowy, jego zastępca lub asystent uprawniony do zastępowania przedstawiciela krajowego albo oddelegowany ekspert krajowy. Przedstawiciel DMK musi być w dostępny w celu podejmowania działań przez całą dobę, siedem dni w tygodniu.

3. Przedstawiciele DMK skutecznie i niezwłocznie podejmują działania związane z wykonaniem wniosku w ich państwie członkowskim.

Artykuł 20

Krajowy system koordynacyjny Eurojustu

1. Każde państwo członkowskie powołuje co najmniej jednego korespondenta krajowego Eurojustu.

2. Wszyscy korespondenci krajowi powołani przez państwa członkowskie zgodnie z ust. 1 muszą posiadać umiejętności i doświadczenie wymagane do wykonywania ich zadań.

3. Każde państwo członkowskie tworzy krajowy system koordynacyjny Eurojustu, tak by zapewnić koordynację działań podejmowanych przez:

a) krajowych korespondentów Eurojustu;

b) krajowych korespondentów do spraw związanych z właściwością Prokuratury Europejskiej;

c) krajowego korespondenta Eurojustu do spraw terroryzmu;

d) krajowego korespondenta Europejskiej Sieci Sądowej w sprawach karnych oraz maksymalnie trzy inne punkty kontaktowe Europejskiej Sieci Sądowej;

e) przedstawicieli krajowych lub punkty kontaktowe sieci wspólnych zespołów dochodzeniowo-śledczych oraz przedstawicieli krajowych lub punkty kontaktowe sieci utworzonych decyzjami 2002/494/WSiSW, 2007/845/WSiSW oraz 2008/852/WSiSW;

f) w stosownych przypadkach – każdy inny stosowny organ sądowy.

4. Osoby, o których mowa w ust. 1 i 3, zachowują swoje stanowisko i status zgodnie z prawem krajowym, co nie może wywierać znaczącego wpływu na wykonywanie przez nie obowiązków wynikających z niniejszego rozporządzenia.

5. Krajowi korespondenci Eurojustu odpowiadają za działanie swego krajowego systemu koordynacyjnego Eurojustu. W przypadku gdy powołano kilku korespondentów Eurojustu, za działanie ich krajowego systemu koordynacyjnego Eurojustu odpowiada jeden z nich.

6. Przedstawiciele krajowi są informowani o wszelkich posiedzeniach ich krajowego systemu koordynacyjnego Eurojustu, w przypadku gdy omawiane są kwestie związane z prowadzonymi sprawami. W razie potrzeby mogą oni brać udział w tych posiedzeniach.

7. Każdy krajowy system koordynacyjny Eurojustu ułatwia wykonywanie zadań Eurojustu w danym państwie członkowskim, w szczególności poprzez:

a) zapewnienie, by do zautomatyzowanego systemu zarządzania sprawami, o którym mowa w art. 23, przekazywano informacje odnoszące się do danego państwa członkowskiego w sposób sprawny i niezawodny;

b) pomoc w ustalaniu, czy dany wniosek należy rozpatrywać z wykorzystaniem Eurojustu czy Europejskiej Sieci Sądowej;

c) udzielanie przedstawicielowi krajowemu pomocy w identyfikacji organów właściwych do wykonywania wniosków i decyzji dotyczących współpracy wymiarów sprawiedliwości, w tym także wniosków i decyzji opartych na instrumentach służących wdrożeniu zasady wzajemnego uznawania;

d) utrzymywanie bliskich stosunków z krajową jednostką Europolu, innymi punktami kontaktowymi Europejskiej Sieci Sądowej oraz innymi odpowiednimi właściwymi organami krajowymi.

8. Aby realizować cele, o których mowa w ust. 7, osoby, o których mowa w ust. 1 i w ust. 3 lit. a), b) i c), są podłączone, a osoby lub organy, o których mowa w ust. 3 lit. d) i e), mogą zostać podłączone do zautomatyzowanego systemu zarządzania sprawami zgodnie z niniejszym artykułem oraz z art. 23, 24, 25 i 34. Koszty podłączenia do zautomatyzowanego systemu zarządzania sprawami ponoszone są z budżetu ogólnego Unii.

9. Utworzenie krajowego systemu koordynacyjnego Eurojustu i powołanie korespondentów krajowych nie wyklucza bezpośrednich kontaktów przedstawiciela krajowego z właściwymi organami jego państwa członkowskiego.

Artykuł 21

Wymiana informacji z państwami członkowskimi i między przedstawicielami krajowymi

1. Właściwe organy państw członkowskich wymieniają z Eurojustem wszelkie informacje konieczne do wykonywania jego zadań, o których mowa w art. 2 i 4,zgodnie z mającymi zastosowanie przepisami dotyczącymi ochrony danych. Wymiana ta obejmuje przynajmniej informacje, o których mowa w ust. 4, 5 i 6 niniejszego artykułu.

2. Przekazanie informacji Eurojustowi jest traktowane jako złożenie wniosku o pomoc Eurojustu w danej sprawie wyłącznie wtedy, gdy właściwy organ tak wyraźnie wskazał.

3. Przedstawiciele krajowi dokonują, bez uprzedniej zgody, między sobą lub ze swoimi właściwymi organami krajowymi, wymiany wszelkich informacji koniecznych do wykonywania zadań Eurojustu. W szczególności właściwe organy krajowe niezwłocznie informują swoich przedstawicieli krajowych o dotyczącej ich sprawie.

4. Właściwe organy krajowe informują swoich przedstawicieli krajowych o utworzeniu wspólnych zespołów dochodzeniowo-śledczych oraz o wynikach prac takich zespołów.

5. Właściwe organy krajowe bez zbędnej zwłoki informują swoich przedstawicieli krajowych o wszelkich przypadkach, które dotyczą co najmniej trzech państw członkowskich i w odniesieniu do których wnioski lub decyzje dotyczące współpracy wymiarów sprawiedliwości, w tym wnioski i decyzje oparte na instrumentach służących wdrożeniu zasady wzajemnego uznawania, zostały przekazane do co najmniej dwóch państw członkowskich, w przypadku gdy zachodzi jedna lub więcej z poniższych przesłanek:

a) za dane przestępstwo w państwie członkowskim występującym z wnioskiem lub wydającym decyzję grozi kara pozbawienia wolności lub środek zabezpieczający polegający na pozbawieniu wolności na maksymalny okres co najmniej pięciu lub sześciu lat – zależnie od decyzji danego państwa członkowskiego – i przestępstwo to jest umieszczone w następującym wykazie:

   (i) handel ludźmi;

   (ii) niegodziwe traktowanie w celach seksualnych lub wykorzystywanie seksualne, w tym pornografia dziecięca i nagabywanie dzieci w celach seksualnych;

   (iii) handel narkotykami;

   (iv) nielegalny handel bronią palną, jej częściami lub komponentami oraz amunicją lub materiałami wybuchowymi;

   (v) korupcja;

   (vi) przestępstwa przeciwko interesom finansowym Unii;

   (vii) fałszowanie pieniądza lub środków płatniczych;

   (viii) działalność związana z praniem pieniędzy;

   (ix) przestępczość komputerowa;

b) stan faktyczny wskazuje, że dana sprawa dotyczy organizacji przestępczej;

c) z przesłanek wynika, że sprawa może mieć istotny wymiar transgraniczny lub może mieć następstwa na poziomie Unii, lub może dotyczyć innych państw członkowskich niż te, które są bezpośrednio zaangażowane.

6. Właściwe organy krajowe informują swoich przedstawicieli krajowych o:

a) przypadkach, w których wystąpił lub może wystąpić konflikt jurysdykcji;

b) przesyłkach niejawnie nadzorowanych dotyczących co najmniej trzech państw, z których co najmniej dwa są państwami członkowskimi;

c) powtarzających się trudnościach lub odmowach dotyczących wykonania wniosków lub decyzji w sprawie współpracy wymiarów sprawiedliwości, w tym wniosków i decyzji opartych na instrumentach służących wdrożeniu zasady wzajemnego uznawania.

7. W szczególnych przypadkach organy krajowe nie mają obowiązku przekazywania informacji, jeżeli ich przekazanie zaszkodziłoby żywotnym interesom bezpieczeństwa narodowego lub bezpieczeństwu osób.

8. Niniejszy artykuł nie narusza warunków określonych w umowach dwustronnych bądź wielostronnych lub uzgodnień między państwami członkowskimi a państwami trzecimi, w tym wszelkich warunków określonych przez państwa trzecie w odniesieniu do sposobu wykorzystania informacji po ich dostarczeniu.

9. Niniejszy artykuł nie narusza innych obowiązków dotyczących przekazywania informacji Eurojustowi, w tym decyzji Rady 2005/671/WSiSW ([1]).

10. Informacje, o których mowa w niniejszym artykule, są przekazywane w postaci uporządkowanej określonej przez Eurojust. Właściwy organ krajowy nie ma obowiązku udzielania tych informacji, jeżeli zostały już one przekazane Eurojustowi zgodnie z innymi przepisami niniejszego rozporządzenia.

Artykuł 22

Informacje dostarczane przez Eurojust właściwym organom krajowym

1. Eurojust dostarcza właściwym organom krajowym bez zbędnej zwłoki informacje o wynikach przetwarzania informacji, w tym o powiązaniach ze sprawami już zarejestrowanymi w zautomatyzowanym systemie zarządzania sprawami. Informacje te mogą obejmować dane osobowe.

2. Jeżeli właściwy organ krajowy wystąpi do Eurojustu o dostarczenie mu informacji w określonym terminie, Eurojust przekazuje te informacje w tym terminie.

Artykuł 23

Zautomatyzowany system zarządzania sprawami, indeks i akta tymczasowe

1. Eurojust tworzy zautomatyzowany system zarządzania sprawami składający się z akt tymczasowych i z indeksu, w których zawarte są dane osobowe określone w załączniku II i dane inne niż osobowe.

2. Celem zautomatyzowanego systemu zarządzania sprawami jest:

a) wspieranie prowadzenia i koordynacji postępowań przygotowawczych oraz wnoszenia i popierania oskarżeń w przypadkach, w których Eurojust udziela pomocy, w szczególności poprzez zestawianie informacji;

b) ułatwianie dostępu do informacji na temat postępowań przygotowawczych oraz wniesionych i popieranych oskarżeń, które są w toku;

c) ułatwianie monitorowania legalności przetwarzania danych osobowych przez Eurojust oraz jego zgodności z odpowiednimi przepisami dotyczącymi ochrony danych.

3. Zautomatyzowany system zarządzania sprawami może być podłączony do bezpiecznego połączenia telekomunikacyjnego, o którym mowa w art. 9 decyzji Rady 2008/976/WSiSW ([2]).

4. Indeks zawiera odniesienia do akt tymczasowych przetwarzanych w Eurojuście i nie może zawierać żadnych danych osobowych innych niż dane, o których mowa w załączniku II pkt 1 lit. a)–i), k) oraz m), a także w pkt 2.

5. Wykonując swoje obowiązki, przedstawiciele krajowi mogą przetwarzać dane dotyczące indywidualnych spraw, nad którymi pracują, w aktach tymczasowych. Udzielają oni dostępu do akt tymczasowych inspektorowi ochrony danych. Dany przedstawiciel krajowy informuje inspektora ochrony danych o każdym przypadku otwarcia nowych akt tymczasowych, które zawierają dane osobowe.

6. Do celów przetwarzania operacyjnych danych osobowych Eurojust nie może tworzyć żadnych innych zautomatyzowanych plików danych niż zautomatyzowany system zarządzania sprawami. Przedstawiciel krajowy może jednak tymczasowo przechowywać i analizować dane osobowe do celów ustalenia, czy takie dane są istotne dla zadań Eurojustu i czy mogą zostać włączone do zautomatyzowanego systemu zarządzania sprawami. Dane te można zatrzymać przez okres nie dłuższy niż 3 miesiące.

Artykuł 24

Funkcjonowanie akt tymczasowych i indeksu

1. Przedstawiciel krajowy otwiera akta tymczasowe w przypadku każdej sprawy, w odniesieniu do której przekazano mu informacje, o ile takie przekazanie informacji odbyło się zgodnie z niniejszym rozporządzeniem lub innymi odnośnymi instrumentami prawnymi. Przedstawiciel krajowy ponosi odpowiedzialność za prowadzenie akt tymczasowych, które otworzył.

([1]) Decyzja Rady 2005/671/WSiSW z dnia 20 września 2005 r. w sprawie wymiany informacji i współpracy dotyczącej przestępstw terrorystycznych (Dz.U. L 253 z 29.9.2005, s. 22).

([2]) Decyzja Rady 2008/976/WSiSW z dnia 16 grudnia 2008 r. w sprawie Europejskiej Sieci Sądowej (Dz.U. L 348 z 24.12.2008, s. 130).

2. Przedstawiciel krajowy, który otworzył akta tymczasowe, decyduje w poszczególnych przypadkach, czy dostęp do tych akta powinien pozostać ograniczony, czy też należy udostępnić je w całości lub części innym przedstawicielom krajowym, upoważnionym pracownikom Eurojustu lub innej osobie pracującej w imieniu Eurojustu, która otrzymała niezbędne do tego upoważnienie dyrektora administracyjnego.

3. Przedstawiciel krajowy, który otworzył akta tymczasowe, decyduje, które informacje odnoszące się do tych akt, należy umieścić w indeksie zgodnie z art. 23 ust. 4.

Artykuł 25

Dostęp do zautomatyzowanego systemu zarządzania sprawami na poziomie krajowym

1. Jeżeli osoby, o których mowa w art. 20 ust. 3, są podłączone do zautomatyzowanego systemu zarządzania sprawami, mogą one mieć dostęp wyłącznie do:

a) indeksu, chyba że przedstawiciel krajowy, który zdecydował o wprowadzeniu danych do indeksu, wyraźnie zabronił takiego dostępu;

b) akt tymczasowych otwartych przez przedstawiciela krajowego państwa członkowskiego, z którego pochodzą te osoby;

c) akt tymczasowych otwartych przez przedstawicieli krajowych innych państw członkowskich, do których to akt udzielono dostępu przedstawicielowi krajowemu państwa członkowskiego, z którego osoby te pochodzą, chyba że przedstawiciel krajowy, który otworzył te akta, wyraźnie odmówił dostępu.

2. W ramach ograniczeń określonych w ust. 1 niniejszego artykułu przedstawiciel krajowy decyduje o tym, w jakim zakresie w jego państwie członkowskim zezwala się na dostęp do akt tymczasowych osobom, o których mowa w art. 20 ust. 3, jeżeli są one podłączone do zautomatyzowanego systemu zarządzania sprawami.

3. Każde państwo członkowskie po konsultacji ze swoim przedstawicielem krajowym decyduje o tym, w jakim zakresie w tym państwie członkowskim zezwala się na dostęp do indeksu osobom, o których mowa w art. 20 ust. 3, jeżeli są one podłączone do zautomatyzowanego systemu zarządzania sprawami. Państwa członkowskie informują Eurojust i Komisję o decyzjach, jakie podjęły w odniesieniu do wdrożenia niniejszego ustępu. Komisja informuje o tym pozostałe państwa członkowskie.

4. Osoby, którym udzielono dostępu zgodnie z ust. 2, mają co najmniej dostęp do indeksu w zakresie, w jakim jest to niezbędne, aby uzyskać dostęp do akt tymczasowych, do których udzielono im dostępu.

ROZDZIAŁ IV

PRZETWARZANIE INFORMACJI

Artykuł 26

Przetwarzanie danych osobowych przez Eurojust

1. Niniejsze rozporządzenie oraz art. 3 i rozdział IX rozporządzenia (UE) 2018/1725 stosuje się do przetwarzania przez Eurojust operacyjnych danych osobowych. Rozporządzenie (UE) 2018/1725 stosuje się do przetwarzania przez Eurojust administracyjnych danych osobowych, z wyjątkiem rozdziału IX tego rozporządzenia.

2. Odesłania w niniejszym rozporządzeniu do „mających zastosowanie przepisów dotyczących ochrony danych" należy rozumieć jako odesłania do przepisów dotyczących danych osobowych określonych w niniejszym rozporządzeniu oraz w rozporządzeniu (UE) 2018/1725.

3. Przepisy o ochronie danych dotyczące przetwarzania operacyjnych danych osobowych zawarte w niniejszym rozporządzeniu uznaje się za przepisy szczegółowe do przepisów ogólnych określonych w art. 3 i rozdziale IX rozporządzenia (UE) 2018/1725.

4. Eurojust określa terminy przechowywania administracyjnych danych osobowych w przepisach odnoszących się do ochrony danych w swoim regulaminie wewnętrznym.

Artykuł 27

Przetwarzanie operacyjnych danych osobowych

1. O ile jest to niezbędne do wykonywania zadań Eurojustu, może on w ramach swojej właściwości i do celów wykonywania swoich funkcji operacyjnych przetwarzać w sposób zautomatyzowany lub w ręcznie uporządkowanych katalogach, zgodnie z niniejszym rozporządzeniem, wyłącznie operacyjne dane osobowe wymienione w pkt 1 załącznika II dotyczące osób, które zgodnie z prawem krajowym zainteresowanych państw członkowskich są osobami, co do których istnieją poważne powody, by podejrzewać, że popełniły lub popełnią przestępstwo, w przypadku którego Eurojust jest właściwy, lub które zostały skazane za popełnienie takiego przestępstwa.

2. Eurojust może przetwarzać wyłącznie operacyjne dane osobowe wymienione w pkt 2 załącznika II dotyczące osób, które zgodnie z prawem krajowym zainteresowanych państw członkowskich uważane są za pokrzywdzonych lub dotyczące osób innych w stosunku do przestępstwa, takich jak osoby, które mogą zostać wezwane do złożenia zeznań w ramach postępowania przygotowawczego lub wniesienia i popierania oskarżenia w sprawach dotyczących co najmniej jednego rodzaju przestępczości i przestępstw określonych w art. 3, osoby, które mogą dostarczyć informacji o przestępstwach lub osoby, które mają kontakty lub powiązania z osobą, o której mowa w ust. 1. Przetwarzanie takich operacyjnych danych osobowych może mieć miejsce wyłącznie wówczas, gdy jest to niezbędne do realizacji zadań Eurojustu w ramach jego właściwości i do celów wykonywania jego funkcji operacyjnych.

3. W wyjątkowych przypadkach, przez ograniczony okres, który nie może przekraczać czasu niezbędnego do zamknięcia sprawy, w związku z którą przetwarzane są dane, Eurojust może również przetwarzać operacyjne dane osobowe inne niż dane osobowe, o których mowa w załączniku II, odnoszące się do okoliczności przestępstwa, jeżeli dane takie dotyczą bezpośrednio toczącego się postępowania przygotowawczego, które Eurojust koordynuje lub pomaga koordynować, i stanowią jego część, oraz pod warunkiem że przetwarzanie tych danych jest niezbędne dla celów określonych w ust. 1. Inspektor ochrony danych, o którym mowa w art. 36, jest niezwłocznie informowany o przetwarzaniu takich operacyjnych danych osobowych oraz o szczególnych okolicznościach, które uzasadniają konieczność przetwarzania takich danych. W przypadku gdy takie inne dane dotyczą świadków lub poszkodowanych w rozumieniu ust. 2 niniejszego artykułu, decyzja o przetwarzaniu danych podejmowana jest wspólnie przez zainteresowanych przedstawicieli krajowych.

4. Eurojust może przetwarzać szczególne kategorie operacyjnych danych osobowych zgodnie z art. 76 rozporządzenia (UE) 2018/1725. Dane takie nie mogą być przetwarzane w indeksie, o którym mowa w art. 23 ust. 4 niniejszego rozporządzenia. W przypadku gdy takie inne dane dotyczą świadków lub poszkodowanych w rozumieniu ust. 2 niniejszego artykułu, decyzja o przetwarzaniu danych podejmowana jest przez zainteresowanych przedstawicieli krajowych.

Artykuł 28

Przetwarzanie z upoważnienia Eurojustu lub podmiotu przetwarzającego

Podmiot przetwarzający i osoba działająca z upoważnienia Eurojustu lub podmiotu przetwarzającego, która ma dostęp do operacyjnych danych osobowych, przetwarzają je wyłącznie na polecenie Eurojustu, chyba że są oni zobowiązani do przetwarzania danych na podstawie prawa Unii lub prawa państwa członkowskiego.

Artykuł 29

Terminy przechowywania operacyjnych danych osobowych

1. Operacyjne dane osobowe przetwarzane przez Eurojust są przechowywane przez Eurojust tylko tak długo, jak długo jest to niezbędne do wykonywania jego zadań. W szczególności, z zastrzeżeniem ust. 3 niniejszego artykułu, operacyjne dane osobowe, o których mowa w art. 27, nie mogą być przechowywane po tym spośród poniższych terminów, który nastąpi wcześniej:

a) terminie, w którym upłynął okres przedawnienia ścigania we wszystkich państwach członkowskich, których dotyczą postępowanie przygotowawcze oraz wniesienie i popieranie oskarżenia;

b) terminie, w którym Eurojust został poinformowany o tym, że dana osoba została uniewinniona, a orzeczenie sądowe stało się ostateczne; w takim przypadku zainteresowane państwo członkowskie niezwłocznie informuje o tym Eurojust;

c) terminie trzech lat od dnia, w którym orzeczenie sądowe ostatniego z państw członkowskich, których dotyczą postępowanie przygotowawcze lub wniesienie i popieranie oskarżenia, stało się ostateczne;

d) terminie, w którym Eurojust i zainteresowane państwa członkowskie wspólnie stwierdziły lub ustaliły, że nie jest już konieczne, by Eurojust koordynował postępowanie przygotowawcze oraz wniesienie i popieranie oskarżenia, chyba że istnieje obowiązek przedstawiania Eurojustowi takich informacji zgodnie z art. 21 ust. 5 lub 6;

e) terminie trzech lat od dnia, w którym przekazano operacyjne dane osobowe zgodnie z art. 21 ust. 5 lub 6.

2. Przestrzeganie terminów przechowywania, o których mowa w ust. 1 niniejszego artykułu, jest stale sprawdzane przez Eurojust przy pomocy właściwych środków automatycznego przetwarzania, w szczególności od momentu, w którym Eurojust zamyka sprawę. Co trzy lata od wprowadzenia danych sprawdzana jest również celowości ich przechowywania; rezultaty takiego sprawdzenia stosuje się do całej sprawy. Jeżeli operacyjne dane osobowe, o których mowa w art. 27 ust. 4, przechowywane są przez okres dłuższy niż pięć lat, informuje się o tym EIOD.

3. Przed upływem jednego z terminów przechowywania, o których mowa w ust. 1, Eurojust sprawdza, czy i jak długo konieczne jest dalsze przechowywanie operacyjnych danych osobowych do celów wykonywania jego zadań. Eurojust może zdecydować na zasadzie odstępstwa o przechowywaniu takich danych do czasu następnego sprawdzenia. Powody dalszego przechowywania należy uzasadnić i odnotować. Jeżeli w momencie sprawdzenia nie podjęto decyzji o dalszym przechowywaniu operacyjnych danych osobowych, dane te są automatycznie usuwane.

4. W przypadku gdy zgodnie z ust. 3 operacyjne dane osobowe były przechowywane po upływie terminów przechowywania, o których mowa w ust. 1, EIOD dokonuje również przeglądu celowości przechowywania tych danych co trzy lata.

5. Po upływie terminu przechowywania ostatniej pozycji zautomatyzowanych danych w aktach wszystkie dokumenty w tych aktach zostają zniszczone, z wyjątkiem wszelkich oryginalnych dokumentów, które Eurojust otrzymał od organów krajowych i które należy zwrócić organowi, który je dostarczył.

6. W przypadku gdy Eurojust koordynował postępowanie przygotowawcze lub wniesienie i popieranie oskarżenia, zainteresowani przedstawiciele krajowi informują się wzajemnie o umorzeniu sprawy lub o tym, że wszystkie orzeczenia sądowe związane ze sprawą stały się ostateczne.

7. Ust. 5 nie ma zastosowania, jeżeli:

a) naruszałoby to interesy wymagającej ochrony osoby, której dane dotyczą; w takich przypadkach operacyjne dane osobowe wykorzystywane są jedynie za wyraźną i pisemną zgodą osoby, której dane dotyczą;

b) osoba, której operacyjne dane osobowe dotyczą, kwestionuje ich prawidłowość; w takich przypadkach ust. 5 nie ma zastosowania przez okres umożliwiający państwom członkowskim lub, w stosownych przypadkach, Europolowi weryfikację prawidłowości tych danych;

c) operacyjne dane osobowe muszą być zachowane do celów dowodowych lub ustalenia, dochodzenia lub obrony roszczeń przed sądem;

d) osoba, której dane dotyczą, sprzeciwia się usunięciu operacyjnych danych osobowych, a zamiast tego występuje o ograniczenie ich wykorzystywania; lub

e) operacyjne dane osobowe są nadal potrzebne do celów archiwalnych w interesie publicznym lub do celów statystycznych.

Artykuł 30

Bezpieczeństwo operacyjnych danych osobowych

Eurojust i państwa członkowskie określają mechanizmy mające na celu zapewnienie uwzględniania środków bezpieczeństwa, o których mowa w art. 91 rozporządzenia (UE) 2018/1725, ponad granicami systemów informacyjnych.

Artykuł 31

Prawo dostępu przysługujące osobie, której dane dotyczą

1. Osoba, której dane dotyczą, pragnąca skorzystać z prawa dostępu, o którym mowa w art. 80 rozporządzenia (UE) 2018/1725, do dotyczących tej osoby operacyjnych danych osobowych, które są przetwarzane przez Eurojust, może złożyć wniosek do Eurojustu lub do krajowego organu nadzorczego w wybranym przez siebie państwie członkowskim. Organ ten niezwłocznie, a w każdym razie nie później niż w ciągu miesiąca od otrzymania wniosku, przekazuje go Eurojustowi.

2. Eurojust odpowiada na wniosek bez zbędnej zwłoki, a w każdym razie nie później niż w ciągu trzech miesięcy od jego otrzymania.

3. Eurojust konsultuje się z właściwymi organami zainteresowanych państw członkowskich w sprawie decyzji podejmowanej w odpowiedzi na wniosek. Decyzja o dostępie do danych jest podejmowana przez Eurojust wyłącznie w ścisłej współpracy z państwami członkowskimi, których przekazanie takich danych bezpośrednio dotyczy. W przypadku gdy państwo członkowskie sprzeciwia się proponowanej decyzji Eurojustu, przekazuje Eurojustowi uzasadnienie sprzeciwu. Eurojust stosuje się do takiego sprzeciwu. Odnośni przedstawiciele krajowi informują następnie właściwe organy o treści decyzji Eurojustu.

4. Zainteresowani przedstawiciele krajowi rozpatrują wniosek i podejmują decyzję w imieniu Eurojustu. W przypadku gdy zainteresowani przedstawiciele krajowi nie mogą osiągnąć porozumienia, przekazują sprawę kolegium, które podejmuje decyzję w sprawie wniosku większością dwóch trzecich głosów.

Artykuł 32

Ograniczenia prawa dostępu

W przypadkach, o których mowa w art. 81 rozporządzenia (UE) 2018/1725, Eurojust przekazuje informacje osobie, której dane dotyczą, po skonsultowaniu się z właściwymi organami zainteresowanych państw członkowskich zgodnie z art. 31 ust. 3 niniejszego rozporządzenia.

Artykuł 33

Ograniczenia przetwarzania

Z zastrzeżeniem wyjątków ustanowionych w art. 29 ust. 7 tego rozporządzenia, w przypadku gdy przetwarzanie operacyjnych danych osobowych jest ograniczone na mocy art. 82 ust. 3 rozporządzenia (UE) 2018/1725 takie operacyjne dane osobowe są przetwarzane wyłącznie do celów ochrony praw osoby, której dane dotyczą, lub innej osoby fizycznej lub prawnej będącej stroną postępowania, którego stroną jest Eurojust, lub do celów określonych w art. 82 ust. 3 rozporządzenia (UE) 2018/1725.

Artykuł 34

Udzielenie dostępu do operacyjnych danych osobowych w ramach Eurojustu

Tylko przedstawiciele krajowi, ich zastępcy i asystenci, upoważnieni oddelegowani eksperci krajowi oraz osoby, o których mowa w art. 20 ust. 3, jeżeli osoby te są podłączone do zautomatyzowanego systemu zarządzania sprawami, oraz upoważniony personel Eurojustu mogą, w celu wykonywania zadań Eurojustu" mieć dostęp do operacyjnych danych osobowych przetwarzanych przez Eurojust z zachowaniem ograniczeń przewidzianych w art. 23, 24 i 25.

Artykuł 35

Rejestry kategorii czynności przetwarzania

1. Eurojust prowadzi rejestr wszystkich kategorii czynności przetwarzania, za które odpowiada. Rejestr ten zawiera wszystkie następujące informacje:

a) dane kontaktowe Eurojustu oraz imię i nazwisko i dane kontaktowe inspektora ochrony danych;

b) cele przetwarzania;

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

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

e) w stosownych przypadkach informacje o przekazaniu operacyjnych danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej;

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. 91 rozporządzenia (UE) 2018/1725.

2. Rejestr, o którym mowa w ust. 1, ma formę pisemną, w tym formę elektroniczną.

3. Eurojust udostępnia rejestr EIOD na jego wniosek.

Artykuł 36

Wyznaczenie inspektora ochrony danych

1. Zarząd wyznacza inspektora ochrony danych. Inspektor ochrony danych jest członkiem personelu specjalnie powołanym do pełnienia tej funkcji. Wykonując swoje zadania, inspektor ochrony danych działa niezależnie i nie może przyjmować żadnych instrukcji.

2. Inspektora ochrony danych wybiera się na podstawie jego kwalifikacji zawodowych oraz, w szczególności, wiedzy fachowej na temat prawa i praktyki w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań wynikających z niniejszego rozporządzenia, w szczególności tych, o których mowa w art. 38.

3. Wybór inspektora ochrony danych nie może powodować konfliktu interesów między jego obowiązkami jako inspektora ochrony danych a innymi jego obowiązkami służbowymi, w szczególności w odniesieniu do stosowania niniejszego rozporządzenia.

4. Inspektor ochrony danych zostaje powołany na okres czterech lat i może zostać ponownie powołany na maksymalny łączny okres ośmiu lat. Inspektor ochrony danych może zostać odwołany ze swojego stanowiska przez zarząd tylko za zgodą EIOD, jeśli przestał spełniać warunki konieczne do wykonywania swoich obowiązków.

5. Eurojust publikuje dane kontaktowe inspektora ochrony danych i przekazuje je EIOD.

Artykuł 37

Status inspektora ochrony danych

1. Eurojust zapewnia właściwe i odpowiednio wczesne włączanie inspektora ochrony danych we wszystkie sprawy dotyczące ochrony danych osobowych.

2. Eurojust wspiera inspektora ochrony danych w wypełnianiu przez niego zadań, o których mowa w art. 38, zapewniając mu zasoby i personel niezbędne do wykonywania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej.

3. Eurojust zapewnia, aby inspektor ochrony danych nie otrzymywał instrukcji dotyczących wykonywania swoich zadań. Inspektor ochrony danych nie może zostać odwołany ani ukarany przez zarząd za wypełnianie swoich zadań. Inspektor ochrony danych podlega bezpośrednio kolegium w odniesieniu do operacyjnych danych osobowych oraz zarządowi w odniesieniu do administracyjnych danych osobowych.

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 oraz na mocy rozporządzenia (UE) 2018/1725.

5. Zarząd przyjmuje przepisy wykonawcze dotyczące inspektora ochrony danych. Przepisy wykonawcze dotyczą w szczególności procedury wyboru na stanowisko inspektora ochrony danych, odwołania z tego stanowiska, a także zadań, obowiązków i uprawnień oraz ochrony niezależności inspektora ochrony danych.

6. Inspektor ochrony danych i jego personel podlegają obowiązkowi zachowania poufności zgodnie z art. 72.

7. Administrator i podmiot przetwarzający, odpowiedni komitet personelu i dowolne osoby mogą konsultować się z inspektorem ochrony danych, w każdej sprawie dotyczącej wykładni lub stosowania niniejszego rozporządzenia i rozporządzenia (UE) 2018/1725 bez korzystania z kanałów oficjalnych. Nikt nie może doznać uszczerbku z powodu tego, że zwrócił uwagę odpowiedniego inspektora ochrony danych na fakt zarzucanego naruszenia niniejszego rozporządzenia lub rozporządzenia (UE) 2018/1725.

8. Po powołaniu na stanowisko inspektor ochrony danych jest rejestrowany u EIOD przez Eurojust.

Artykuł 38

Zadania inspektora ochrony danych

1. W odniesieniu do przetwarzania danych osobowych inspektor ochrony danych ma w szczególności następujące zadania:

a) zapewnienie w sposób niezależny przestrzegania przez Eurojust przepisów dotyczących ochrony danych zawartych w niniejszym rozporządzeniu, rozporządzenia (UE) nr 2018/1725 oraz odpowiednich przepisów dotyczących ochrony danych zawartych w regulaminie wewnętrznym Eurojust; obejmuje to monitorowanie przestrzegania niniejszego rozporządzenia, rozporządzenia (UE) 2018/1725, innych unijnych lub krajowych przepisów o ochronie danych oraz strategii Eurojustu w dziedzinie ochrony danych osobowych, w tym podziału obowiązków, działań uświadamiających, szkoleń pracowników uczestniczących w operacjach przetwarzania oraz powiązanych z tym audytów;

b) informowanie Eurojustu oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia, rozporządzenia (UE) 2018/1725 oraz innych unijnych lub krajowych przepisów o ochronie danych i doradzanie im w tej sprawie;

c) udzielanie na wniosek porad co do oceny skutków dla ochrony danych oraz monitorowanie jej wyników zgodnie z art. 89 rozporządzenia 2018/1725;

d) zapewnianie, aby przekazywanie i otrzymywanie danych osobowych było rejestrowane zgodnie z przepisami, które zostaną określone w regulaminie wewnętrznym Eurojustu;

e) współpraca z pracownikami Eurojustu odpowiedzialnymi za procedury, szkolenia i doradztwo w zakresie przetwarzania danych;

f) współpraca z EIOD;

g) zapewnianie, aby osoby, których dane dotyczą, były informowane o prawach przysługujących im na mocy niniejszego rozporządzenia oraz rozporządzenia (UE) 2018/1725;

h) pełnienie funkcji punktu kontaktowego dla EIOD w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 90 rozporządzenia (UE) 2018/1725, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach;

i) udzielanie na wniosek porad co do konieczności zgłoszenia naruszenia ochrony danych osobowych lub zawiadomienia o takim naruszeniu na podstawie przepisów art. 92 i 93 rozporządzenia (UE) 2018/1725;

j) przygotowanie rocznego sprawozdania i przekazanie go zarządowi, kolegium oraz EIOD.

2. Inspektor ochrony danych pełni funkcje określone w rozporządzeniu (UE) 2018/1725 w odniesieniu do administracyjnych danych osobowych.

3. Inspektor ochrony danych i pracownicy Eurojustu wspomagający inspektora ochrony danych w wykonywaniu jego obowiązków mają dostęp do danych osobowych przetwarzanych przez Eurojust oraz do jego pomieszczeń w zakresie niezbędnym do realizacji swoich zadań.

4. Jeśli inspektor ochrony danych uzna, że przepisy rozporządzenia (UE) 2018/1725 dotyczące przetwarzania administracyjnych danych osobowych lub że przepisy niniejszego rozporządzenia lub art. 3 i rozdział IX rozporządzenia (UE) 2018/1725 dotyczące przetwarzania operacyjnych danych osobowych nie są przestrzegane, informuje o tym zarząd i wzywa go do usunięcia tego naruszenia w określonym terminie. Jeżeli zarząd nie usunie w określonym terminie naruszenia, inspektor ochrony danych przekazuje sprawę EIOD.

Artykuł 39

Zgłoszenie naruszenia ochrony danych osobowych odpowiednim organom

1. Jeżeli dojdzie do naruszenia ochrony danych osobowych, Eurojust bez zbędnej zwłoki zgłasza to naruszenie właściwym organom zainteresowanych państw członkowskich.

2. W zgłoszeniu, o którym mowa w ust. 1, muszą znaleźć się co najmniej:

a) opis charakteru naruszenia ochrony danych osobowych, w tym jeżeli to możliwe i stosowne, wskazanie kategorii i liczby osób, których dane dotyczą, oraz kategorii i liczby rekordów danych, których dotyczy naruszenie;

b) opis prawdopodobnych konsekwencji naruszenia ochrony danych osobowych;

c) opis środków zaproponowanych lub przedsięwziętych przez Eurojust w celu zaradzenia naruszeniu ochrony danych osobowych oraz

d) w stosownych przypadkach zalecenie co do środków mających zminimalizować ewentualne negatywne skutki naruszenia ochrony danych osobowych.

Artykuł 40

Nadzór ze strony EIOD

1. EIOD jest odpowiedzialny za monitorowanie i zapewnianie stosowania przepisów niniejszego rozporządzenia i rozporządzenia (UE) 2018/1725 dotyczących ochrony podstawowych praw i wolności osób fizycznych w zakresie przetwarzania operacyjnych danych osobowych przez Eurojust oraz za doradzanie Eurojustowi i osobom, których dane dotyczą, we wszelkich sprawach związanych z przetwarzaniem operacyjnych danych osobowych. W tym celu EIOD wykonuje obowiązki określone w ust. 2 niniejszego artykułu, korzysta z uprawnień przyznanych mu w ust. 3 niniejszego artykułu i współpracuje z krajowymi organami nadzorczymi zgodnie z art. 42.

2. EIOD ma na mocy niniejszego rozporządzenia oraz rozporządzenia (UE) 2018/1725 następujące obowiązki:

a) przyjmowanie i rozpatrywanie skargi oraz informowanie osoby, której dane dotyczą, w rozsądnym terminie, o wyniku tych działań;

b) prowadzenie postępowań wyjaśniających, zarówno z własnej inicjatywy, jak i na podstawie skarg, oraz informowanie osoby, której dane dotyczą, w rozsądnym terminie, o wyniku tych postępowań;

c) monitorowanie i zapewnianie stosowania przez Eurojust przepisów niniejszego rozporządzenia oraz rozporządzenia (UE) 2018/1725 dotyczących ochrony osób fizycznych w odniesieniu do przetwarzania operacyjnych danych osobowych przez Eurojust;

d) doradzanie Eurojustowi – z własnej inicjatywy lub w odpowiedzi na konsultacje – we wszystkich kwestiach związanych z przetwarzaniem operacyjnych danych osobowych, w szczególności zanim Eurojust przyjmie przepisy wewnętrzne dotyczące ochrony podstawowych praw i wolności w odniesieniu do przetwarzania operacyjnych danych osobowych.

3. Na mocy niniejszego rozporządzenia oraz rozporządzenia (UE) 2018/1725, uwzględniając skutki dla postępowań przygotowawczych oraz wniesienia i popierania oskarżeń w państwach członkowskich, EIOD może:

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

b) przekazać sprawę Eurojustowi w przypadku zarzutu naruszenia przepisów regulujących przetwarzanie operacyjnych danych osobowych i w stosownych przypadkach przedstawić propozycje usunięcia tego naruszenia i poprawy ochrony osób, których dane dotyczą;

c) konsultować się z Eurojustem, jeżeli wnioski o skorzystanie z określonych praw w odniesieniu do operacyjnych danych osobowych zostały odrzucone z naruszeniem art. 31, 32 lub 33 niniejszego rozporządzenia lub art. 77–82 lub art. 84 rozporządzenia (UE) 2018/1725;

d) ostrzegać Eurojust;

e) nakazać Eurojustowi, by dokonał sprostowania operacyjnych danych osobowych przetwarzanych przez Eurojust z naruszeniem przepisów dotyczących przetwarzania operacyjnych danych osobowych, ograniczył przetwarzanie takich danych lub usunął takie dane oraz by powiadomił o takich działaniach osoby trzecie, którym takie dane zostały ujawnione, o ile nie koliduje to z zadaniami Eurojustu określonymi w art. 2;

f) przekazać sprawę Trybunałowi Sprawiedliwości Unii Europejskiej (zwanemu dalej „Trybunałem”) zgodnie z warunkami określonymi w TFUE;

g) interweniować w sprawach wniesionych do Trybunału.

4. EIOD ma dostęp do operacyjnych danych osobowych przetwarzanych przez Eurojust oraz do jej pomieszczeń w zakresie niezbędnym do realizacji swoich zadań.

5. EIOD sporządza roczne sprawozdanie ze swej działalności nadzorczej w odniesieniu do Eurojustu. Sprawozdanie to stanowi część sprawozdania rocznego EIOD, o którym mowa w art. 60 rozporządzenia (UE) 2018/1725. Krajowe organy nadzorcze są proszone o przedstawienie uwag na temat tego sprawozdania, zanim stanie się ono częścią sprawozdania rocznego EIOD, o którym mowa w art. 60 rozporządzenia (UE) 2018/1725. EIOD w największym możliwym stopniu uwzględnia uwagi krajowych organów nadzorczych i w każdym razie odnosi się do nich w sprawozdaniu rocznym.

6. Na wniosek EIOD Eurojust współpracuje z nim w wykonywaniu jego obowiązków.

Artykuł 41

Obowiązek zachowania tajemnicy służbowej przez EIOD

1. EIOD oraz jego pracownicy podlegają – w trakcie kadencji i po jej zakończeniu – obowiązkowi zachowania tajemnicy służbowej w odniesieniu do wszelkich informacji poufnych, które uzyskali w trakcie wykonywania obowiązków służbowych.

2. EIOD, w ramach wykonywania swoich uprawnień nadzorczych, uwzględnia w najwyższym stopniu tajemnicę postępowania sądowego i postępowania przygotowawczego, zgodnie z prawem Unii lub prawem państwa członkowskiego.

Artykuł 42

Współpraca między EIOD a krajowymi organami nadzorczymi

1. EIOD działa w ścisłej współpracy z krajowymi organami nadzorczymi w konkretnych kwestiach wymagających podjęcia działań krajowych, w szczególności jeżeli EIOD lub krajowy organ nadzorczy stwierdzi znaczące rozbieżności między praktykami państw członkowskich lub stwierdzi potencjalnie niezgodne z prawem przekazanie przy wykorzystaniu kanałów komunikacji Eurojustu, lub w kontekście zapytań zgłoszonych przez co najmniej jeden krajowy organ nadzorczy w sprawie wykonania i wykładni niniejszego rozporządzenia.

2. W przypadkach, o których mowa w ust. 1, zapewnia się skoordynowany nadzór zgodnie z art. 62 rozporządzenia (UE) nr 2018/1725.

3. EIOD w pełni informuje krajowe organy nadzorcze o wszelkich kwestiach, które mają na nie bezpośredni wpływ lub dotyczą ich w inny sposób. Na wniosek co najmniej jednego krajowego organu nadzorczego EIOD informuje te organy o konkretnych kwestiach.

4. W przypadkach dotyczących danych pochodzących z co najmniej jednego państwa członkowskiego, w tym w przypadkach, o których mowa w art. 43 ust. 3, EIOD konsultuje się z zainteresowanymi krajowymi organami nadzorczymi. EIOD nie podejmuje decyzji o dalszych działaniach, zanim te krajowe organy nadzorcze nie poinformują EIOD o zajmowanym stanowisku w określonym przez EIOD terminie. Termin ten nie może być krótszy niż jeden miesiąc ani dłuższy niż trzy miesiące. EIOD uwzględnia w największym możliwym stopniu stanowisko zainteresowanych krajowych organów nadzorczych. W przypadkach gdy EIOD nie zamierza uwzględnić tego stanowiska, informuje o tym te organy, przedstawia uzasadnienie i kieruje daną sprawę do Europejskiej Rady Ochrony Danych.

W przypadkach uznanych przez EIOD za nadzwyczaj pilne może on podjąć natychmiastowe działania. W takich przypadkach EIOD niezwłocznie informuje krajowe organy nadzorcze i wykazuje pilny charakter sytuacji, a także uzasadnia podjęte przez niego działanie.

5. Krajowe organy nadzorcze informują EIOD o wszelkich działaniach, które podejmują w odniesieniu do przekazywania, pobierania lub każdego innego udostępniania operacyjnych danych osobowych przez państwa członkowskie na mocy niniejszego rozporządzenia.

Artykuł 43

Prawo do złożenia skargi do EIOD w odniesieniu do operacyjnych danych osobowych

1. Każda osoba, której dane dotyczą, ma prawo do złożenia skargi do EIOD, jeżeli uważa, że przetwarzanie przez Eurojust dotyczących jej operacyjnych danych osobowych nie jest zgodne z niniejszym rozporządzeniem lub rozporządzeniem (UE) 2018/1725.

2. Jeżeli skarga dotyczy decyzji, o której mowa w art. 31, 32 lub 33 niniejszego rozporządzenia lub art. 80, 81 lub 82 rozporządzenia (UE) 2018/1725, EIOD zasięga opinii krajowych organów nadzorczych lub właściwego organu sądowego państwa członkowskiego, które dostarczyło dane, lub bezpośrednio zainteresowanego państwa członkowskiego. Przy podejmowaniu decyzji, która może obejmować odmowę udostępnienia jakichkolwiek informacji, EIOD uwzględnia opinię krajowego organu nadzorczego lub właściwego organu sądowego.

3. Jeżeli skarga dotyczy przetwarzania danych dostarczonych Eurojustowi przez państwo członkowskie, EIOD i krajowy organ nadzorczy państwa członkowskiego, które dostarczyło te dane, zapewniają, działając w zakresie swoich odpowiednich kompetencji, prawidłowe przeprowadzenie niezbędnych kontroli zgodności przetwarzania tych danych z prawem.

4. Jeżeli skarga dotyczy przetwarzania danych dostarczonych Eurojustowi przez organy lub jednostki organizacyjne Unii, przez państwa trzecie lub organizacje międzynarodowe lub przetwarzania danych pobranych przez Eurojust z publicznie dostępnych źródeł, EIOD zapewnia prawidłowe przeprowadzenie przez Eurojust niezbędnych kontroli zgodności przetwarzania tych danych z prawem.

5. EIOD informuje osobę, której dane dotyczą, o przebiegu i wyniku rozpatrzenia skargi, jak również o możliwości wniesienia środka odwoławczego na mocy art. 44.

Artykuł 44

Prawo do kontroli sądowej w odniesieniu do decyzji EIOD

Odwołania od decyzji EIOD dotyczących operacyjnych danych osobowych wnoszone są do Trybunału.

Artykuł 45

Odpowiedzialność w sprawach dotyczących ochrony danych

1. Eurojust przetwarza operacyjne dane osobowe w taki sposób, by można było ustalić, który organ dostarczył dane lub skąd je pobrano.

2. Za prawidłowość operacyjnych danych osobowych odpowiada:

a) Eurojust – w odniesieniu do operacyjnych danych osobowych dostarczonych przez państwo członkowskie lub instytucję, organ lub jednostkę organizacyjną Unii, w przypadku gdy dostarczone dane uległy zmianie w toku ich przetwarzania przez Eurojust;

b) państwo członkowskie lub instytucja, organ lub jednostka organizacyjna Unii, które dostarczyły danych Eurojustowi – w przypadku gdy dostarczone dane nie uległy zmianie w toku ich przetwarzania przez Eurojust;

c) Eurojust – w odniesieniu do operacyjnych danych osobowych dostarczonych przez państwa trzecie lub organizacje międzynarodowe, a także w odniesieniu do operacyjnych danych osobowych pobranych przez Eurojust z publicznie dostępnych źródeł.

3. Za zgodność z rozporządzeniem (UE) 2018/1725 w odniesieniu do administracyjnych danych osobowych oraz za zgodność z niniejszym rozporządzeniem, z art. 3 i z rozdziałem IX rozporządzenia (UE) 2018/1725 w odniesieniu do operacyjnych danych osobowych odpowiada Eurojust.

Za zgodność przekazania operacyjnych danych osobowych z prawem odpowiada:

a) państwo członkowskie – w przypadku gdy państwo członkowskie dostarczyło te operacyjne dane osobowe Eurojustowi;

b) Eurojust – w przypadku gdy Eurojust dostarczył operacyjne dane osobowe państwom członkowskim, instytucjom, organom lub jednostkom organizacyjnym Unii, państwom trzecim lub organizacjom międzynarodowym.

4. Z zastrzeżeniem innych przepisów niniejszego rozporządzenia Eurojust jest odpowiedzialny za wszystkie dane, które przetwarza..

Artykuł 46

Odpowiedzialność za nieuprawnione lub niewłaściwe przetwarzanie danych

1. Zgodnie z art. 340 TFUE Eurojust odpowiada za wszelkie szkody wyrządzone osobom fizycznym, wynikające z prowadzonego przez niego nieuprawnionego lub niewłaściwego przetwarzania danych.

2. Skargi przeciwko Eurojustowi dotyczące odpowiedzialności, o której mowa w ust. 1 niniejszego artykułu, rozstrzyga Trybunał zgodnie z art. 268 TFUE.

3. Każde państwo członkowskie jest odpowiedzialne, zgodnie z jego prawem krajowym, za wszelkie szkody wyrządzone osobom fizycznym, wynikające z prowadzonego przez nie nieuprawnionego lub niewłaściwego przetwarzania danych przekazanych do Eurojustu.

ROZDZIAŁ V

STOSUNKI Z PARTNERAMI

SEKCJA I

przepisy wspólne

Artykuł 47

Przepisy wspólne

1. W zakresie, w jakim jest to konieczne do wykonywania zadań Eurojustu, może on nawiązywać i prowadzić współpracę z instytucjami, organami i jednostkami organizacyjnymi Unii zgodnie z ich odpowiednimi celami, z właściwymi organami państw trzecich i organizacjami międzynarodowymi, zgodnie ze strategią współpracy, o której mowa w art. 52.

2. W zakresie, w jakim jest to istotne dla wykonywania zadań Eurojustu, z zastrzeżeniem wszelkich ograniczeń zgodnie z art. 21 ust. 8 i art. 76, Eurojust może wymieniać wszystkie informacje, z wyjątkiem danych osobowych, bezpośrednio z podmiotami, o których mowa w ust. 1 niniejszego artykułu.

3. Do celów określonych w ust. 1 i 2 Eurojust może zawierać uzgodnienia robocze z podmiotami, o których mowa w ust. 1. Takie uzgodnienia robocze nie stanowią podstawy do umożliwienia wymiany danych osobowych i nie są wiążące dla Unii ani jej państw członkowskich.

4. Eurojust może otrzymywać i przetwarzać dane osobowe pochodzące od podmiotów, o których mowa w ust. 1, w zakresie, w jakim jest to niezbędne do realizacji jego zadań, z zastrzeżeniem mających zastosowanie przepisów dotyczących ochrony danych.

5. Eurojust przekazuje dane osobowe instytucjom, organom lub jednostkom organizacyjnym Unii, państwom trzecim lub organizacjom międzynarodowym wyłącznie wtedy, jeżeli jest to konieczne do wykonania jego zadań oraz jest zgodne z art. 55 i 56. Jeżeli dane, które mają zostać przekazane, zostały dostarczone przez państwo członkowskie, Eurojust uzyskuje zgodę odpowiedniego właściwego organu w tym państwie członkowskim, chyba że dane państwo członkowskie udzieliło uprzedniej zgody na takie dalsze przekazanie, ogólnie lub na specjalnych warunkach. Taką zgodę można w każdej chwili wycofać.

6. W przypadku gdy państwo członkowskie, instytucje, organy lub jednostki organizacyjne Unii, państwa trzecie lub organizacje międzynarodowe otrzymały dane osobowe od Eurojustu, dalsze przekazywanie takich danych osobom trzecim jest zakazane, chyba że spełnione są wszystkie następujące warunki:

a) Eurojust uzyskał uprzednią zgodę państwa członkowskiego, które dostarczyło te dane;

b) Eurojust, po rozważeniu okoliczności przedmiotowej sprawy, udzielił na to wyraźnej zgody;

c) dalsze przekazanie odbywa się wyłącznie w określonym celu, który nie jest niezgodny z celem, dla którego dane te zostały przesłane.

SEKCJA II

Stosunki z partnerami w Unii

Artykuł 48

Współpraca z Europejską Siecią Sądową i innymi sieciami działającymi w Unii, które prowadzą współpracę wymiarów sprawiedliwości w sprawach karnych

1. Eurojust utrzymuje uprzywilejowane stosunki z Europejską Siecią Sądową w sprawach karnych, oparte na konsultacjach i komplementarności, w szczególności między przedstawicielem krajowym, punktami kontaktowymi Europejskiej Sieci Sądowej w tym samym państwie członkowskim, co przedstawiciel krajowy oraz korespondentami krajowymi Eurojustu i Europejskiej Sieci Sądowej. W celu zapewnienia skutecznej współpracy podejmuje się następujące środki:

a) w poszczególnych przypadkach przedstawiciele krajowi informują punkty kontaktowe Europejskiej Sieci Sądowej o wszelkich sprawach, w przypadku których uważają, że Sieć ta ma lepsze warunki, by się nimi zająć;

b) sekretariat Europejskiej Sieci Sądowej stanowi część personelu Eurojustu; działa on jako odrębna jednostka; może on korzystać z administracyjnych zasobów Eurojustu, które są potrzebne Europejskiej Sieci Sądowej do realizacji jej zadań, w tym do pokrywania kosztów posiedzeń plenarnych Sieci;

c) punkty kontaktowej Europejskiej Sieci Sądowej mogą być zapraszane, w poszczególnych przypadkach, do udziału w posiedzeniach Eurojustu;

d) Eurojust i Europejska Sieć Sądowa mogą korzystać z krajowego systemu koordynacyjnego Eurojustu przy ustalaniu, na podstawie art. 20 ust. 7 lit. b), czy dany wniosek należy rozpatrywać z wykorzystaniem Eurojustu, czy Europejskiej Sieci Sądowej.

2. Sekretariat sieci wspólnych zespołów dochodzeniowo-śledczych oraz sekretariat sieci utworzonej decyzją Rady 2002/494/WSiSW stanowią część personelu Eurojustu. Sekretariaty te działają jako odrębne jednostki. Mogą one korzystać z zasobów administracyjnych Eurojustu, które są im potrzebne do realizacji ich zadań. Eurojust zapewnia koordynację między tymi sekretariatami. Niniejszy ustęp stosuje się do sekretariatu każdej odpowiedniej sieci zaangażowanej we współpracę wymiarów sprawiedliwości w sprawach karnych, w przypadku której Eurojust ma zapewniać wsparcie w postaci sekretariatu. Eurojust może wspierać odpowiednie sieci i organy europejskie zaangażowane we współpracę wymiarów sprawiedliwości w sprawach karnych, w tym w razie potrzeby za pośrednictwem sekretariatu w siedzibie Eurojustu.

3. Sieć utworzona decyzją 2008/852/WSiSW może wystąpić do Eurojustu o zapewnienie jej sekretariatu. W takim przypadku stosuje się ust. 2.

Artykuł 49

Stosunki z Europolem

1. Eurojust podejmuje wszelkie stosowne środki, aby umożliwić Europolowi, w ramach zakresu działania Europolu, pośredni dostęp do informacji dostarczonych Eurojustowi w oparciu o system trafieniowy (figuruje/nie figuruje), z zastrzeżeniem wszelkich ograniczeń wskazanych przez państwo członkowskie, organ lub jednostkę organizacyjną Unii, państwo trzecie lub organizację międzynarodową, które dostarczyły danych informacji. W przypadku trafienia Eurojust wszczyna procedurę, dzięki której można wymieniać informacje będące przedmiotem trafienia, zgodnie z decyzją państwa członkowskiego, organu lub jednostki organizacyjnej Unii, państwa trzeciego lub organizacji międzynarodowej, które dostarczyły informacje Eurojustowi.

2. Wyszukiwania informacji zgodnie z ust. 1 dokonuje się jedynie w celu ustalenia, czy informacje dostępne w Europolu pasują do informacji przetwarzanych w Eurojuście.

3. Eurojust umożliwia wyszukiwanie zgodnie z ust. 1 jedynie po otrzymaniu od Europolu informacji na temat tego, których członków personelu wyznaczono do przeprowadzenia takiego wyszukiwania.

4. Jeżeli podczas działań Eurojustu związanych z przetwarzaniem informacji w odniesieniu do danego postępowania przygotowawczego Eurojust lub dane państwo członkowskie stwierdzi potrzebę koordynacji, współpracy lub wsparcia zgodnie z zakresem działania Europolu, Eurojust powiadamia o tym Europol oraz wszczyna procedurę wymiany informacji, zgodnie z decyzją państwa członkowskiego dostarczającego informacje. W takim przypadku Eurojust konsultuje się z Europolem.

5. Eurojust nawiązuje i prowadzi ścisłą współpracę z Europolem w stopniu, w jakim jest to istotne dla wykonywania zadań obu agencji oraz dla osiągnięcia ich celów, biorąc pod uwagę potrzebę unikania powielania pracy.

W tym celu dyrektor wykonawczy Europolu i przewodniczący Eurojustu odbywają regularne spotkania, aby omówić kwestie będące przedmiotem wspólnego zainteresowania.

6. Europol przestrzega wszelkich ograniczeń dostępu lub wykorzystywania, na ogólnych lub szczególnych warunkach, które zostały wskazane przez państwo członkowskie, organ lub jednostkę organizacyjną Unii, państwo trzecie lub organizację międzynarodową, w odniesieniu do dostarczonych przez nie informacji.

Artykuł 50

Stosunki z Prokuraturą Europejską

1. Eurojust nawiązuje i utrzymuje bliskie stosunki z Prokuraturą Europejską oparte na wzajemnej współpracy w ramach ich zakresów działania i właściwości oraz na utworzeniu określonych w niniejszym artykule wzajemnych powiązań operacyjnych, administracyjnych i zarządczych. W tym celu przewodniczący Eurojustu i Europejski Prokurator Generalny odbywają regularne spotkania, aby omówić kwestie będące przedmiotem wspólnego zainteresowania. Ich spotkania odbywają się na wniosek przewodniczącego Eurojustu lub Europejskiego Prokuratora Generalnego.

2. Eurojust bez zbędnej zwłoki zajmuje się wnioskami o wsparcie pochodzącymi od Prokuratury Europejskiej i w stosownych przypadkach rozpatruje takie wnioski, jak gdyby otrzymał je od organu krajowego właściwego w zakresie współpracy wymiarów sprawiedliwości.

3. W razie potrzeby, aby wspierać współpracę podjętą zgodnie z ust. 1 niniejszego artykułu, Eurojust korzysta z krajowych systemów koordynacyjnych Eurojustu utworzonych zgodnie z art. 20, a także ze stosunków nawiązanych z państwami trzecimi, w tym za pośrednictwem swoich sędziów łącznikowych.

4. W kwestiach operacyjnych odnoszących się do właściwości Prokuratury Europejskiej Eurojust informuje Prokuraturę Europejską oraz, w stosownych przypadkach, włącza ją w swoje działania dotyczące spraw transgranicznych, w tym przez:

a) udostępnienie informacji dotyczących prowadzonych przez siebie spraw, w tym danych osobowych, zgodnie z odpowiednimi przepisami niniejszego rozporządzenia;

b) zwrócenie się do Prokuratury Europejskiej o wsparcie.

5. Eurojust ma pośredni dostęp do informacji znajdujących się w systemie zarządzania sprawami Prokuratury Europejskiej w oparciu o system trafieniowy (figuruje/nie figuruje). Ilekroć znalezione zostanie dopasowanie między danymi wprowadzonymi do systemu zarządzania sprawami przez Prokuraturę Europejską a danymi będącymi w posiadaniu Eurojustu, o znalezieniu takiego dopasowania powiadamia się zarówno Eurojust, jak i Prokuraturę Europejską, a także państwo członkowskie, które dostarczyło dane Eurojustowi. Eurojust podejmuje stosowne środki, aby umożliwić Prokuraturze Europejskiej pośredni dostęp do informacji w systemie zarządzania sprawami w oparciu o system trafieniowy (figuruje/nie figuruje).

6. Prokuratura Europejska może korzystać ze wsparcia i zasobów administracyjnych Eurojustu. W tym celu Eurojust może świadczyć na rzecz Prokuratury Europejskiej usługi będące przedmiotem wspólnego zainteresowania. Szczegóły są regulowane w drodze uzgodnień.

Artykuł 51

Stosunki z pozostałymi organami i jednostkami organizacyjnymi Unii

1. Eurojust nawiązuje i prowadzi współpracę z Europejską Siecią Szkolenia Kadr Wymiaru Sprawiedliwości.

2. OLAF wspomaga pracę koordynacyjną Eurojustu w zakresie ochrony interesów finansowych Unii zgodnie ze swoim zakresem działania na mocy rozporządzenia (UE, Euratom) nr 883/2013.

3. Europejska Agencja Straży Granicznej i Przybrzeżnej wspomaga pracę Eurojustu, w tym przez przesyłanie stosownych informacji przetwarzanych zgodnie z jego zakresem działania i zadaniami wynikającymi z art. 8 ust. 1 lit. m) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/1624 ([1]). Przetwarzanie przez Europejską Agencję Straży Granicznej i Przybrzeżnej danych osobowych w związku z tym jest regulowane rozporządzeniem (UE) 2018/1725.

4. Do celów odbioru i przekazywania informacji między Eurojustem a OLAF, z zastrzeżeniem art. 8 niniejszego rozporządzenia, państwa członkowskie zapewniają, by przedstawiciele krajowi Eurojustu uważani byli za właściwe organy państw członkowskich wyłącznie do celów rozporządzenia (UE, Euratom) nr 883/2013. Wymiana informacji między OLAF a przedstawicielami krajowymi prowadzona jest z zastrzeżeniem obowiązków przekazywania informacji innym właściwym organom na mocy tych rozporządzeń.

SEKCJA III

Współpraca międzynarodowa

Artykuł 52

Stosunki z organami państw trzecich i organizacjami międzynarodowymi

1. Eurojust może nawiązywać i prowadzić współpracę z organami państw trzecich i organizacjami międzynarodowymi.

W tym celu Eurojust, w porozumieniu z Komisją, opracowuje co cztery lata strategię współpracy, określającą państwa trzecie i organizacje międzynarodowe, z którymi ze względów operacyjnych należy współpracować.

2. Eurojust może zawierać uzgodnienia robocze z podmiotami, o których mowa w art. 47 ust. 1.

3. W porozumieniu z zainteresowanymi właściwymi organami Eurojust może wyznaczać punkty kontaktowe w państwach trzecich w celu ułatwienia współpracy stosownie do potrzeb operacyjnych Eurojustu.

Artykuł 53

Sędziowie łącznikowi skierowani na placówkę do państw trzecich

1. Z myślą o ułatwieniu współpracy wymiarów sprawiedliwości z państwami trzecimi w przypadkach, gdy Eurojust zapewnia pomoc zgodnie z niniejszym rozporządzeniem, kolegium może skierować sędziów łącznikowych na placówkę do państwa trzeciego, jeżeli z właściwym organem tego państwa trzeciego zawarto uzgodnienia robocze, o których mowa w art. 47 ust. 3.

2. Zadania sędziów łącznikowych obejmują wszelkie działania zmierzające do wspierania i przyspieszania wszelkich form współpracy wymiarów sprawiedliwości w sprawach karnych, w szczególności przez tworzenie bezpośrednich powiązań z właściwymi organami danego państwa trzeciego. W ramach wykonywania swoich zadań sędziowie łącznikowi mogą dokonywać wymiany operacyjnych danych osobowych z właściwymi organami danego państwa trzeciego zgodnie z art. 56.

3. Sędzia łącznikowy, o którym mowa w ust. 1, musi posiadać doświadczenie w pracy z Eurojustem i odpowiedni poziom wiedzy o współpracy wymiarów sprawiedliwości i działaniu Eurojustu. Skierowanie sędziego łącznikowego na placówkę z ramienia Eurojustu zależy od uprzedniej zgody samego sędziego i jego państwa członkowskiego.

4. Jeżeli sędzia łącznikowy skierowany przez Eurojust na placówkę został wybrany spośród przedstawicieli krajowych, ich zastępców lub asystentów:

a) zainteresowane państwo członkowskie wyznacza inną osobę, która zastępuje go na stanowisku przedstawiciela krajowego, jego zastępcy lub asystenta;

b) nie jest on dłużej uprawniony do wykonywania uprawnień przyznanych mu zgodnie z art. 8.

([1]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/1624 z dnia 14 września 2016 r. w sprawie Europejskiej Straży Granicznej i Przybrzeżnej oraz zmieniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/399 i uchylające rozporządzenie (WE) nr 863/2007 Parlamentu Europejskiego i Rady, rozporządzenie Rady (WE) nr 2007/2004 i decyzję Rady 2005/267/WE (Dz.U. L 251 z 16.9.2016, s. 1).

5. Z zastrzeżeniem art. 110 regulaminu pracowniczego urzędników, kolegium opracowuje warunki kierowania sędziów łącznikowych na placówki, z uwzględnieniem poziomu wynagrodzenia. Kolegium przyjmuje w tym zakresie niezbędne środki wykonawcze w porozumieniu z Komisją.

6. Działania sędziów łącznikowych skierowanych na placówkę przez Eurojust podlegają nadzorowi EIOD. Sędziowie łącznikowi składają sprawozdanie kolegium, które w odpowiedni sposób w sprawozdaniu rocznym informuje Parlament Europejski i Radę o ich działaniach. Sędziowie łącznikowi informują przedstawicieli krajowych i właściwe organy krajowe o wszystkich sprawach dotyczących ich państwa członkowskiego.

7. Właściwe organy państw członkowskich i sędziowie łącznikowi, o których mowa w ust. 1, mogą kontaktować się ze sobą bezpośrednio. W takim przypadku sędzia łącznikowy informuje o takich kontaktach zainteresowanego przedstawiciela krajowego.

8. Sędziowie łącznikowi, o których mowa w ust. 1, są podłączeni do systemu zarządzania sprawami.

Artykuł 54

Wnioski o współpracę wymiarów sprawiedliwości skierowane do państw trzecich i składane przez te państwa

1. Eurojust może za zgodą zainteresowanych państw członkowskich koordynować wykonanie wniosków państwa trzeciego o współpracę wymiarów sprawiedliwości, jeżeli wnioski takie wymagają wykonania w co najmniej dwóch państwach członkowskich w ramach tego samego postępowania przygotowawczego. Takie wnioski mogą być także przekazywane Eurojustowi przez właściwe organy krajowe.

2. W nagłych przypadkach oraz zgodnie z art. 19 wnioski, o których mowa w ust. 1 niniejszego artykułu, wydane przez państwo trzecie, które zawarło z Eurojustem umowę o współpracy lub uzgodnienia robocze, może przyjmować i przekazywać DMK.

3. Z zastrzeżeniem art. 3 ust. 5, jeżeli wnioski o współpracę wymiarów sprawiedliwości dotyczące tego samego postępowania przygotowawczego i wymagające wykonania w państwie trzecim są składane przez zainteresowane państwo członkowskie, Eurojust podejmuje działania w celu ułatwienia współpracy wymiarów sprawiedliwości z tym państwem trzecim.

SEKCJA IV

Przekazywanie danych osobowych

Artykuł 55

Przesyłanie operacyjnych danych osobowych instytucjom, organom i jednostkom organizacyjnym Unii

1. Z zastrzeżeniem dalszych ograniczeń na mocy niniejszego rozporządzenia, w szczególności zgodnie z art. 21 ust. 8, art. 47 ust. 5 i art. 76, Eurojust przesyła operacyjne dane osobowe innym instytucjom, organom lub jednostkom organizacyjnym Unii wyłącznie wówczas, gdy dane te są niezbędne do zgodnego z prawem wykonywania zadań leżących w zakresie właściwości tych instytucji, organów lub jednostek organizacyjnych Unii.

2. Jeżeli operacyjne dane osobowe są przesyłane na wniosek innej instytucji, organu lub jednostki organizacyjnej Unii, zarówno administrator, jak i odbiorca ponoszą odpowiedzialność za zgodność z prawem tego przesłania.

Eurojust jest zobowiązany do sprawdzenia zakresu właściwości tej innej instytucji, organu lub jednostki organizacyjnej Unii i dokonania wstępnej oceny niezbędności przesłania operacyjnych danych osobowych. W razie wątpliwości, czy jest to niezbędne, Eurojust występuje do odbiorcy o udzielenie dalszych informacji.

Inna instytucja, organ lub jednostka organizacyjna Unii zapewnia, by niezbędność przesłania operacyjnych danych mogła być zweryfikowana po dokonaniu przesłania.

3. Inna instytucja, organ lub jednostka organizacyjna Unii przetwarza operacyjne dane osobowe tylko do celów, dla których zostały one przesłane.

Artykuł 56

Zasady ogólne dotyczące przekazywania operacyjnych danych osobowych do państw trzecich i organizacji międzynarodowych

1. Eurojust może przekazywać operacyjne dane osobowe do państwa trzeciego lub organizacji międzynarodowej – z zastrzeżeniem przestrzegania mających zastosowanie przepisów dotyczących ochrony danych i innych przepisów niniejszego rozporządzenia – tylko wtedy, gdy spełnione są następujące warunki:

a) przekazanie jest niezbędne do wykonywania przez Eurojust jego zadań;

b) organ państwa trzeciego lub organizacja międzynarodowa, którym przekazywane są dane operacyjne, są właściwe w zakresie ścigania przestępstw i spraw karnych;

c) jeżeli operacyjne dane osobowe, które mają zostać przekazane zgodnie z niniejszym artykułem, zostały przesłane lub udostępnione Eurojustowi przez jedno z państw członkowskich, Eurojust uzyskuje uprzednią zgodę odpowiedniego właściwego organu tego państwa członkowskiego zgodnie z jego prawem krajowym, chyba że to państwo członkowskie zezwoliło na takie przekazywanie danych – ogólnie lub pod określonymi warunkami;

d) w przypadku dalszego przekazania danych przez państwo trzecie lub organizację międzynarodową do innego państwa trzeciego lub organizacji międzynarodowej Eurojust wymaga od przekazującego państwa trzeciego lub przekazującej organizacji międzynarodowej uzyskania uprzedniej zgody Eurojustu na to dalsze przekazanie.

Eurojust może udzielić zgody na mocy lit. d) wyłącznie po uzyskaniu uprzedniej zgody państwa członkowskiego, z którego dane pochodzą, po należytym uwzględnieniu wszystkich istotnych czynników, w tym wagi przestępstwa, celu, w jakim operacyjne dane osobowe zostały pierwotnie przekazane, oraz stopnia ochrony danych osobowych w państwie trzecim lub organizacji międzynarodowej, do których operacyjne dane osobowe mają zostać dalej przekazane.

2. Z zastrzeżeniem warunków określonych w ust. 1 niniejszego artykułu Eurojust może przekazać operacyjne dane osobowe do państwa trzeciego lub organizacji międzynarodowej tylko w następujących przypadkach:

a) gdy Komisja stwierdziła w drodze decyzji na podstawie art. 57, że dane państwo trzecie lub dana organizacja międzynarodowa zapewniają odpowiedni poziom ochrony, lub – w razie braku takiej decyzji stwierdzającej odpowiedni poziom ochrony – przewidziane są lub istnieją odpowiednie zabezpieczenia zgodnie z art. 58 ust. 1, lub w razie braku zarówno decyzji stwierdzającej odpowiedni poziom ochrony, jak i takich odpowiednich zabezpieczeń, zastosowanie ma odstępstwo w szczególnych sytuacjach zgodnie z art. 59 ust. 1;

b) przed dniem 12 grudnia 2019 r. zawarto umowę o współpracy umożliwiającą wymianę operacyjnych danych osobowych między Eurojustem a danym państwem trzecim lub organizacją międzynarodową zgodnie z art. 26a decyzji 2002/187/WSiSW; lub

c) zawarto umowę międzynarodową między Unią a danym państwem trzecim lub organizacją międzynarodową zgodnie z art. 218 TFUE, która przewiduje odpowiednie zabezpieczenia w odniesieniu do ochrony prywatności oraz podstawowych praw i wolności osób fizycznych.

3. Uzgodnienia robocze, o których mowa w art. 47 ust. 3, mogą być wykorzystywane do określania zasad wykonywania umów lub decyzji stwierdzających odpowiedni poziom ochrony, o których mowa w ust. 2 niniejszego artykułu.

4. Eurojust może w nagłych przypadkach przekazywać operacyjne dane osobowe bez uprzedniej zgody państwa członkowskiego, o której mowa w ust. 1 lit. c). Eurojust może tego dokonać wyłącznie wtedy, gdy przekazanie operacyjnych danych osobowych jest niezbędne do zapobieżenia bezpośredniemu i poważnemu zagrożeniu dla bezpieczeństwa publicznego państwa członkowskiego lub państwa trzeciego lub gdy jest ono niezbędne dla ważnych interesów państwa członkowskiego, a uprzedniej zgody nie da się uzyskać w odpowiednim terminie. Organ odpowiadający za wydanie uprzedniej zgody zostaje powiadomiony niezwłocznie.

5. Państwa członkowskie a także instytucje, organy i jednostki organizacyjne Unii nie mogą przekazywać dalej państwu trzeciemu lub organizacji międzynarodowej operacyjnych danych osobowych otrzymanych od Eurojustu. Na zasadzie wyjątku mogą dokonywać takiego przekazania w przypadku, gdy Eurojust wyraził zgodę na takie przekazanie, po należytym uwzględnieniu wszystkich istotnych czynników, w tym wagi przestępstwa, celu, w którym operacyjne dane osobowe zostały pierwotnie przesłane, oraz stopnia ochrony danych osobowych w państwie trzecim lub organizacji międzynarodowej, do których operacyjne dane osobowe są dalej przekazywane.

6. Art. 57, 58 i 59 stosuje się w celu zapewnienia, by nie został naruszony stopień ochrony osób fizycznych zapewniony w niniejszym rozporządzeniu i prawie Unii.

Artykuł 57

Przekazywanie na podstawie decyzji stwierdzającej odpowiedni poziom ochrony

Eurojust może przekazywać operacyjne dane osobowe do państwa trzeciego lub organizacji międzynarodowej, jeżeli Komisja zgodnie z art. 36 dyrektywy (UE) 2016/680 stwierdzi w drodze decyzji, że to państwo trzecie, dane terytorium lub co najmniej jeden określony sektor w tym państwie trzecim lub dana organizacja międzynarodowa zapewniają odpowiedni stopień ochrony.

Artykuł 58

Przekazywanie podlegające odpowiednim zabezpieczeniom

1. W razie braku decyzji stwierdzającej odpowiedni poziom ochrony Eurojust może przekazywać operacyjne dane osobowe do państwa trzeciego lub organizacji międzynarodowej, jeżeli:

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

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

2. Eurojust informuje EIOD o kategoriach przekazania na podstawie ust. 1 lit. b).

3. Jeżeli przekazanie odbywa się na podstawie ust. 1 lit. b), musi być ono udokumentowane, a dokumentację udostępnia się EIOD na jego wniosek. Dokumentacja obejmuje zapis daty i godziny przekazania oraz informacje o właściwym organie odbierającym, o uzasadnieniu przekazania oraz o przekazanych operacyjnych danych osobowych

Artykuł 59

Odstępstwa w szczególnych sytuacjach

1. W razie braku decyzji stwierdzającej odpowiedni poziom ochrony lub braku odpowiednich zabezpieczeń zgodnie z art. 58 Eurojust może przekazywać operacyjne dane osobowe do państwa trzeciego lub organizacji międzynarodowej wyłącznie pod warunkiem że przekazanie jest niezbędne:

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

b) w celu zabezpieczenia uzasadnionych interesów osoby, której dane dotyczą;

c) w celu zapobieżenia bezpośredniemu i poważnemu zagrożeniu dla bezpieczeństwa publicznego państwa członkowskiego lub państwa trzeciego; lub

d) w indywidualnych przypadkach w celu wykonania zadań Eurojustu, chyba że Eurojust stwierdzi, że podstawowe prawa i wolności konkretnej osoby, której dane dotyczą, są nadrzędne wobec interesu publicznego przemawiającego za przekazaniem.

2. Jeżeli przekazanie odbywa się na podstawie ust. 1, musi być ono udokumentowane, a dokumentację udostępnia się EIOD na jego wniosek Dokumentacja obejmuje zapis daty i godziny przekazania oraz informacje o właściwym organie odbierającym, o uzasadnieniu przekazania oraz o przekazanych operacyjnych danych osobowych.

ROZDZIAŁ VI

PRZEPISY FINANSOWE

Artykuł 60

Budżet

1. Preliminarz wszystkich dochodów i wydatków Eurojustu jest przygotowywany na każdy rok budżetowy, który odpowiada rokowi kalendarzowemu, i jest wykazywany w budżecie Eurojustu.

2. Budżet Eurojustu musi być zrównoważony pod względem dochodów i wydatków.

3. Z zastrzeżeniem innych zasobów dochody Eurojustu obejmują:

a) wkład Unii zapisany w budżecie ogólnym Unii;

b) wszelkie dobrowolne wkłady finansowe państw członkowskich;

c) opłaty za publikacje i wszelkie usługi świadczone przez Eurojust;

d) dotacje *ad hoc*.

4. Wydatki Eurojustu obejmują wynagrodzenia personelu, wydatki administracyjne, wydatki związane z infrastrukturą oraz koszty operacyjne, w tym środki na wspólne zespoły dochodzeniowo-śledcze.

Artykuł 61

Ustanowienie budżetu

1. Co roku dyrektor administracyjny sporządza projekt preliminarza dochodów i wydatków Eurojustu na kolejny rok budżetowy, zawierający plan zatrudnienia, i przesyła go zarządowi. Europejska Sieć Sądowa i inne unijne sieci prowadzące współpracę wymiarów sprawiedliwości w sprawach karnych, o których mowa w art. 48, otrzymują informacje na temat tych części, które dotyczą ich działalności, w stosownym czasie przed przekazaniem preliminarza Komisji.

2. Na podstawie projektu preliminarza zarząd dokonuje przeglądu wstępnego projektu preliminarza dochodów i wydatków Eurojustu na kolejny rok budżetowy, który to projekt przekazuje się kolegium do przyjęcia.

3. Co roku wstępny projekt preliminarza dochodów i wydatków Eurojustu przesyłany jest Komisji nie później niż do dnia 31 stycznia. Eurojust przesyła Komisji ostateczny projekt preliminarza, który zawiera projekt planu zatrudnienia, do dnia 31 marca tego samego roku.

4. Komisja przesyła preliminarz Parlamentowi Europejskiemu i Radzie („władza budżetowa") wraz z projektem budżetu ogólnego Unii.

5. Na podstawie preliminarza Komisja wprowadza do projektu budżetu ogólnego Unii szacunkowe kwoty, które uważa za niezbędne w odniesieniu do planu zatrudnienia, oraz kwoty wkładu, jaki ma być wniesiony z budżetu ogólnego, i przedstawia je władzy budżetowej zgodnie z art. 313 i 314 TFUE.

6. Władza budżetowa zatwierdza środki przewidziane na wkład Unii dla Eurojustu.

7. Władza budżetowa przyjmuje plan zatrudnienia Eurojustu. Kolegium przyjmuje budżet Eurojustu. Budżet staje się ostateczny po ostatecznym przyjęciu budżetu ogólnego Unii. W razie potrzeby budżet Eurojustu jest odpowiednio dostosowywany przez kolegium.

8. W odniesieniu do wszelkich projektów z zakresu nieruchomości, które mogą mieć znaczący wpływ na budżet Eurojustu, stosuje się art. 88 rozporządzenia delegowanego Komisji (UE) nr 1271/2013 ([1]).

Artykuł 62

Wykonanie budżetu

Dyrektor administracyjny działa w charakterze urzędnika zatwierdzającego Eurojustu i wykonuje budżet Eurojustu na własną odpowiedzialność, w ramach ograniczeń zatwierdzonych w tym budżecie.

Artykuł 63

Prezentacja sprawozdania finansowego i absolutorium

1. Księgowy Eurojustu przesyła księgowemu Komisji i Trybunałowi Obrachunkowemu wstępne sprawozdanie finansowe za rok budżetowy (rok N) do dnia 1 marca kolejnego roku budżetowego (rok N+1).

([1]) Rozporządzenie delegowane Komisji (UE) nr 1271/2013 z dnia 30 września 2013 r. w sprawie ramowego rozporządzenia finansowego dotyczącego organów, o których mowa w art. 208 rozporządzenia Parlamentu Europejskiego i Rady (UE, Euratom) nr 966/2012 (Dz.U. L 328 z 7.12.2013, s. 42).

2. Eurojust przesyła Parlamentowi Europejskiemu, Radzie i Trybunałowi Obrachunkowemu sprawozdanie dotyczące zarządzania budżetem i finansami za rok N do dnia 31 marca roku N+1.

3. Księgowy Komisji przesyła Trybunałowi Obrachunkowemu wstępne sprawozdanie finansowe Eurojustu za rok N, skonsolidowane ze sprawozdaniem finansowym Komisji, do dnia 31 marca roku N+1.

4. Zgodnie z art. 246 ust. 1 rozporządzenia (UE, Euratom) 2018/1046 Trybunał Obrachunkowy przedstawia swoje uwagi na temat wstępnego sprawozdania finansowego Eurojustu do dnia 1 czerwca roku N+1.

5. Po otrzymaniu uwag Trybunału Obrachunkowego na temat wstępnego sprawozdania finansowego Eurojustu zgodnie z przepisami art. 246 rozporządzenia (UE, Euratom) 2018/1046, dyrektor administracyjny sporządza na własną odpowiedzialność końcowe sprawozdanie finansowe i przedkłada je zarządowi w celu zaopiniowania.

6. Zarząd wydaje opinię w sprawie końcowego sprawozdania finansowego Eurojustu.

7. Do dnia 1 lipca roku N+1 dyrektor administracyjny przesyła końcowe sprawozdanie finansowe za rok N Parlamentowi Europejskiemu, Radzie, Komisji oraz Trybunałowi Obrachunkowemu wraz z opinią zarządu.

8. Końcowe sprawozdanie finansowe za rok N publikowane jest w *Dzienniku Urzędowym Unii Europejskiej* do dnia 15 listopada roku N+1.

9. Do dnia 30 września roku N+1 dyrektor administracyjny przesyła Trybunałowi Obrachunkowemu odpowiedź na jego uwagi. Dyrektor administracyjny przesyła tę odpowiedź również zarządowi i Komisji.

10. Dyrektor administracyjny przedkłada Parlamentowi Europejskiemu, na jego wniosek, wszelkie informacje niezbędne do sprawnego zastosowania procedury udzielania absolutorium za dany rok budżetowy zgodnie z art. 261 ust. 3 rozporządzenia (UE, Euratom) 2018/1046.

11. Przed dniem 15 maja roku N + 2 Parlament Europejski, na zalecenie Rady stanowiącej większością kwalifikowaną, udziela dyrektorowi administracyjnemu absolutorium z wykonania budżetu za rok budżetowy N.

12. Absolutorium z wykonania budżetu Eurojustu jest udzielane przez Parlament Europejski na zalecenie Rady zgodnie z procedurą na wzór procedury przewidzianej w art. 319 TFUE oraz w art. 260, 261 i 262 rozporządzenia (UE, Euratom) 2018/1046, a także w oparciu o sprawozdanie z kontroli przeprowadzonej przez Trybunał Obrachunkowy.

Jeżeli Parlament Europejski odmówi udzielenia absolutorium do dnia 15 marca roku N+2, dyrektor administracyjny jest proszony o wyjaśnienie swego stanowiska kolegium, które w świetle zaistniałych okoliczności podejmuje ostateczną decyzję w sprawie stanowiska dyrektora administracyjnego.

Artykuł 64

Przepisy finansowe

1. Zarząd przyjmuje przepisy finansowe mające zastosowanie do Eurojustu zgodnie z rozporządzeniem delegowanym (UE) 1271/2013, po konsultacjach z Komisją. Te przepisy finansowe nie mogą różnić się od przepisów rozporządzenia delegowanego (UE) 1271/2013, chyba że taka różnica jest konkretnie wymagana do celów działań Eurojustu, a Komisja wyraziła na nią uprzednią zgodę.

W odniesieniu do wsparcia finansowego na działania wspólnych zespołów dochodzeniowo-śledczych Eurojust i Europol wspólnie określają zasady i warunki rozpatrywania wniosków o takie wsparcie.

2. Europol może przyznawać dotacje związane z wykonywaniem jego zadań, o których mowa w art. 4 ust. 1. Dotacje przyznawane na zadania określone w art. 4 ust. 1 lit. f) mogą być udzielane państwom członkowskim bez zaproszenia do składania wniosków.

ROZDZIAŁ VII

PRZEPISY DOTYCZĄCE PERSONELU

Artykuł 65

Przepisy ogólne

1. Do personelu Eurojustu zastosowanie mają regulamin pracowniczy urzędników i warunki zatrudnienia innych pracowników oraz przepisy przyjęte w drodze porozumienia między instytucjami Unii w celu wykonania tego regulaminu pracowniczego urzędników i warunków zatrudnienia innych pracowników.

2. Personel Eurojustu składa się z pracowników zatrudnionych zgodnie z zasadami i przepisami mającymi zastosowanie do urzędników i innych pracowników Unii, z uwzględnieniem wszystkich kryteriów, o których mowa w art. 27 regulaminu pracowniczego urzędników, w tym ich reprezentacji geograficznej.

Artykuł 66

Oddelegowani eksperci krajowi i inny personel

1. Eurojust oprócz własnego personelu może korzystać z oddelegowanych ekspertów krajowych lub innego personelu niezatrudnionego przez Eurojust.

2. Kolegium przyjmuje decyzję ustanawiającą zasady delegowania ekspertów krajowych do Eurojustu oraz korzystania z usług innego personelu, w szczególności w celu uniknięcia ewentualnych konfliktów interesów.

3. Eurojust podejmuje odpowiednie działania administracyjne, m.in. w postaci szkoleń i strategii prewencyjnych, aby uniknąć konfliktów interesów, w tym w odniesieniu do konfliktów interesów, które pojawiają się po zakończeniu zatrudnienia.

ROZDZIAŁ VIII

OCENA I SPRAWOZDAWCZOŚĆ

Artykuł 67

Uczestnictwo instytucji Unii oraz parlamentów narodowych

1. Eurojust przekazuje sprawozdanie roczne Parlamentowi Europejskiemu, Radzie i parlamentom narodowym, które mogą przedstawiać swoje uwagi i wnioski.

2. Niezwłocznie po wyborze nowo wybrany przewodniczący Eurojustu składa oświadczenie przed właściwą komisją lub właściwymi komisjami Parlamentu Europejskiego oraz udziela odpowiedzi na pytania członków tych komisji. Dyskusja nie odnosi się bezpośrednio ani pośrednio do konkretnych działań podejmowanych w odniesieniu do określonych spraw operacyjnych.

3. Raz w roku przewodniczący Eurojustu bierze udział we wspólnej ocenie działań Eurojustu przez Parlament Europejski i parlamenty narodowe, w ramach międzyparlamentarnego posiedzenia komisji, aby omówić bieżące działania Eurojustu oraz przedstawić sprawozdanie roczne lub inne kluczowe dokumenty Eurojustu.

Dyskusja nie odnosi się bezpośrednio ani pośrednio do konkretnych działań podejmowanych w odniesieniu do określonych spraw operacyjnych.

4. Oprócz innych obowiązków w zakresie informowania i konsultowania określonych w niniejszym rozporządzeniu Eurojust przekazuje Parlamentowi Europejskiemu oraz parlamentom narodowym w odnośnych językach urzędowych do celów informacyjnych:

a) wyniki badań i projektów strategicznych opracowanych lub zleconych przez Eurojust;

b) dokument programowy, o którym mowa w art. 15;

c) uzgodnienia robocze zawarte z osobami trzecimi.

Artykuł 68

Opinie w sprawie proponowanych aktów ustawodawczych

Komisja i państwa członkowskie wykonując swoje prawa na podstawie art. 76 lit. b) TFUE mogą zwrócić się do Eurojustu o wydanie opinii w sprawie wszystkich wniosków dotyczących aktów ustawodawczych, o których mowa w art. 76 TFUE.

Artykuł 69

Ocena i przegląd

1. Do dnia 13 grudnia 2024 r., a następnie co 5 lat Komisja zleca przeprowadzenie oceny wykonania i wpływu niniejszego rozporządzenia, a także skuteczności i efektywności Eurojustu i jego praktyk roboczych. Kolegium jest wysłuchiwane w procesie oceny. W ocenie tej można uwzględnić w szczególności ewentualne potrzeby dokonania zmian zakresu działania Eurojustu oraz skutki finansowe takich zmian.

2. Komisja przekazuje sprawozdanie z oceny wraz ze swoimi wnioskami Parlamentowi Europejskiemu, parlamentom narodowym, Radzie i kolegium. Ustalenia z oceny podaje się do wiadomości publicznej.

ROZDZIAŁ IX

PRZEPISY OGÓLNE I KOŃCOWE

Artykuł 70

Przywileje i immunitety

Wobec Eurojustu i jego personelu stosuje się Protokół nr 7 w sprawie przywilejów i immunitetów Unii Europejskiej, załączony do TUE i TFUE.

Artykuł 71

System językowy

1. Do Eurojustu stosuje się rozporządzenie Rady nr 1 ([1]).

2. Kolegium podejmuje decyzję w sprawie wewnętrznych zasad Eurojustu dotyczących systemu językowego większością dwóch trzecich głosów członków.

3. Usługi tłumaczenia pisemnego niezbędne do funkcjonowania Eurojustu świadczy Centrum Tłumaczeń dla organów Unii Europejskiej ustanowione rozporządzeniem Rady (WE) nr 2965/94 ([2]), chyba że ze względu na niedostępność usług Centrum Tłumaczeń niezbędne jest znalezienie innego rozwiązania.

Artykuł 72

Poufność

1. Przedstawiciele krajowi oraz ich zastępcy i asystenci, o których mowa w art. 7, personel Eurojustu, korespondenci krajowi, oddelegowani eksperci krajowi, sędziowie łącznikowi, inspektor ochrony danych oraz członkowie i personel EIOD są zobowiązani do zachowania poufności w odniesieniu do wszelkich informacji, które uzyskali w toku wykonywania powierzonych im zadań.

2. Obowiązek zachowania poufności stosuje się do wszystkich osób i wszystkich organów współpracujących z Eurojustem.

([1]) Rozporządzenie Rady nr 1 z dnia 15 kwietnia 1958 r. w sprawie określenia systemu językowego Europejskiej Wspólnoty Gospodarczej (Dz.U. 17 z 6.10.1958, s. 385).

([2]) Rozporządzenie Rady (WE) nr 2965/94 z dnia 28 listopada 1994 r. ustanawiające Centrum Tłumaczeń dla organów Unii Europejskiej (Dz.U. L 314 z 7.12.1994, s. 1).

3. Obowiązek zachowania poufności pozostaje w mocy także po zakończeniu kadencji, ustaniu zatrudnienia lub po zakończeniu czynności przez osoby, o których mowa w ust. 1 i 2.

4. Obowiązek zachowania poufności stosuje się do wszystkich informacji, które Eurojust otrzymał lub których wymiany dokonał, chyba że informacje te zostały już zgodnie z prawem podane do wiadomości publicznej lub są dostępne publicznie.

Artykuł 73

Warunki poufności postępowań krajowych

1. Z zastrzeżeniem art. 21 ust. 3, w przypadku otrzymania lub wymiany informacji za pośrednictwem Eurojustu organ państwa członkowskiego, który dostarczył informacje, może określić warunki, zgodnie ze swoim prawem krajowym, wykorzystania tych informacji w postępowaniu krajowym przez organ otrzymujący informacje.

2. Organ państwa członkowskiego, który otrzymuje informacje, o których mowa w ust. 1, jest związany tymi warunkami.

Artykuł 74

Przejrzystość

1. Do dokumentów będących w posiadaniu Eurojustu stosuje się rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 1049/2001 ([1]).

2. W terminie sześciu miesięcy od pierwszego posiedzenia zarząd opracowuje szczegółowe zasady stosowania rozporządzenia (WE) nr 1049/2001 do przyjęcia ich przez kolegium.

3. Decyzje podjęte przez Eurojust na mocy art. 8 rozporządzenia (WE) nr 1049/2001 mogą stanowić przedmiot skargi do Europejskiego Rzecznika Praw Obywatelskich lub skargi do Trybunału na warunkach określonych odpowiednio w art. 228 oraz 263 TFUE.

4. Eurojust publikuje na swojej stronie internetowej wykaz członków zarządu oraz podsumowania wyników posiedzeń zarządu. Z publikacji tych podsumowań można tymczasowo lub na stałe zrezygnować lub tymczasowo lub na stałe ją ograniczyć, jeżeli takie publikowanie mogłoby niekorzystnie wpłynąć na wykonywanie przez Eurojust jego zadań, biorąc pod uwagę obowiązek zachowania przez Eurojust dyskrecji i poufności oraz operacyjny charakter Eurojustu.

Artykuł 75

OLAF i Trybunał Obrachunkowy

1. Aby ułatwić zwalczanie nadużyć finansowych, korupcji i wszelkich innych nielegalnych działań na mocy rozporządzenia (UE, Euratom) nr 883/2013, w terminie sześciu miesięcy od dnia wejścia w życie niniejszego rozporządzenia Eurojust przystępuje do porozumienia międzyinstytucjonalnego z dnia 25 maja 1999 r. między Parlamentem Europejskim, Radą Unii Europejskiej i Komisją Wspólnot Europejskich dotyczącego dochodzeń wewnętrznych prowadzonych przez Europejski Urząd ds. Zwalczania Nadużyć Finansowych (OLAF) ([2]). Eurojust przyjmuje odpowiednie przepisy, które mają zastosowanie do wszystkich przedstawicieli krajowych, ich zastępców i asystentów, wszystkich oddelegowanych ekspertów krajowych oraz całego personelu Eurojustu, wykorzystując wzór zawarty w załączniku do tego porozumienia.

2. Trybunał Obrachunkowy jest uprawniony do przeprowadzania kontroli, na podstawie dokumentacji i na miejscu, obejmujących wszystkich beneficjentów dotacji, wykonawców i podwykonawców, którzy otrzymują od Eurojustu środki unijne.

([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).

([2]) Dz.U. L 136 z 31.5.1999, s. 15.

3. OLAF może przeprowadzać dochodzenia, w tym kontrole i inspekcje na miejscu, zgodnie z przepisami i procedurami określonymi w rozporządzeniu (UE, Euratom) nr 883/2013 i w rozporządzeniu Rady (Euratom, WE) nr 2185/96 ([1]), aby ustalić, czy miały miejsce jakiekolwiek nieprawidłowości naruszające interesy finansowe Unii w związku z wydatkami finansowanymi przez Eurojust.

4. Z zastrzeżeniem ust. 1, 2 i 3, uzgodnienia robocze Eurojustu z państwami trzecimi lub organizacjami międzynarodowymi, jego umowy, umowy o udzielenie dotacji i decyzje o udzieleniu dotacji zawierają postanowienie wyraźnie uprawniające Trybunał Obrachunkowy i OLAF do przeprowadzania tego rodzaju audytów i dochodzeń, zgodnie z ich odpowiednimi kompetencjami.

5. Pracownicy Eurojustu, dyrektor administracyjny oraz członkowie kolegium i zarządu niezwłocznie powiadamiają OLAF i Prokuraturę Europejską o wszelkich podejrzeniach, które dotyczą nieprawidłowych lub nielegalnych działań w ramach zakresów działania tych organów, a które powzięli w trakcie wykonywania swoich obowiązków, przy czym powiadomienie takie nie może skutkować pociągnięciem ich do odpowiedzialności.

Artykuł 76

Przepisy dotyczące ochrony informacji wrażliwych niebędących informacjami niejawnymi oraz informacji niejawnych

1. Eurojust ustanawia przepisy wewnętrzne dotyczące postępowania z informacjami i ich poufności oraz ochrony informacji wrażliwych niebędących informacjami niejawnymi, w tym przepisy dotyczące tworzenia i przetwarzania takich informacji w Eurojuście.

2. Eurojust ustanawia przepisy wewnętrzne dotyczące ochrony informacji niejawnych UE, które to przepisy są zgodne z decyzją Rady 2013/488/UE ([2]), aby zapewnić równoważny poziom ochrony takich informacji.

Artykuł 77

Dochodzenia administracyjne

Działania administracyjne Eurojustu podlegają dochodzeniom administracyjnym prowadzonym przez Rzecznika Praw Obywatelskich zgodnie z art. 228 TFUE.

Artykuł 78

Odpowiedzialność inna niż odpowiedzialność za nieuprawnione lub niewłaściwe przetwarzanie danych

1. Odpowiedzialność umowną Eurojustu regulują przepisy mające zastosowanie do danej umowy.

2. Do orzekania w sprawie wszelkich klauzul arbitrażowych zamieszczonych w umowie zawartej przez Eurojust właściwy jest Trybunał.

3. W przypadku odpowiedzialności pozaumownej Eurojust, zgodnie z ogólnymi zasadami wspólnymi dla porządków prawnych państw członkowskich i niezależnie od jakiejkolwiek odpowiedzialności wynikającej z art. 46, naprawia wszelkie szkody spowodowane przez Eurojust lub jego pracowników w trakcie wykonywania przez nich obowiązków.

4. Ust. 3 stosuje się również do szkody powstałej na skutek błędu popełnionego przez przedstawiciela krajowego, jego zastępcę lub asystenta w trakcie wykonywania ich obowiązków. Jeżeli jednak działają oni na podstawie uprawnień przyznanych im zgodnie z art. 8, ich państwo członkowskie pokrywa koszty poniesione przez Eurojust w celu naprawienia szkody.

5. Do orzekania w sporach dotyczących odszkodowania za szkody, o których mowa w ust. 3, właściwy jest Trybunał.

([1]) Rozporządzenie Rady (Euratom, WE) nr 2185/96 z dnia 11 listopada 1996 r. w sprawie kontroli na miejscu oraz inspekcji przeprowadzanych przez Komisję w celu ochrony interesów finansowych Wspólnot Europejskich przed nadużyciami finansowymi i innymi nieprawidłowościami (Dz.U. L 292 z 15.11.1996, s. 2).

([2]) Decyzja Rady 2013/488/UE z dnia 23 września 2013 r. w sprawie przepisów bezpieczeństwa dotyczących ochrony informacji niejawnych UE (Dz.U. L 274 z 15.10.2013, s. 1).

6. Sądy krajowe państw członkowskich właściwe do rozstrzygania sporów dotyczących odpowiedzialności Eurojustu, o której mowa w niniejszym artykule, określa się na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1215/2012 ([1]).

7. Odpowiedzialność osobistą pracowników Eurojustu wobec Eurojustu regulują przepisy regulaminu pracowniczego urzędników lub warunków zatrudnienia innych pracowników.

Artykuł 79

Umowa w sprawie siedziby i warunki prowadzenia działalności

1. Siedziba Eurojustu mieści się w Hadze, w Niderlandach.

2. Niezbędne ustalenia dotyczące obiektów, jakie należy zapewnić Eurojustowi w Niderlandach, i dotyczące infrastruktury udostępnianej przez Niderlandy, a także przepisy szczególne mające zastosowanie w Niderlandach do dyrektora administracyjnego, członków kolegium, personelu Eurojustu i do członków ich rodzin określone są w porozumieniu w sprawie siedziby zawieranym między Eurojustem a Niderlandami po uzyskaniu zgody kolegium.

Artykuł 80

Przepisy przejściowe

1. Eurojust ustanowiony na mocy niniejszego rozporządzenia jest ogólnym następcą prawnym w odniesieniu do wszystkich zawartych umów, zaciągniętych zobowiązań i mienia nabytego przez Eurojust ustanowiony na mocy decyzji 2002/187/WSiSW.

2. Przedstawiciele krajowi Eurojustu ustanowionego na mocy decyzji 2002/187/WSiSW, którzy zostali oddelegowani przez państwa członkowskie na mocy tej decyzji, działają jako przedstawiciele krajowi Eurojustu zgodnie z rozdziałem II sekcja II niniejszego rozporządzenia. Ich kadencja może zostać jednokrotnie przedłużona na mocy art. 7 ust. 5 niniejszego rozporządzenia po jego wejściu w życie, niezależnie od wcześniejszego przedłużenia tej kadencji.

3. W chwili wejścia w życie niniejszego rozporządzenia przewodniczący i wiceprzewodniczący Eurojustu ustanowionego na mocy decyzji 2002/187/WSiSW działają jako przewodniczący i wiceprzewodniczący Eurojustu zgodnie z art. 11 niniejszego rozporządzenia do czasu wygaśnięcia ich kadencji zgodnie z tą decyzją. Mogą oni zostać jednokrotnie ponownie wybrani na te stanowiska na mocy art. 11 ust. 4 niniejszego rozporządzenia po jego wejściu w życie, niezależnie od wcześniejszego ponownego wybrania.

4. Dyrektor administracyjny, który został jako ostatni mianowany na mocy art. 29 decyzji 2002/187/WSiSW, działa jako dyrektor administracyjny zgodnie z art. 17 niniejszego rozporządzenia do czasu wygaśnięcia jego kadencji zgodnie z tą decyzją. Kadencja dyrektora administracyjnego może zostać jednokrotnie przedłużona po wejściu w życie niniejszego rozporządzenia.

5. Niniejsze rozporządzenie nie narusza umów zawartych przez Eurojust ustanowiony na mocy decyzji Rady 2002/187/WSiSW. W szczególności wszelkie umowy międzynarodowe zawarte przez Eurojust przed dniem 12 grudnia 2019 r. pozostają w mocy.

6. Procedura udzielania absolutorium w odniesieniu do budżetów zatwierdzonych na podstawie art. 35 decyzji 2002/187/WSiSW jest przeprowadzana zgodnie z przepisami ustanowionymi w art. 36 tej decyzji.

7. Rozporządzenie nie ma wpływu na umowy o pracę, które zawarto na mocy decyzji 2002/187/WSiSW przed wejściem w życie niniejszego rozporządzenia. Inspektor ochrony danych, który został jako ostatni mianowany na mocy art. 17 tej decyzji, działa jako inspektor ochrony danych zgodnie z art. 36 niniejszego rozporządzenia.

Artykuł 81

Zastąpienie i uchylenie

1. Decyzję 2002/187/WSiSW zastępuje się w odniesieniu do państw członkowskich związanych niniejszym rozporządzeniem ze skutkiem od dnia 12 grudnia 2019 r.

W związku z tym decyzja 2002/187/WSiSW traci moc ze skutkiem od dnia 12 grudnia 2019 r.

2. W odniesieniu do państw członkowskich związanych niniejszym rozporządzeniem odesłania do decyzji, o której mowa w ust. 1, traktuje się jako odesłania do niniejszego rozporządzenia.

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

Artykuł 82

Wejście w życie i stosowanie

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

2. Niniejsze rozporządzenie stosuje się od dnia 12 grudnia 2019 r.

Niniejsze rozporządzenie wiąże w całości i jest bezpośrednio stosowane w państwach członkowskich zgodnie z Traktatami.

Sporządzono w Strasburgu dnia 14 listopada 2018 r.

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

ZAŁĄCZNIK I

Wykaz form poważnej przestępczości, w odniesieniu do których Eurojust jest właściwy do podejmowania działań zgodnie z art. 3 ust. 1:

— terroryzm,

— przestępczość zorganizowana,

— handel narkotykami,

— działalność związana z praniem pieniędzy,

— przestępstwa związane z substancjami jądrowymi i promieniotwórczymi,

— przemyt imigrantów,

— handel ludźmi,

— przestępstwa związane z pojazdami silnikowymi,

— zabójstwo i spowodowanie ciężkiego uszczerbku na zdrowiu,

— nielegalny obrót organami i tkankami ludzkimi,

— uprowadzenie, bezprawne pozbawienie wolności i wzięcie zakładników,

— rasizm i ksenofobia,

— rozbój i kradzież rozbójnicza,

— nielegalny handel dobrami kultury, w tym antykami i dziełami sztuki,

— oszustwa i nadużycia finansowe,

— przestępstwa przeciwko interesom finansowym Unii,

— wykorzystywanie informacji wewnętrznych i manipulacja na rynku finansowym,

— wymuszenie rozbójnicze,

— podrabianie i piractwo produktów,

— fałszowanie dokumentów urzędowych i obrót takimi dokumentami,

— fałszowanie pieniądza i środków płatniczych,

— przestępczość komputerowa,

— korupcja,

— nielegalny handel bronią, amunicją i materiałami wybuchowymi,

— nielegalny obrót zagrożonymi gatunkami zwierząt,

— nielegalny obrót zagrożonymi gatunkami i odmianami roślin,

— przestępstwa przeciw środowisku, w tym zanieczyszczenia pochodzące ze statków,

— nielegalny obrót hormonami i innymi stymulatorami wzrostu,

— niegodziwe traktowanie w celach seksualnych oraz wykorzystywanie seksualne, w tym materiały przedstawiające niegodziwe traktowanie dzieci oraz nagabywanie dzieci w celach seksualnych,

— ludobójstwo, zbrodnie przeciw ludzkości oraz zbrodnie wojenne.

ZAŁĄCZNIK II

KATEGORIE DANYCH OSOBOWYCH, O KTÓRYCH MOWA W ART. 27

1. a) Nazwisko, nazwisko rodowe, imiona oraz wszelkie pseudonimy lub nazwiska przybrane;

   b) data i miejsce urodzenia;

   c) obywatelstwo;

   d) płeć;

   e) miejsce zamieszkania, zawód i miejsce pobytu danej osoby;

   f) numer ubezpieczenia społecznego lub inne oficjalne numery wykorzystywane w państwach członkowskich do identyfikacji osób, prawa jazdy, dane z dokumentów tożsamości i dane paszportowe oraz numery identyfikacji celnej i podatkowej;

   g) informacje dotyczące osób prawnych, o ile zawierają dane dotyczące zidentyfikowanych lub identyfikowalnych osób, które są objęte postępowaniem przygotowawczym lub wniesieniem i popieraniem oskarżenia;

   h) dane rachunków bankowych lub rachunków w innych instytucjach finansowych;

   i) opis i charakter zarzucanych przestępstw, daty, w których zostały popełnione, kategoria karna przestępstwa oraz przebieg postępowania przygotowawczego;

   j) fakty wskazujące na międzynarodowy wymiar sprawy;

   k) szczegóły dotyczące zarzucanej przynależności do organizacji przestępczej;

   l) numery telefonów, adresy poczty elektronicznej, dane o połączeniach i lokalizacji oraz wszelkie odnośne dane potrzebne do zidentyfikowania abonenta lub użytkownika;

   m) dane rejestracyjne pojazdów;

   n) profile DNA ustalone na podstawie niekodującej części DNA, zdjęcia oraz odciski palców.

2. a) Nazwisko, nazwisko rodowe, imiona oraz wszelkie pseudonimy lub nazwiska przybrane;

   b) data i miejsce urodzenia;

   c) obywatelstwo;

   d) płeć;

   e) miejsce zamieszkania, zawód i miejsce pobytu danej osoby;

   f) opis i charakter przestępstw, z którymi dana osoba miała związek, daty, w których przestępstwa zostały popełnione, kategoria karna przestępstw oraz przebieg postępowania przygotowawczego;

   g) numer ubezpieczenia społecznego lub inne oficjalne numery wykorzystywane w państwach członkowskich do identyfikacji osób, prawa jazdy, dane z dokumentów tożsamości i dane paszportowe oraz numery identyfikacji celnej i podatkowej;

   h) dane rachunków bankowych lub rachunków w innych instytucjach finansowych;

   i) numery telefonów, adresy poczty elektronicznej, dane o połączeniach i lokalizacji oraz wszelkie dane potrzebne do zidentyfikowania abonenta lub użytkownika;

   j) dane rejestracyjne pojazdów.

ISSN 1977-0766 (wydanie elektroniczne)
ISSN 1725-5139 (wydanie papierowe)

Urząd Publikacji Unii Europejskiej
2985 Luksemburg
LUKSEMBURG

PL