DECYZJA RADY (UE) 2021/1093

z dnia 28 czerwca 2021 r.

w sprawie ustanowienia przepisów wykonawczych dotyczących inspektora ochrony danych w Radzie, stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725 i ograniczeń praw osób, których dane dotyczą, w związku z wykonywaniem zadań inspektora ochrony danych w Radzie oraz uchylenia decyzji Rady 2004/644/WE

RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 240 ust. 3,

uwzględniając 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 ([1]), w szczególności jego art. 45 ust. 3,

a także mając na uwadze, co następuje:

(1) Rozporządzenie (UE) 2018/1725 ustala zasady i przepisy mające zastosowanie do wszystkich instytucji i organów Unii oraz stanowi o powołaniu inspektora ochrony danych przez każdą instytucję lub organ Unii.

(2) Art. 45 ust. 3 rozporządzenia (UE) 2018/1725 wymaga przyjęcia przepisów wykonawczych dotyczących inspektora ochrony danych przez każdą instytucję lub organ Unii (zwanych dalej „przepisami wykonawczymi"). Przepisy wykonawcze powinny w szczególności dotyczyć zadań, obowiązków i uprawnień inspektora ochrony danych w Radzie i Sekretariacie Generalnym Rady.

(3) Przepisy wykonawcze powinny ustanawiać procedury dotyczące wykonywania praw przez podmioty, których dane dotyczą, oraz wypełniania obowiązków przez wszystkie zainteresowane podmioty w Radzie i Sekretariacie Generalnym Rady (SGR) w zakresie przetwarzania danych osobowych.

(4) Rozporządzenie (UE) 2018/1725 jasno określa obowiązki administratorów, w szczególności w odniesieniu do praw osób, których dane dotyczą. Przepisy wykonawcze powinny zapewniać, by Rada i SGR wypełniały swoje obowiązki jako administrator w sposób jednolity i przejrzysty. Należy ustanowić przepisy pozwalające ustalić, kto jest odpowiedzialny za operację przetwarzania przeprowadzaną w imieniu Rady lub SGR. W związku z tym należy wprowadzić pojęcie „administratora delegowanego", aby dokładnie wskazać obowiązki podmiotów SGR, w szczególności w odniesieniu do indywidualnych decyzji dotyczących praw osób, których dane dotyczą. Należy ponadto wprowadzić pojęcie „administratora odpowiedzialnego za operacje przetwarzania", który – na odpowiedzialność administratora delegowanego – został wyznaczony do zapewnienia zgodności z przepisami w praktyce oraz do rozpatrywania wniosków osób, których dane dotyczą, w odniesieniu do operacji przetwarzania. Aby dokładnie określić obowiązki w SGR w odniesieniu do każdej czynności przetwarzania, w zapisie dokonanym w rejestrze należy jednoznacznie wskazać administratora odpowiedzialnego za operacje przetwarzania. Powołanie administratora odpowiedzialnego za operacje przetwarzania nie uniemożliwia korzystania w praktyce z punktu kontaktowego, na przykład w postaci funkcyjnej skrzynki pocztowej, która zostanie udostępniona osobom, których dane dotyczą.

(5) W niektórych przypadkach kilka dyrekcji generalnych lub służb SGR przeprowadza wspólnie operację przetwarzania w celu realizowania swojej misji. W takich przypadkach powinny one zapewnić istnienie porozumień wewnętrznych w celu przejrzystego określenia swoich odpowiednich obowiązków wynikających z rozporządzenia (UE) 2018/1725, w szczególności w odniesieniu do praw osób, których dane dotyczą, powiadamiania Europejskiego Inspektora Ochrony Danych (EIOD) oraz dokonywania zapisów.

([1]) Dz.U. L 295 z 21.11.2018, s. 39.

(6) Aby ułatwić wykonywanie obowiązków administratorów delegowanych, każda dyrekcja generalna lub inna służba SGR powinna powołać koordynatora ds. ochrony danych. Koordynatorzy ds. ochrony danych powinni wspierać dyrekcję generalną lub inną służbę SGR we wszystkich aspektach ochrony danych osobowych i uczestniczyć w sieci koordynatorów ds. ochrony danych w SGR, aby zapewnić spójne wdrożenie i interpretację rozporządzenia (UE) 2018/1725.

(7) Na podstawie art. 45 ust. 1 lit. b) rozporządzenia (UE) 2018/1725 inspektor ochrony danych może wydawać dodatkowe wytyczne dotyczące funkcji koordynatora ds. ochrony danych.

(8) Art. 25 ust. 1 rozporządzenia (UE) 2018/1725 daje każdej instytucji lub organowi Unii możliwość ograniczenia zastosowania art. 14–17, 19, 20 i 35 tego rozporządzenia, a także zasady przejrzystości określonej w art. 4 ust. 1 lit. a) tego rozporządzenia, w zakresie w jakim przepisy tego artykułu odpowiadają prawom i obowiązkom przewidzianym w art. 14–17, 19 i 20 tego rozporządzenia.

(9) W niektórych przypadkach inspektor ochrony danych może być zmuszony do ograniczenia praw osób, których dane dotyczą, by wykonywać zadania w zakresie monitorowania, prowadzenia postępowań wyjaśniających, audytów lub konsultacji określone w art. 45 rozporządzenia (UE) 2018/1725, przy jednoczesnym poszanowaniu standardów ochrony danych osobowych określonych w tym rozporządzeniu. Konieczne jest przyjęcie przepisów wewnętrznych, na mocy których inspektor ochrony danych może ograniczać prawa osób, których dane dotyczą, zgodnie z art. 25 tego rozporządzenia (zwanych dalej „przepisami wewnętrznymi").

(10) Przepisy wewnętrzne należy stosować do wszystkich operacji przetwarzania danych przeprowadzanych przez Radę i SGR w ramach wykonywania przez inspektora ochrony danych zadań w zakresie monitorowania, prowadzenia postępowań wyjaśniających, audytów lub konsultacji. Przepisy wewnętrzne powinny być również stosowane do operacji przetwarzania, które stanowią część zadań związanych ze sprawowaną przez inspektora ochrony danych funkcją w zakresie prowadzenia postępowań wyjaśniających lub audytów, takich jak postępowania skargowe prowadzone przez inspektora ochrony danych. Przepisy wewnętrzne powinny być również stosowane do monitorowania przez inspektora ochrony danych i konsultacji z inspektorem ochrony danych, w przypadku gdy inspektor ten zapewnia wsparcie i współpracę dyrekcjom generalnym i służbom SGR poza prowadzonymi przez niego administracyjnymi postepowaniami wyjaśniającymi i audytami.

(11) Rada i SGR mogą być zmuszone do stosowania ograniczeń w oparciu o podstawy, o których mowa w art. 25 ust. 1 lit. c), g) i h) rozporządzenia (UE) 2018/1725, do operacji przetwarzania danych przeprowadzanych w ramach wykonywanych przez inspektora ochrony danych zadań w zakresie monitorowania, prowadzenia postępowań wyjaśniających, audytów lub konsultacji, gdy jest to konieczne do ochrony zadań inspektora ochrony danych, powiązanych postępowań wyjaśniających i postępowań, narzędzi i metod prowadzenia przez inspektora ochrony danych postępowań wyjaśniających i audytów, a także praw innych osób związanych z zadaniami inspektora ochrony danych.

(12) W celu utrzymania skutecznej współpracy Rada i SGR mogą też być zmuszone do stosowania ograniczeń praw osób, których dane dotyczą, w celu ochrony informacji zawierających dane osobowe pochodzących od innych dyrekcji generalnych i służb SGR lub innych instytucji lub organów Unii. W związku z tym inspektor ochrony danych powinien konsultować się z tymi dyrekcjami generalnymi i służbami lub z innymi instytucjami lub organami w kwestii stosownych podstaw oraz konieczności i proporcjonalności takich ograniczeń.

(13) Inspektor ochrony danych – a w stosownych przypadkach dyrekcje generalne i służby SGR – powinny w sposób przejrzysty podchodzić do wszystkich ograniczeń oraz rejestrować każde zastosowanie ograniczeń w odpowiednim systemie zapisów.

(14) Zgodnie z art. 25 ust. 8 rozporządzenia (UE) 2018/1725 administratorzy mogą wstrzymać przekazanie osobie, której dane dotyczą, informacji o powodach zastosowania ograniczenia lub odmówić przekazania takich informacji, jeżeli mogłoby to w jakikolwiek sposób zagrozić celowi ograniczenia. W szczególności gdy stosuje się ograniczenie praw określonych w art. 16 i 35 tego rozporządzenia, zgłoszenie takiego ograniczenia zagrażałoby celowi ograniczenia. W celu zapewnienia, aby prawo osoby, której dane dotyczą, do uzyskania informacji zgodnie z tymi artykułami było ograniczone tylko dopóty, dopóki istnieją powody takiego wstrzymania, inspektor ochrony danych lub stosujące takie ograniczenie dyrekcje generalne lub służby SGR powinny regularnie dokonywać przeglądu swojego stanowiska.

(15) W przypadku ograniczenia innych praw osób, których dane dotyczą, inspektor ochrony danych powinien ocenić w poszczególnych przypadkach, czy powiadomienie o ograniczeniu zagrażałoby jego celowi.

(16) Inspektor ochrony danych powinien przeprowadzić niezależny przegląd stosowania ograniczeń na podstawie niniejszej decyzji przez inne dyrekcje generalne lub służby SGR w celu zapewnienia zgodności z niniejszą decyzją.

(17) Wszelkie ograniczenia stosowane na podstawie niniejszej decyzji powinny być konieczne i proporcjonalne w społeczeństwie demokratycznym.

(18) Zgodnie z art. 41 ust. 1 i 2 rozporządzenia (UE) 2018/1725 poinformowano EIOD i skonsultowano się z nim; opinia została wydana ([2]).

(19) Przepisy wykonawcze dotyczące rozporządzenia (UE) 2018/1725 stosuje się bez uszczerbku dla rozporządzenia (WE) nr 1049/2001 Parlamentu Europejskiego i Rady ([3]), decyzji Rady2004/338/WE, Euratom ([4]), w szczególności jej załącznika II, decyzji Rady 2013/488/UE ([5]), w szczególności części II sekcji VI jej załącznika, jak również decyzji Sekretarza Generalnego Rady/Wysokiego Przedstawiciela ds. Wspólnej Polityki Zagranicznej i Bezpieczeństwa z dnia 25 czerwca 2001 r. ([6])

(20) Decyzja Rady 2004/644/WE ([7]) ustanawia przepisy wykonawcze dotyczące rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 45/2001. Rozporządzeniem (UE) 2018/1725 uchylono rozporządzenie (WE) nr 45/2001 ze skutkiem od dnia 11 grudnia 2019 r. W celu zapewnienia, aby zastosowanie miał tylko jeden zestaw przepisów wykonawczych, należy uchylić decyzję 2004/644/WE,

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

SEKCJA 1

POSTANOWIENIA OGÓLNE

Artykuł 1

Przedmiot i zakres stosowania

1. Niniejsza decyzja ustanawia przepisy i procedury dotyczące stosowania rozporządzenia (UE) 2018/1725 przez Radę i Sekretariat Generalny Rady (SGR) oraz ustanawia dalsze przepisy wykonawcze dotyczące inspektora ochrony danych w Radzie.

2. Niniejsza decyzja ustanawia przepisy, jakie ma stosować Rada i SGR w odniesieniu do wykonywanych przez inspektora ochrony danych zadań w zakresie monitorowania, prowadzenia postępowań wyjaśniających, audytów lub konsultacji, kiedy informują one osoby, których dane dotyczą, o przetwarzaniu ich danych osobowych zgodnie z art. 14, 15 i 16 rozporządzenia (UE) 2018/1725.

3. Niniejsza decyzja określa warunki, na jakich Rada i SGR, w odniesieniu do prowadzonych przez inspektora ochrony danych działań w zakresie monitorowania, prowadzenia postępowań wyjaśniających, audytów lub konsultacji, mogą ograniczyć stosowanie art. 4, 14–17, 19, 20 i 35 rozporządzenia (UE) 2018/1725, zgodnie z art. 25 ust. 1 lit. c), g) i h) tego rozporządzenia.

4. Niniejszą decyzję stosuje się do przetwarzania danych osobowych przez Radę i SGR w celu wykonywania przez inspektora ochrony danych zdań, o których mowa w art. 45 rozporządzenia (UE) 2018/1725, lub w związku z wykonywaniem tych zadań.

([2]) Opinia z dnia 6 kwietnia 2021 r. (dotychczas nieopublikowana w Dzienniku Urzędowym).

([3]) 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).

([4]) Decyzja Rady 2004/338/WE, Euratom z dnia 22 marca 2004 r. dotycząca przyjęcia regulaminu wewnętrznego Rady (Dz.U. L 106 z 15.4.2004, s. 22).

([5]) 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]) Decyzja Sekretarza Generalnego Rady/Wysokiego Przedstawiciela ds. Wspólnej Polityki Zagranicznej i Bezpieczeństwa z dnia 25 czerwca 2001 r. w sprawie kodeksu dobrego postępowania administracyjnego dla Sekretariatu Generalnego Rady Unii Europejskiej oraz jego personelu w kontaktach zawodowych ze społeczeństwem (Dz.U. C 189 z 5.7.2001, s. 1).

([7]) Decyzja Rady 2004/644/WE z dnia 13 września 2004 r. ustanawiająca reguły wykonawcze dotyczące rozporządzenia (WE) nr 45/2001 Parlamentu Europejskiego i Rady o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych (Dz.U. L 296 z 21.9.2004, s. 16.).

Artykuł 2

Administrowanie

Do celów niniejszej decyzji Radę i SGR uznaje się za administratora w rozumieniu art. 3 pkt 8 rozporządzenia (UE) 2018/1725.

Artykuł 3

Definicje

Na potrzeby niniejszej decyzji stosuje się następujące definicje:

1) „inspektor ochrony danych" oznacza osobę wyznaczoną przez Sekretarza Generalnego Rady na podstawie art. 43 rozporządzenia (UE) 2018/1725;

2) „zadania inspektora ochrony danych" oznaczają zadania, o których mowa w art. 45 rozporządzenia (UE) 2018/1725;

3) „personel SGR" oznacza wszystkich urzędników SGR i inne osoby objęte regulaminem pracowniczym urzędników Unii Europejskiej i warunkami zatrudnienia innych pracowników Unii, określonymi w rozporządzeniu Rady (EWG, Euratom, EWWiS) nr 259/68 ([8]) (zwanymi dalej „regulaminem pracowniczym") lub pracujące na rzecz SGR na podstawie umowy (mianowicie stażyści, konsultanci, wykonawcy, urzędnicy oddelegowani przez państwa członkowskie);

4) „administrator delegowany" oznacza osobę stojącą na czele dyrekcji generalnej lub służby SGR, która to dyrekcja generalna lub służba, samodzielnie lub wspólnie z innymi, określa cele i sposoby przetwarzania danych osobowych w imieniu Rady lub SGR w ramach realizowanej przez siebie misji;

5) „administrator odpowiedzialny za operacje przetwarzania" oznacza członka personelu SGR na średnim lub wyższym szczeblu kierowniczym, który został wyznaczony przez administratora delegowanego do wspierania go w zapewnianiu zgodności z rozporządzeniem (UE) 2018/1725 w odniesieniu do operacji przetwarzania, za które jest odpowiedzialny, oraz do pełnienia funkcji głównego punktu kontaktowego dla osób, których dane dotyczą;

6) „koordynator ds. ochrony danych" oznacza członka personelu SGR wyznaczonego w każdej dyrekcji generalnej lub w innych służbach SGR w porozumieniu z inspektorem ochrony danych, aby wspierać daną dyrekcję generalną lub służbę we wszystkich aspektach ochrony danych osobowych oraz zajmować się jako jej przedstawiciel kwestiami ochrony danych w ścisłej współpracy z inspektorem ochrony danych.

SEKCJA 2

INSPEKTOR OCHRONY DANYCH

Artykuł 4

Wyznaczenie i status inspektora ochrony danych

1. Sekretarz Generalny Rady wyznacza spośród personelu SGR inspektora ochrony danych i rejestruje go u Europejskiego Inspektora Ochrony Danych (EIOD) zgodnie z art. 43 rozporządzenia (UE) 2018/1725.

2. Inspektor ochrony danych jest wybierany 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 rozporządzenia (UE) 2018/1725. Inspektor ochrony danych ma również solidną wiedzę na temat SGR, jego struktur oraz przepisów i procedur administracyjnych. Aby wykonywać swoje zadania inspektor ochrony danych jest zwolniony z wszelkich innych zadań w SGR.

3. Inspektor ochrony danych jest wyznaczany na okres pięciu lat i może zostać wyznaczony ponownie.

4. Inspektor ochrony danych i jego pracownicy podlegają bezpośrednio Sekretarzowi Generalnemu Rady i to bezpośrednio jemu składają sprawozdania.

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

5. Wykonując swoje zadania, inspektor ochrony danych działa w sposób niezależny i nie otrzymuje żadnych instrukcji od Sekretarza Generalnego Rady, administratorów delegowanych, administratorów odpowiedzialnych za operacje przetwarzania ani od żadnej innej osoby dotyczących wewnętrznego stosowania przepisów rozporządzenia (UE) 2018/1725 lub jego współpracy z EIOD.

6. Rada i SGR wspierają inspektora ochrony danych w wykonywaniu przez niego zadań, o których mowa w art. 45 rozporządzenia (UE) 2018/1725, zapewniając mu zasoby niezbędne do wykonywania tych zadań, udzielenia dostępu do danych osobowych i operacji przetwarzania, a także do utrzymania jego wiedzy fachowej.

7. Inspektor ochrony danych nie może zostać odwoływany ani ukarany za wykonywanie swoich zadań. Inspektor ochrony danych może zostać odwołany jedynie zgodnie z art. 44 ust. 8 rozporządzenia (UE) 2018/1725. Aby uzyskać zgodę EIOD na takie odwołanie zgodnie z przywołanym artykułem zasięga się opinii EIOD na piśmie. Kopię tej zgody przesyła się inspektorowi ochrony danych.

8. SGR, w szczególności administratorzy delegowani i administratorzy odpowiedzialni za operacje przetwarzania, zapewniają, by inspektor ochrony danych był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych.

Artykuł 5

Zadania i obowiązki

1. Inspektor ochrony danych wykonuje wszystkie zadania określone w art. 45 rozporządzenia (UE) 2018/1725. Inspektor ochrony danych w szczególności:

a) zapewnia stosowanie i wdrażanie przez Radę i SGR rozporządzenia (UE) 2018/1725 oraz monitoruje zgodność z tym rozporządzeniem i mającymi zastosowanie ramami prawnymi dotyczącymi ochrony danych osobowych;

b) doradza Sekretarzowi Generalnemu Rady, administratorom delegowanym i administratorom odpowiedzialnym za operacje przetwarzania w kwestiach dotyczących stosowania przepisów o ochronie danych;

c) doradza administratorom delegowanym i administratorom odpowiedzialnym za operacje przetwarzania oraz wspiera ich w przeprowadzaniu oceny skutków dla ochrony danych zgodnie z art. 39 i 40 rozporządzenia (UE) 2018/1725;

d) zapewnia, by operacje przetwarzania nie wpływały negatywnie na prawa i wolności osób, których dane dotyczą;

e) upowszechnia wiedzę na temat mających zastosowanie ram prawnych dotyczących ochrony danych osobowych i przyczynia się do stworzenia kultury ochrony danych osobowych w SGR.

Sekretarz Generalny Rady, zainteresowani administratorzy, Komitet Pracowniczy i dowolne inne osoby mogą konsultować się z inspektorem ochrony danych, bez korzystania z oficjalnych kanałów, w każdej sprawie dotyczącej stosowania lub wdrażania rozporządzenia (UE) 2018/1725.

2. Inspektor ochrony danych prowadzi rejestr zapisów czynności przetwarzania i udostępnia go publicznie, zgodnie z art. 12.

3. Inspektor ochrony danych prowadzi wewnętrzny rejestr naruszeń ochrony danych osobowych w rozumieniu art. 3 pkt 16 rozporządzenia (UE) 2018/1725.

4. Inspektor ochrony danych doradza administratorowi delegowanemu, na wniosek, w sprawie stosowania ograniczenia stosowania art. 14–22, 35 i 36, a także art. 4 rozporządzenia (UE) 2018/1725.

5. Inspektor ochrony danych organizuje regularne posiedzenia koordynatorów ds. ochrony danych i przewodniczy tym posiedzeniom.

6. Inspektor ochrony danych składa roczne sprawozdanie ze swojej działalności Sekretarzowi Generalnemu Rady i udostępnia je personelowi SGR.

7. Inspektor ochrony danych współpracuje z inspektorami ochrony danych wyznaczonymi przez inne instytucje i organy Unii oraz regularnie uczestniczy w posiedzeniach zwoływanych przez EIOD lub inspektorów ochrony danych innych instytucji i organów Unii z myślą o ułatwieniu dobrej współpracy, w szczególności poprzez wymianę doświadczeń i najlepszych praktyk.

8. Inspektor ochrony danych jest uważany za administratora delegowanego w odniesieniu do operacji przetwarzania przeprowadzanych w ramach wykonywania jego zadań.

Artykuł 6

Uprawnienia

Podczas wykonywania swoich zadań i obowiązków inspektor ochrony danych:

a) ma w każdej chwili dostęp do danych będących przedmiotem operacji przetwarzania i do wszystkich biur, urządzeń przetwarzających dane i nośników danych;

b) może wnioskować o opinię prawną Służby Prawnej Rady;

c) może zwrócić się o inne wsparcie do odpowiednich dyrekcji generalnych i służb SGR;

d) może przydzielać akta do odpowiednich dyrekcji generalnych i służb SGR w celu podjęcia odpowiednich działań następczych;

e) może przeprowadzać – na wniosek lub z własnej inicjatywy – postępowania wyjaśniające dotyczące spraw i zdarzeń bezpośrednio związanych z zadaniami inspektora ochrony danych, zgodnie z procedurą określoną w art. 14;

f) może zaproponować środki administracyjne Sekretarzowi Generalnemu Rady i wydać ogólne zalecenia dotyczące właściwego stosowania rozporządzenia (UE) 2018/1725;

g) może formułować zalecenia dla SGR, administratorów delegowanych i administratorów odpowiedzialnych za operacje przetwarzania dotyczące praktycznego usprawnienia stosowania rozporządzenia (UE) 2018/1725, a także:

   (i) wezwać administratora delegowanego lub podmiot przetwarzający do uczynienia zadość wnioskowi osoby, której dane dotyczą, dotyczącego wykonywania praw przysługujących jej na mocy rozporządzenia (UE) 2018/1725;

   (ii) wydawać ostrzeżenia skierowane do administratora delegowanego lub podmiotu przetwarzającego, jeżeli operacja przetwarzania narusza przepisy rozporządzenia (UE) 2018/1725, oraz w stosownych przypadkach wezwać administratora delegowanego lub podmiot przetwarzający do zapewnienia zgodności operacji przetwarzania z przepisami w określony sposób i w określonym terminie;

   (iii) wezwać administratora delegowanego lub podmiot przetwarzający do zawieszenia przepływu danych do odbiorcy w państwie członkowskim, do państwa trzeciego lub do organizacji międzynarodowej;

   (iv) zwrócić się do administratora delegowanego lub do podmiotu przetwarzającego o złożenie do inspektora ochrony danych w określonym terminie sprawozdania na temat działań następczych podjętych w związku z zaleceniem lub radą tego inspektora;

h) może zwrócić się o usługi ekspertów zewnętrznych w dziedzinie technologii informacyjno-komunikacyjnych po uprzednim uzyskaniu zgody urzędnika zatwierdzającego zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE, Euratom) 2018/1046 ([9]);

i) jest zapraszany do odpowiednich podmiotów zarządzających i komitetów SGR, za każdym razem gdy przedmiotem dyskusji są kwestie związane z przetwarzaniem danych osobowych, i może proponować umieszczenie odpowiednich punktów w porządkach obrad tych podmiotów i komitetów;

j) może zwrócić uwagę organu powołującego SGR na niewywiązywanie się przez członka personelu SGR z obowiązków ustanowionych w rozporządzeniu (UE) 2018/1725 i zasugerować wszczęcie administracyjnego postępowania wyjaśniającego, mając na uwadze ewentualne zastosowanie kar określonych w art. 69 tego rozporządzenia;

k) odpowiada, w porozumieniu z odpowiednimi służbami SGR, za wstępne decyzje w sprawie wniosków o dostęp do dokumentów przechowywanych przez jego biuro na podstawie rozporządzenia (WE) nr 1049/2001.

([9]) 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).

SEKCJA 3

PRAWA I OBOWIĄZKI PODMIOTÓW W ZAKRESIE OCHRONY DANYCH

Artykuł 7

Konsultowanie się z inspektorem ochrony danych i przekazywanie mu informacji

1. Administratorzy włączają inspektora ochrony danych w planowanie i omawianie działania, które wiąże się z przetwarzaniem danych osobowych. Inspektor ochrony danych jest informowany o każdej operacji przetwarzania, a także o każdej istotnej zmianie istniejącej operacji przetwarzania.

2. Inspektor ochrony danych jest informowany o projektach wewnętrznych not i decyzji SGR bezpośrednio związanych z wewnętrznym stosowaniem rozporządzenia (UE) 2018/1725.

3. Inspektor ochrony danych jest informowany o wszelkich kontaktach ze stronami zewnętrznymi dotyczących wewnętrznego stosowania rozporządzenia (UE) 2018/1725 oraz o wszelkich kontaktach z EIOD, w szczególności w przypadku konsultowania się z EIOD lub informowania go zgodnie z art. 40 i 41 tego rozporządzenia.

4. W przypadku przetwarzania danych osobowych przez podmiot przetwarzający konsultuje się z inspektorem ochrony danych w sprawie projektów porozumień między współadministratorami oraz projektów klauzul umownych dotyczących ochrony danych lub innych aktów prawnych.

Artykuł 8

Administratorzy delegowani

1. Administratorzy delegowani są odpowiedzialni za zapewnienie, aby wszystkie operacje przetwarzania będące w ich gestii były zgodne z rozporządzeniem (UE) 2018/1725.

2. Administratorzy delegowani w szczególności:

a) wyznaczają administratora odpowiedzialnego za operacje przetwarzania, który ma wspierać administratora delegowanego w zapewnieniu zgodności z rozporządzeniem (UE) 2018/1725, w szczególności w stosunku do osób, których dane dotyczą;

b) dokonują zapisów czynności przetwarzania, za które odpowiadają, oraz zapewniają, by zapisy i związane z nimi oświadczenie o ochronie prywatności były przekazywane inspektorowi ochrony danych przez administratora odpowiedzialnego za operacje przetwarzania w celu wpisania ich do rejestru, o którym mowa a art. 12;

c) są odpowiedzialni za działania podmiotów przetwarzających i podwykonawców przetwarzania, które przetwarzają dane osobowe w ich imieniu, i zapewniają, by przetwarzanie odbywało się na podstawie umowy lub innego aktu prawnego zgodnie z art. 29 ust. 3 rozporządzenia (UE) 2018/1725.

3. Administratorzy delegowani zapewniają, aby inspektor ochrony danych był terminowo włączany we wszystkie kwestie związane z danymi osobowymi i wprowadzają odpowiednie rozwiązania w celu zapewnienia właściwego włączenia koordynatora ds. ochrony danych we wszystkie kwestie związane z ochroną danych w swojej dyrekcji generalnej lub innej służbie SGR.

4. Administratorzy delegowani zapewniają wprowadzenie odpowiednich środków technicznych i organizacyjnych w celu wykazania, że czynności przetwarzania są zgodne z rozporządzeniem (UE) 2018/1725, oraz udzielają personelowi SGR odpowiednich instrukcji, aby zapewnić zarówno poufność przetwarzania, jak i poziom bezpieczeństwa odpowiedni do zagrożeń związanych z przetwarzaniem. Wybierając takie środki mogą zasięgać opinii inspektora ochrony danych.

5. Administratorzy delegowani informują inspektora ochrony danych o rozpatrywaniu wszelkich wniosków otrzymanych od osoby, której dane dotyczą, dotyczących wykonywania przysługujących jej praw i wspierają inspektora ochrony danych i EIOD w wykonywaniu ich obowiązków, w szczególności udzielając informacji w odpowiedzi na ich wnioski w terminie 30 dni.

6. Administratorzy delegowani są odpowiedzialni za stosowanie ograniczenia stosowania art. 14–22, 35 i 36 rozporządzenia (UE) 2018/1725, a także art. 4 tego rozporządzenia, zgodnie z odpowiednimi przepisami wewnętrznymi. Stosując takie ograniczenie, administratorzy delegowani zapewniają udział inspektora ochrony danych w trakcie całej procedury.

7. Administratorzy delegowani zapewniają istnienie wewnętrznych porozumień z innymi dyrekcjami generalnymi lub służbami SGR, jeżeli administrator delegowany przeprowadza operacje przetwarzania wspólnie z tymi dyrekcjami generalnymi lub służbami SGR lub jeżeli przeprowadzają one część operacji przetwarzania administratora delegowanego.

W porozumieniach, o których mowa w akapicie pierwszym, określa się zakres odpowiedzialności administratorów delegowanych i innych dyrekcji generalnych lub służb SGR za niewywiązywanie się z obowiązków w zakresie ochrony danych. W szczególności w porozumieniach tych wskazuje się administratora delegowanego, który określa sposoby i cele operacji przetwarzania, a także administratora odpowiedzialnego za operacje przetwarzania odpowiadającego za daną operację oraz, w stosownych przypadkach, osoby lub podmioty udzielające wsparcia administratorowi odpowiedzialnemu za operacje przetwarzania, między innymi za pomocą informacji o ewentualnym naruszeniu ochrony danych lub w zakresie uwzględnienia praw osób, których dane dotyczą.

Artykuł 9

Administratorzy odpowiedzialni za operacje przetwarzania

1. Administratorzy odpowiedzialni za operacje przetwarzania wspierają administratora delegowanego w zapewnieniu zgodności z rozporządzeniem (UE) 2018/1725 w odniesieniu do operacji przetwarzania, za które jest odpowiedzialny, i pełnią funkcję głównego punktu kontaktowego dla osób, których dane dotyczą.

2. Administratorzy odpowiedzialni za operacje przetwarzania w szczególności:

a) przyjmują i rozpatrują wszystkie wnioski osób, których dane dotyczą;

b) przygotowują w porozumieniu z koordynatorem ds. ochrony danych zapisy czynności przetwarzania, za które są odpowiedzialni, oraz związane z nimi oświadczenie o ochronie prywatności;

c) zapewniają, aby umowy lub inne akty prawne regulujące przetwarzanie danych osobowych przez podmiot przetwarzający były zgodne z rozporządzeniem (UE) 2018/1725, oraz konsultują się z inspektorem ochrony danych w sprawie projektów klauzul umownych dotyczących ochrony danych;

d) zapewniają dostępność dokumentacji w celu wykazania zgodności z rozporządzeniem (UE) 2018/1725.

3. Administratorzy odpowiedzialni za operacje przetwarzania bez zbędnej zwłoki informują inspektora ochrony danych osobowych o naruszeniu ochrony danych osobowych i przekazują mu wszelkie informacje niezbędne, aby umożliwić mu zapewnienie wywiązywania się przez Radę z obowiązków dotyczących naruszeń ochrony danych osobowych wynikających z art. 34 i 35 rozporządzenia (UE) 2018/1725.

4. W koordynacji z administratorem delegowanym i inspektorem ochrony danych administratorzy odpowiedzialni za operacje przetwarzania powiadamiają EIOD w stosownych przypadkach o naruszeniu ochrony danych osobowych. W stosownych przypadkach informują o tym również osoby, których dane dotyczą.

5. Administratorzy odpowiedzialni za operacje przetwarzania zapewniają, aby koordynator ds. ochrony danych wiedział o wszelkich kwestiach związanych z ochroną danych.

6. Administratorzy odpowiedzialni za operacje przetwarzania oceniają zagrożenie dla praw i wolności osoby, której dane dotyczą, w związku z operacjami przetwarzania, za które są odpowiedzialni, oraz, w stosownych przypadkach, przeprowadzają ocenę skutków dla ochrony danych. Przy przeprowadzaniu tych ocen skutków administratorzy odpowiedzialni za operacje przetwarzania zasięgają porady inspektora ochrony danych; zasięgają również jego porady w sprawie konieczności przeprowadzenia uprzednich konsultacji zgodnie z art. 39 i 40 rozporządzenia (UE) 2018/1725.

7. Administratorzy odpowiedzialni za operacje przetwarzania wykonują wszelkie inne zadania wchodzące w zakres stosowania niniejszej decyzji.

Artykuł 10

Koordynatorzy ds. ochrony danych

1. Każda dyrekcja generalna lub inna służba SGR powołuje, w porozumieniu z inspektorem ochrony danych, co najmniej jednego koordynatora ds. ochrony danych, który ma wspierać administratora delegowanego i administratorów odpowiedzialnych za operacje przetwarzania w swojej dyrekcji generalnej lub innej służbie SGR we wszystkich aspektach związanych z ochroną danych osobowych.

2. Koordynatorów ds. ochrony danych wybiera się na podstawie ich wiedzy i doświadczenia w zakresie funkcjonowania danej dyrekcji generalnej lub innej służby SGR, nadawania się do sprawowania tej funkcji, kompetencji związanych z ochroną danych, wiedzy o zasadach systemów informacyjnych i umiejętności komunikacyjnych. Nowo powołani koordynatorzy ds. ochrony danych muszą ukończyć, w ciągu sześciu miesięcy od powołania, szkolenie w celu zdobycia kompetencji niezbędnych do pełnienia funkcji koordynatora ds. ochrony danych. Koordynator ds. ochrony danych, który pracował wcześniej jako osoba kontaktowa w innej dyrekcji generalnej lub innej służbie SGR w ciągu dwóch lat przed powołaniem, jest zwolniony z tego wymogu szkoleniowego.

3. Funkcja koordynatora ds. ochrony danych wchodzi w skład opisu stanowiska pracy każdego członka personelu SGR powołanego na stanowisko osoby kontaktowej. W rocznym sprawozdaniu z oceny tych osób należy odnieść się do ich obowiązków i osiągnięć.

4. Koordynatorzy ds. ochrony danych są odpowiednio i terminowo włączani we wszystkie kwestie związane z ochroną danych w swojej dyrekcji generalnej lub innej służbie SGR i wykonują swoje obowiązki w ścisłej współpracy z inspektorem ochrony danych.

5. Koordynatorzy ds. ochrony danych mają prawo do otrzymania od administratorów i od personelu odpowiednich i niezbędnych informacji potrzebnych do wykonywania swoich zadań w ramach swojej dyrekcji generalnej lub innej służby SGR. Nie obejmuje to dostępu do danych osobowych przetwarzanych na odpowiedzialność administratora delegowanego. Koordynatorzy ds. ochrony danych mają dostęp do danych osobowych wyłącznie wtedy, gdy jest to niezbędne do wykonywania ich zadań.

6. Koordynatorzy ds. ochrony danych upowszechniają wiedzę o kwestiach związanych z ochroną danych i wspierają administratorów delegowanych w swojej dyrekcji generalnej lub innej służbie SGR w wywiązywaniu się przez nich z obowiązków, w szczególności w odniesieniu do:

a) wdrażania rozporządzenia (UE) 2018/1725;

b) ustalania administratorów odpowiedzialnych za operacje przetwarzania, i przygotowanie zapisów czynności przetwarzania i oświadczeń o ochronie prywatności przed ich przekazaniem inspektorowi ochrony danych;

c) sporządzania wykazu wszystkich istniejących operacji przetwarzania danych w dyrekcji generalnej lub innej służbie SGR.

7. Koordynatorzy ds. ochrony danych wspierają administratorów odpowiedzialnych za operacje przetwarzania w swojej dyrekcji generalnej lub innej służbie SGR w wywiązywaniu się przez nich z obowiązków, w szczególności w odniesieniu do:

a) przygotowywania zapisów czynności przetwarzania i oświadczeń o ochronie prywatności przed ich przekazaniem inspektorowi ochrony danych;

b) dokumentowania operacji przetwarzania;

c) przetwarzania wniosków osób, których dane dotyczą;

d) postępowania w przypadku naruszeń danych osobowych.

Artykuł 11

Personel SGR

Personel SGR przyczynia się do zapewnienia stosowania i wdrażania rozporządzenia (UE) 2018/1725. Personel SGR nie może mieć dostępu do danych osobowych ani przetwarzać takich danych inaczej niż na polecenie administratora delegowanego lub administratora odpowiedzialnego za operacje przetwarzania, chyba że wymaga tego prawo Unii lub prawo państwa członkowskiego.

SEKCJA 4

INNE OBOWIĄZKI I PROCEDURY

Artykuł 12

Rejestr

1. Inspektor ochrony danych prowadzi rejestr operacji przetwarzania i zapewnia, by był dostępny za pośrednictwem strony inspektora ochrony danych na stronie intranetowej SGR oraz za pośrednictwem strony internetowej Rady.

2. Administrator odpowiedzialny za operacje przetwarzania powiadamia inspektora ochrony danych o każdej operacji przetwarzania i przedkłada zapisy czynności przetwarzania i związane z nimi oświadczenie o ochronie prywatności, korzystając z formularza dostępnego na stronie intranetowej SGR (w zakładce „ochrona danych"). Powiadomienie przesyła się inspektorowi ochrony danych w formie elektronicznej. Po skonsultowaniu się z inspektorem ochrony danych administrator delegowany potwierdza zapisy i związane z nimi oświadczenie o ochronie prywatności, a inspektor ochrony danych publikuje je w rejestrze.

3. Zapisy zawierają wszystkie informacje określone w art. 31 rozporządzenia (UE) 2018/1725. Jednak w wyjątkowych przypadkach informacje wpisane do rejestru przez inspektora ochrony danych mogą być ograniczone do tego, co jest niezbędne do zapewnienia bezpieczeństwa szczególnej operacji przetwarzania. Inspektor ochrony danych jest bezzwłocznie powiadamiany przez administratora odpowiedzialnego za operacje przetwarzania o każdej zmianie mającej wpływ na takie informacje.

Artykuł 13

Naruszenia ochrony danych

1. W przypadku naruszenia ochrony danych osobowych administrator delegowany lub administrator odpowiedzialny za operacje przetwarzania zwraca się o wsparcie do koordynatora ds. ochrony danych i bez zbędnej zwłoki informuje inspektora ochrony danych o tym incydencie i przekazuje mu wszelkie niezbędne informacje umożliwiające mu zapewnienie, by Rada wywiązała się z obowiązku zgłaszania naruszenia ochrony danych osobowych i zawiadamiania o takim naruszeniu zgodnie z art. 34 i 35 rozporządzenia (UE) 2018/1725.

2. Inspektor ochrony danych tworzy i prowadzi wewnętrzny rejestr naruszeń ochrony danych osobowych. Administratorzy delegowani i administratorzy odpowiedzialni za operacje przetwarzania dostarczają informacji niezbędnych do umieszczenia w tym rejestrze.

3. Administratorzy delegowani i administratorzy odpowiedzialni za operacje przetwarzania przygotowują powiadomienie do EIOD w porozumieniu z inspektorem ochrony danych, chyba że jest mało prawdopodobne, aby naruszenie danych osobowych skutkowało zagrożeniem dla praw i wolności osób fizycznych.

Artykuł 14

Postępowania wyjaśniające

1. Inspektor ochrony danych może z własnej inicjatywy lub na wniosek administratora delegowanego, administratora odpowiedzialnego za operacje przetwarzania lub podmiotu przetwarzającego, Komitetu Pracowniczego lub dowolnej osoby prowadzić postępowania wyjaśniające dotyczące kwestii i zdarzeń odnoszących się bezpośrednio do jego zadań oraz udziela odpowiedzi osobie, która zwróciła się o przeprowadzenie postępowania wyjaśniającego lub administratorowi delegowanemu, administratorowi odpowiedzialnemu za operacje przetwarzania lub podmiotowi przetwarzającemu.

2. Wnioski o przeprowadzenie postępowania wyjaśniającego są kierowane do inspektora ochrony danych na piśmie. W przypadku oczywistego nadużycia prawa do wniosku o przeprowadzenie postępowania wyjaśniającego, na przykład gdy ta sama osoba fizyczna złożyła ostatnio identyczny wniosek, inspektor ochrony danych nie jest zobowiązany do udzielenia odpowiedzi wnioskującemu.

3. W terminie 15 dni od otrzymania wniosku o przeprowadzenie postępowania wyjaśniającego inspektor ochrony danych wysyła osobie, która wystąpiła z wnioskiem, potwierdzenie odbioru, i ustala, czy wniosek należy traktować jako niejawny.

4. Inspektor ochrony danych zwraca się do administratora delegowanego, który odpowiada za operację przetwarzania danych, która jest przedmiotem wniosku o przeprowadzenie postępowania wyjaśniającego, o przygotowanie sprawozdania w tej sprawie. Administrator delegowany przedstawia swoją odpowiedź inspektorowi ochrony danych w terminie 15 dni. Inspektor ochrony danych może zwrócić się do administratora delegowanego, administratora odpowiedzialnego za operacje przetwarzania, podmiotu przetwarzającego lub innych odpowiednich służb SGR o informacje uzupełniające. Tam, gdzie to stosowne, może zwracać się z prośbą o wydanie opinii w tej kwestii przez Służbę Prawną Rady. Inspektor ochrony danych otrzymuje wymagane informacje lub opinię w terminie 30 dni.

5. Inspektor ochrony danych udziela odpowiedzi osobie, która wystąpiła z wnioskiem o przeprowadzenie postępowania wyjaśniającego, nie później niż trzy miesiące od otrzymania wniosku. Bieg tego terminu może zostać wstrzymany do momentu, w którym inspektor ochrony danych otrzyma wszelkie niezbędne informacje, o które się zwrócił.

6. Nikt nie może być niekorzystnie traktowany z powodu zwrócenia uwagi inspektora na domniemane naruszenie rozporządzenia (UE) 2018/1725.

Artykuł 15

Ogólne zasady wykonywania praw przez osoby, których dane dotyczą

1. Prawa osób, których dane dotyczą, określone w art. 14–24 rozporządzenia (UE) 2018/1725 mogą być wykonywane wyłącznie przez osobę, której dane dotyczą, lub jej należycie upoważnionego przedstawiciela.

2. Osoba, której dane dotyczą, kieruje wnioski na piśmie do administratora odpowiedzialnego za operacje przetwarzania wraz z kopią do inspektora ochrony danych. W razie konieczności, inspektor ochrony danych pomaga osobie, której dane dotyczą, w ustaleniu właściwego administratora odpowiedzialnego za operacje przetwarzania. Wniosek można kierować w formie elektronicznej i zawiera on:

a) nazwisko, imię oraz dane kontaktowe osoby, której dane dotyczą, oraz datę złożenia wniosku;

b) wskazanie wykonywanego prawa oraz, w stosownych przypadkach, dokumentów uzupełniających związanych z wnioskiem;

c) kategorię lub kategorie danych osobowych, których dotyczy wniosek.

3. Administrator odpowiedzialny za operacje przetwarzania wysyła osobie, której dane dotyczą, potwierdzenie otrzymania wniosku w terminie pięciu dni roboczych od zarejestrowania wniosku. Jeżeli wniosek jest niejasny lub niekompletny administrator odpowiedzialny za operacje przetwarzania zwraca się o niezbędne wyjaśnienia. Mające zastosowanie terminy, o których mowa w art. 14 ust. 3 i 4 rozporządzenia (UE) 2018/1725, rozpoczynają swój bieg dopiero po przedstawieniu wszystkich niezbędnych wyjaśnień.

4. Administrator odpowiedzialny za operacje przetwarzania weryfikuje tożsamość osoby, której dane dotyczą, zgodnie z art. 14 ust. 6 rozporządzenia (UE) 2018/1725. W trakcie weryfikacji tożsamości nie rozpoczyna się bieg mających zastosowanie terminów, o którym mowa w art. 14 ust. 3 i 4 tego rozporządzenia.

5. Administrator odpowiedzialny za operacje przetwarzania przychyla się do wniosku osoby, której dane dotyczą, lub przedstawia na piśmie powody całkowitej lub częściowej odmowy w terminach określonych w art. 14 ust. 3 i 4 rozporządzenia (UE) 2018/1725.

6. W przypadku bardzo złożonego wniosku, nieprawidłowości lub oczywistego nadużycia ze strony osoby, której dane dotyczą, przy wykonywaniu przysługujących jej praw, jeżeli przetwarzanie wniosku może spowodować zagrożenie dla praw i wolności innych osób, których dane dotyczą, lub gdy osoba, której dane dotyczą, zarzuca, że przetwarzanie jest niezgodne z prawem, administrator odpowiedzialny za operacje przetwarzania konsultuje się z inspektorem ochrony danych.

Artykuł 16

Skargi na podstawie art. 90

W przypadku skargi w rozumieniu art. 90 regulaminu pracowniczego (zwanej dalej „skargą na podstawie art. 90") dotyczącej sprawy związanej z przetwarzaniem danych osobowych organ powołujący konsultuje się z inspektorem ochrony danych. Bez wpływu na dopuszczalność skargi na podstawie art. 90 członek personelu SGR wskazuje w skardze na podstawie art. 90, czy skarga do EIOD została złożona równolegle. Inspektor ochrony danych wydaje swoją opinię na piśmie nie później niż 15 dni roboczych od otrzymania wniosku od organu powołującego. Jeżeli po upływie tego terminu inspektor ochrony danych nie przedstawił swojej opinii, nie jest już ona wymagana. Opinia inspektora ochrony danych nie jest wiążąca dla organu powołującego.

SEKCJA 5

OGRANICZENIA PRAW OSÓB, KTÓRYCH DANE DOTYCZĄ, W ZWIĄZKU Z WYKONYWANIEM ZADAŃ INSPEKTORA OCHRONY DANYCH

Artykuł 17

Zwolnienia i ograniczenia

1. Wykonując swoje obowiązki w odniesieniu do praw osób, których dane dotyczą, zgodnie z rozporządzeniem (UE) 2018/1725, Rada lub SGR uwzględniają, czy zastosowanie mają jakiekolwiek wyjątki określone w tym rozporządzeniu.

2. Z zastrzeżeniem art. 18–22 niniejszej decyzji, Rada lub SGR mogą ograniczyć, zgodnie z art. 25 ust. 1 lit. c), g) i h) rozporządzenia (UE) 2018/1725, stosowanie art. 14–17, 19, 20 i 35 tego rozporządzenia, a także stosowanie zasady przejrzystości określonej w art. 4 ust. 1 lit. a) tego rozporządzenia, w zakresie, w jakim przepisy tego artykułu odpowiadają prawom i obowiązkom określonym w art. 14–17, 19 i 20 tego rozporządzenia, w przypadku gdy wykonywanie tych praw i obowiązków zagrażałoby wykonywaniu zadań inspektora ochrony danych, między innymi przez ujawnienie jego narzędzi i metod prowadzenia postępowań wyjaśniających i audytów, lub naruszałoby prawa i wolności innych osób, których dane dotyczą.

3. Z zastrzeżeniem art. 18–22 niniejszej decyzji Rada lub SGR mogą ograniczyć prawa i obowiązki, o których mowa w ust. 2 niniejszego artykułu, w odniesieniu do danych osobowych uzyskanych przez inspektora ochrony danych od dyrekcji generalnych lub służb SGR lub innych instytucji lub organów Unii. Rada lub SGR mogą to uczynić, gdy wykonywanie tych praw i obowiązków może zostać ograniczone przez te dyrekcje generalne lub służby SGR lub inne instytucje lub organy na podstawie innych aktów, o których mowa w art. 25 rozporządzenia (UE) 2018/1725, lub zgodnie z rozdziałem IX tego rozporządzenia lub zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/794 ([10]) lub rozporządzeniem Rady (UE) 2017/1939 ([11]).

Przed zastosowaniem ograniczeń w okolicznościach, o których mowa w akapicie pierwszym, Rada lub SGR konsultują się z odpowiednią instytucją lub organem Unii, chyba że jest jasne, że stosowanie ograniczenia jest przewidziane w jednym z aktów, o których mowa w tym akapicie.

4. Wszelkie ograniczenia praw i obowiązków, o których mowa w ust. 2, muszą być konieczne i proporcjonalne oraz uwzględniać zagrożenia dla praw i wolności osób, których dane dotyczą.

Artykuł 18

Przekazywanie informacji osobom, których dane dotyczą

1. SGR publikuje na stronie internetowej Rady noty na temat ochrony danych, w których informuje osoby, których dane dotyczą, o zadaniach inspektora ochrony danych obejmujących przetwarzanie ich danych osobowych.

2. SGR indywidualnie informuje, w odpowiedniej formie, każdą osobę fizyczną, którą uważa za osobę, której dotyczą zadania inspektora ochrony danych.

3. W przypadku gdy SGR ogranicza, całkowicie lub częściowo, przekazywanie informacji osobom, których dane dotyczą, o których mowa w ust. 2 niniejszego artykułu, zapisuje i rejestruje powody ograniczenia zgodnie z art. 21.

([10]) 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).

([11]) 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).

Artykuł 19

Prawo dostępu przysługujące osobom, których dane dotyczą, prawo do usunięcia danych oraz prawo do ograniczenia przetwarzania

1. W przypadku ograniczenia, całkowitego lub częściowego, prawa dostępu do danych osobowych przysługującego osobom, których dane dotyczą, prawa do usunięcia danych lub prawa do ograniczenia przetwarzania, o których mowa odpowiednio w art. 17, 19 i 20 rozporządzenia (UE) 2018/1725, Rada lub SGR informuje zainteresowaną osobę, której dane dotyczą, w odpowiedzi na jej wniosek o dostęp, usunięcie lub ograniczenie przetwarzania, o zastosowanym ograniczeniu i o jego głównych powodach oraz o możliwości złożenia skargi do EIOD lub do skorzystania ze środka ochrony prawnej przed Trybunałem Sprawiedliwości Unii Europejskiej.

2. Przekazanie informacji dotyczących powodów ograniczenia, o którym mowa w ust. 1, może zostać wstrzymane, pominięte lub można go odmówić tak długo, jak długo takie przekazanie naruszałoby cel ograniczenia. Rada przekazuje informacje osobie, której dane dotyczą, gdy tylko takie informacje nie zagrażają realizacji tego celu.

3. SGR zapisuje i rejestruje powody ograniczenia zgodnie z art. 21.

Artykuł 20

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

W przypadku gdy Rada lub SGR ogranicza zawiadomienie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, jak określono w art. 35 rozporządzenia (UE) 2018/1725, zapisuje i rejestruje powody ograniczenia zgodnie z art. 21 niniejszej decyzji.

Artykuł 21

Zapisywanie i rejestrowanie ograniczeń

1. SGR zapisuje powody wszelkich ograniczeń zastosowanych zgodnie z niniejszą decyzją, dodając przy tym każdorazowo ocenę ich konieczności i proporcjonalności, z uwzględnieniem odpowiednich elementów art. 25 ust. 2 rozporządzenia (UE) 2018/1725.

W tym celu w zapisie określa się, w jaki sposób wykonywanie któregokolwiek z praw, o których mowa w art. 14–17, 19, 20 i 35 tego rozporządzenia, lub stosowanie zasady przejrzystości określonej w art. 4 ust. 1 lit. a) tego rozporządzenia, mogłoby zagrozić działaniom inspektora ochrony danych wykonywanym na podstawie niniejszej decyzji lub ograniczeniom zastosowanym zgodnie z art. 17 ust. 2 lub 3 niniejszej decyzji, lub jaki negatywny wpływ wywarłoby na prawa i wolności innych osób, których dane dotyczą.

2. Zapis oraz, w stosownych przypadkach, dokumenty zawierające stanowiące jego podstawę elementy stanu faktycznego oraz aspekty prawne zamieszcza się w rejestrze. Udostępnia się je EIOD na żądanie.

Artykuł 22

Okres obowiązywania ograniczeń

1. Ograniczenia, o których mowa w art. 18, 19 i 20, stosuje się tak długo, jak długo mają zastosowanie powody uzasadniające ich zastosowanie.

2. W przypadku gdy powody ograniczenia, o którym mowa w art. 18 i 20, nie mają już zastosowania, SGR znosi ograniczenie i podaje powody ograniczenia osobie, której dane dotyczą. Jednocześnie SGR informuje osobę, której dane dotyczą, o możliwości złożenia w dowolnym momencie skargi do EIOD lub możliwości skorzystania ze środka ochrony prawnej przed Trybunałem Sprawiedliwości Unii Europejskiej.

3. SGR dokonuje przeglądu stosowania ograniczeń, o których mowa w art. 18 i 20, co sześć miesięcy od ich przyjęcia, a w każdym razie w momencie zakończenia odpowiedniego zadania inspektora ochrony danych. Po takim zakończeniu SGR monitoruje raz w roku konieczność zachowania jakichkolwiek ograniczeń lub wstrzymania przekazania informacji.

Artykuł 23

Przegląd dokonywany przez inspektora ochrony danych

1. W przypadku gdy inne dyrekcje generalne lub służby SGR stwierdzają, że prawa osoby, której dane dotyczą, powinny zostać ograniczone na podstawie niniejszej decyzji, informują o tym inspektora ochrony danych. Zapewniają ponadto inspektorowi ochrony danych dostęp do zapisów oraz wszelkich dokumentów zawierających stanowiące ich podstawę elementy stanu faktycznego oraz aspekty prawne. Udział inspektora ochrony danych w stosowaniu ograniczeń jest szczegółowo dokumentowany.

2. Inspektor ochrony danych może zwrócić się do danego administratora delegowanego o dokonanie przeglądu stosowania ograniczeń. Dany administrator delegowany informuje na piśmie inspektora ochrony danych osobowych o wyniku wnioskowanego przeglądu.

SEKCJA 6

POSTANOWIENIA KOŃCOWE

Artykuł 24

Uchylenie

Decyzja 2004/644/WE zostaje uchylona.

Artykuł 25

Wejście w życie

Niniejsza decyzja wchodzi w życie dwudziestego dnia po jej opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

Sporządzono w Luksemburgu dnia 28 czerwca 2021 r.

W imieniu Rady
M. do C. ANTUNES
Przewodniczący