

# EUROPEJSKA SŁUŻBA DZIAŁAŃ ZEWNĘTRZNYCH

**Decyzja Wysokiego Przedstawiciela Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa  
z dnia 1 października 2019 r.**

**w sprawie przepisów wykonawczych dotyczących ochrony danych osobowych przez Europejską  
Służbę Działań Zewnętrznych oraz stosowania rozporządzenia Parlamentu Europejskiego i Rady  
(UE) 2018/1725**

(2019/C 370/05)

WYSOKI PRZEDSTAWICIEL UNII DO SPRAW ZAGRANICZNYCH I POLITYKI BEZPIECZEŃSTWA,

uwzględniając decyzję Rady 2010/427/UE z dnia 26 lipca 2010 r. określającą organizację i zasady funkcjonowania Europejskiej Służby Działań Zewnętrznych (2010/427/UE) <sup>(1)</sup> („decyzja Rady ESDZ”), w szczególności jej art. 11 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 <sup>(2)</sup> („rozporządzenie”), w szczególności jego art. 43, 44 i 45,

a także mając na uwadze, co następuje:

- (1) Ustanowiona w rozporządzeniu zwiększona odpowiedzialność administratorów danych wymaga przyjęcia nowej decyzji wykonawczej zastępującej decyzję PROC HR(2011) 016 Wysokiego Przedstawiciela Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa z dnia 8 grudnia 2011 r. w sprawie przepisów dotyczących ochrony danych w ESDZ.
- (2) Rola inspektora ochrony danych i obowiązki administratora danych w ramach Europejskiej Służby Działań Zewnętrznych muszą zostać jasno określone i dostosowane do wymogów rozporządzenia,

STANOWI, CO NASTĘPUJE:

## SEKCJA 1

### PRZEPISY OGÓLNE

#### Artykuł 1

#### Przedmiot i zakres stosowania

1. Zgodnie z art. 45 ust. 3 rozporządzenia w niniejszej decyzji określa się zadania, obowiązki i uprawnienia inspektora ochrony danych (zwanego dalej „IOD”) w ramach ESDZ.
2. W niniejszej decyzji określa się również procedury wewnętrzne i obowiązki administratorów danych i podmiotów przetwarzających oraz rolę, zadania i obowiązki koordynatorów ds. ochrony danych i korespondentów, w szczególności na podstawie art. 26 i 29 rozporządzenia.

#### Artykuł 2

#### Definicje

Do celów niniejszej decyzji i bez uszczerbku dla definicji zawartych w rozporządzeniu:

- a) „administrator danych” oznacza ESDZ lub jej jednostki organizacyjne, w tym delegatury UE, które samodzielnie lub wspólnie z innymi określają cele i sposoby przetwarzania danych osobowych;

<sup>(1)</sup> Dz.U. L 201 z 3.8.2010, s. 30.

<sup>(2)</sup> Dz.U. L 295 z 21.11.2018, s. 39.

- b) „przedstawiciel administratora danych” oznacza członków kierownictwa ESDZ lub kierowników jednostek organizacyjnych sprawujących nadzór nad jednostkami organizacyjnymi administratora danych, o których to jednostkach organizacyjnych mowa powyżej w lit. a) i które są odpowiedzialne za przetwarzanie danych osobowych;
- c) „delegowany administrator danych” oznacza służbę lub personel w jednostce organizacyjnej administratora danych, którym powierzono zarządzanie czynnościami w zakresie przetwarzania danych osobowych;
- d) „współadministratorzy” oznaczają co najmniej dwie jednostki organizacyjne, które wspólnie określają cele i sposoby przetwarzania danych osobowych oraz role i obowiązki administratorów, w tym ich obowiązki związane z wykonywaniem praw osoby, której dane dotyczą, w szczególności gdy ESDZ wspólnie kontroluje przetwarzanie danych z innymi instytucjami, organami, agencjami, urzędami lub innymi podmiotami UE;
- e) „inspektor ochrony danych (»IOD«)” oznacza członka personelu ESDZ wyznaczonego przez ESDZ zgodnie z art. 43 rozporządzenia do wspierania i informowania administratorów danych oraz doradzania im;
- f) „koordynator i korespondent ds. ochrony danych” oznacza odpowiednio pracowników ESDZ w siedzibie głównej i w delegaturach UE, wyznaczonych do wspierania swoich administratorów danych w kwestiach związanych z ochroną danych;
- g) „podmiot przetwarzający” oznacza jednostkę organizacyjną w ESDZ lub poza ESDZ, która przetwarza dane osobowe w imieniu administratora danych;
- h) „informacje o ochronie danych osobowych” to zawiadomienia, takie jak oświadczenia o ochronie prywatności, za pomocą których administrator danych przekazuje informacje osobom, których dane dotyczą, zgodnie z art. 15 i 16 rozporządzenia;
- i) „personel ESDZ” oznacza – zgodnie z art. 6 decyzji Rady ESDZ – urzędników i innych pracowników UE pracujących dla ESDZ, w tym personel służb dyplomatycznych państw członkowskich UE, oddelegowanych ekspertów krajowych i stażystów.

## SEKCJA 2

### INSPEKTOR OCHRONY DANYCH

#### Artykuł 3

#### **Wyznaczenie inspektora ochrony danych**

1. Sekretarz generalny ESDZ wyznacza IOD spośród personelu ESDZ zgodnie z art. 43 rozporządzenia i rejestruje go u Europejskiego Inspektora Ochrony Danych (zwanego dalej „EIOD”).
2. Oprócz wymogów wynikających z art. 43 ust. 3 rozporządzenia IOD posiada solidną wiedzę o służbach ESDZ, ich strukturze, systemach informacyjnych oraz przepisach i procedurach administracyjnych. IOD posiada wiedzę fachową w dziedzinie ochrony danych, zdolność do właściwego osądu oraz do zachowania bezstronnego i obiektywnego podejścia zgodnie z regulaminem pracowniczym.
3. IOD jest wyznaczany na pięcioletnią kadencję i może on zostać mianowany ponownie.
4. IOD może zostać zwolniony ze stanowiska wyłącznie za zgodą EIOD, jeżeli przestał spełniać warunki konieczne do wykonywania swoich obowiązków.
5. IOD jest administracyjnie powiązany z Sekretarzem Generalnym.
6. Dane kontaktowe IOD są publikowane w intranecie ESDZ i na zewnętrznej stronie internetowej ESDZ oraz przekazywane EIOD.

#### Artykuł 4

#### **Status inspektora ochrony danych**

1. IOD działa niezależnie i we współpracy z EIOD. ESDZ nie wydaje IOD żadnych instrukcji w odniesieniu do wykonywania jego zadań.
2. IOD nie może zostać zwolniony ani karany za wykonywanie swoich zadań.
3. IOD jest informowany o wszelkich kontaktach z podmiotami zewnętrznymi w sprawie stosowania rozporządzenia i niniejszej decyzji, w szczególności o wszelkich kontaktach z EIOD i z członkami sieci IOD w instytucjach, organach, urzędach i agencjach UE.

4. Osoby, których dane dotyczą, mogą skontaktować się z IOD w każdej sprawie związanej z przetwarzaniem ich danych osobowych lub z korzystaniem z praw przysługujących im na mocy rozporządzenia.
5. Administrator danych lub jego przedstawiciel, Komitet Pracowniczy oraz każdy członek personelu mogą konsultować się z IOD we wszelkich sprawach dotyczących interpretacji lub stosowania rozporządzenia, bez konieczności korzystania z oficjalnych kanałów. Nikt nie może doznać uszczerbku z powodu zgłoszenia sprawy IOD.

#### Artykuł 5

### Zadania inspektora ochrony danych

IOD:

- a) konsultowany jest we wszystkich kwestiach dotyczących ochrony danych osobowych;
- b) udziela wskazówek i aktywnie doradza jednostkom organizacyjnym ESDZ i ich wykonawcom, którzy prowadzą czynności w zakresie przetwarzania danych osobowych, w sprawie sposobu wykonania rozporządzenia i niniejszej decyzji, w tym prowadzi konsultacje w sprawie powiadomień o naruszeniu ochrony danych, ocen skutków i konieczności uprzednich konsultacji z EIOD;
- c) utrzymuje regularne kontakty z administratorami danych w celu monitorowania zgodności z przepisami w zakresie ochrony danych oraz wspierania ich w realizacji ich zadań, w szczególności w celu przyczynienia się do przygotowywania i publikowania informacji o ochronie danych osobowych i udzielania odpowiedzi na wnioski od osób, których dane dotyczą;
- d) utrzymuje regularne kontakty z koordynatorami i korespondentami ds. ochrony danych w siedzibie głównej ESDZ i delegaturach UE oraz zarządza siecią koordynatorów i korespondentów ds. ochrony danych w ramach ESDZ;
- e) podnosi ogólną świadomość na temat ochrony danych osobowych, organizuje szkolenia i sesje informacyjne;
- f) współpracuje z IOD z innych instytucji, organów, urzędów i agencji UE, w szczególności poprzez wymianę doświadczeń i najlepszych praktyk;
- g) prowadzi centralny rejestr czynności w zakresie przetwarzania prowadzonych przez ESDZ w oparciu o dokumentację przygotowaną przez administratorów danych zgodnie z art. 31 rozporządzenia i udostępnia ten rejestr publicznie;
- h) pomaga w zapewnieniu, by Wysoki Przedstawiciel lub ESDZ byli reprezentowani na szczeblu międzynarodowym we wszystkich kwestiach związanych z ochroną danych.

#### Artykuł 6

### Uprawnienia

Wykonując swoje zadania, IOD:

- a) ma stały dostęp do danych przetwarzanych przez podmioty ESDZ i ich wykonawców oraz do wszystkich biur, centrów przetwarzania danych i nośników danych;
- b) przedstawia swoją opinię organowi powołującemu przed podjęciem jakiegokolwiek decyzji w sprawach dotyczących stosowania przepisów o ochronie danych;
- c) może proponować środki administracyjne i wydawać ogólne zalecenia w sprawie właściwego stosowania rozporządzenia i niniejszej decyzji;
- d) może wydawać zalecenia dotyczące praktycznego usprawnienia ochrony danych skierowane do kierownictwa lub personelu ESDZ bądź każdego odpowiedniego podmiotu zewnętrznego;
- e) może prowadzić dochodzenia w sprawach z zakresu ochrony danych oraz – oprócz osoby, która wystąpiła z wnioskiem o wszczęcie dochodzenia lub złożyła skargę – może poinformować o wyniku dochodzenia administratora danych oraz każdego odpowiedniego członka kierownictwa ESDZ;
- f) może opracowywać wzory dokumentów i procedury wewnętrzne, instrukcje lub polityki w celu zapewnienia wskazówek administratorom danych i podmiotom przetwarzającym;
- g) może korzystać z usług ekspertów zewnętrznych, w tym specjalistów w dziedzinie IT;
- h) może informować organ powołujący ESDZ o wszelkich przypadkach niewywiązania się przez członka personelu z obowiązków wynikających z rozporządzenia i z niniejszej decyzji oraz proponować wszczęcie dochodzenia administracyjnego;
- i) może wydawać wewnętrzne wytyczne w sprawie ochrony danych (noty przewodnie IOD), które są brane pod uwagę przy przetwarzaniu danych osobowych.

## Artykuł 7

**Zasoby**

1. IOD zapewnia się odpowiedni personel i zasoby niezbędne do wykonywania zadań, o których mowa w art. 5 niniejszej decyzji.
2. Wszyscy członkowie personelu ESDZ wspierają IOD w wykonywaniu zadań, o których mowa w art. 5 niniejszej decyzji; w szczególności administratorzy danych i podmioty przetwarzające przekazują wymagane informacje na temat czynności w zakresie przetwarzania danych oraz dostępu do danych osobowych i przygotowują projekty odpowiedzi na wnioski od osób, których dane dotyczą, korzystających z prawa do dostępu do danych, ich zmiany i usuwania, które to wnioski otrzymał IOD, ale są one związane z czynnościami w zakresie przetwarzania, za które odpowiedzialny jest administrator danych.
3. IOD może mieć zastępcę lub asystenta IOD, a także – w razie potrzeby – personel administracyjny i wsparcie sekretarskie. IOD może również korzystać z pomocy innych jednostek organizacyjnych ESDZ lub zaangażowanych podmiotów zewnętrznych i ekspertów zewnętrznych.
4. Po wyznaczeniu zastępcy lub asystent IOD wspiera IOD w wykonywaniu jego zadań i może reprezentować go w razie jego nieobecności. Art. 4, 5 i 6 niniejszej decyzji stosuje się również do zastępcy lub asystenta IOD.
5. IOD posiada odpowiednie pomieszczenia, w których można zagwarantować bezpieczeństwo i poufność informacji, w tym danych osobowych, oraz zapewnić odpowiednie przechowywanie i archiwizowanie danych i dokumentów.
6. IOD ma do dyspozycji narzędzie elektroniczne, które może (i) zarządzać rejestrami działań w zakresie przetwarzania danych osobowych zgodnie z art. 31 rozporządzenia oraz (ii) przechowywać informacje o ochronie danych osobowych, powiadomienia o naruszeniu ochrony danych, oceny skutków dla ochrony danych, wnioski od osób, których dane dotyczą, oraz rejestry dotyczące przekazywania danych.
7. ESDZ wspiera IOD w utrzymywaniu i poszerzaniu jego wiedzy fachowej, między innymi poprzez ułatwianie udziału w międzyinstytucjonalnych lub zewnętrznych szkoleniach, konferencjach lub wydarzeniach związanych z ochroną danych oraz w spotkaniach i szkoleniach organizowanych przez EIOD i sieć IOD instytucji, organów, urzędów i agencji UE.

## SEKCJA 3

**PODMIOTY ZAANGAŻOWANE W PROCEDURY ZWIĄZANE Z OCHRONĄ DANYCH**

## Artykuł 8

**Administratorzy danych i podmioty przetwarzające**

1. Delegowani administratorzy danych, przedstawiciele administratorów danych i podmiotów przetwarzających są odpowiedzialni, w imieniu administratora danych, za zapewnienie zgodności wszystkich czynności w zakresie przetwarzania będących pod ich kontrolą z rozporządzeniem, w szczególności z jego art. 26, oraz z przepisami niniejszej decyzji. W razie potrzeby mogą oni powierzyć zadania przetwarzania danych członkom personelu Europejskiej Służby Działań Zewnętrznych wykonującym pracę pod ich kierownictwem lub podmiotom zewnętrznym na podstawie zlecenia, zgodnie z art. 29 rozporządzenia.
2. W szczególności administratorzy danych:
  - a) ponoszą odpowiedzialność, zapewniają, by przetwarzanie danych odbywało się zgodnie z rozporządzeniem i niniejszą decyzją, oraz wykazują to;
  - b) rejestrują wszelkie czynności w zakresie przetwarzania oraz wszelkie istotne zmiany w istniejących czynnościach w zakresie przetwarzania;
  - c) zapewniają, by osoby, których dane dotyczą, były informowane o przetwarzaniu ich danych zgodnie z art. 15 i 16 rozporządzenia poprzez udostępnianie informacji o ochronie danych osobowych;
  - d) współpracują z IOD i EIOD, w szczególności udzielając informacji w odpowiedzi na ich wnioski w ciągu 14 dni kalendarzowych od daty wniosku;

- e) informują IOD w przypadku wykorzystywania podmiotu zewnętrznego do przetwarzania danych osobowych w imieniu administratora danych;
  - f) wyznaczają koordynatora i korespondenta ds. ochrony danych, wspierają go w wypełnianiu jego obowiązków oraz informują IOD o wszelkich zmianach dotyczących osoby lub funkcji koordynatora i korespondenta ds. ochrony danych;
  - g) przeprowadzają konsultacje z IOD w sprawie tego, czy czynności w zakresie przetwarzania są zgodne z rozporządzeniem i niniejszą decyzją. Mogą konsultować się z IOD lub innymi ekspertami w kwestiach dotyczących poufności, dostępności i integralności czynności w zakresie przetwarzania oraz środków bezpieczeństwa zastosowanych zgodnie z art. 33 rozporządzenia.
3. Administratorzy danych mogą wykorzystywać inne podmioty w ESDZ lub podmioty zewnętrzne jako podmioty przetwarzające zgodnie z przepisami rozporządzenia, o ile dokumentują w swoich rejestrach, jaki podmiot jest podmiotem przetwarzającym, wyszczególniają powierzone mu zadania oraz wprowadzone środki bezpieczeństwa.
4. Administrator danych zapewnia, by IOD został niezwłocznie powiadomiony o:
- a) wszelkich kwestiach, które mają lub mogą mieć wpływ na ochronę danych;
  - b) wszelkich komunikatach i decyzjach kierownictwa ESDZ związanych ze stosowaniem rozporządzenia, w szczególności o wszelkich kontaktach z EIOD.

#### Artykuł 9

#### **Koordinator i korespondent ds. ochrony danych**

1. W zależności od wielkości jednostki organizacyjnej ESDZ i rodzaju przetwarzanych danych osobowych jednostki te posiadają koordynatora i korespondenta ds. ochrony danych, który pełni funkcję centralnego punktu kontaktowego w kwestiach ochrony danych. Każda dyrekcja zarządzająca lub dyrekcja w siedzibie głównej ESDZ i każda delegatura UE wyznaczają koordynatora ds. ochrony danych lub korespondenta ds. ochrony danych. Wszystkie działy, które regularnie przetwarzają znaczną ilość danych osobowych, szczególnie kategorie danych lub szczególnie chronione dane osobowe, których przetwarzanie wiąże się z wysokim ryzykiem, również wyznaczają własnego koordynatora i korespondenta ds. ochrony danych. Funkcja koordynatora i korespondenta ds. ochrony danych jest przypisana do stanowiska, które posiada przegląd działań danej jednostki organizacyjnej.
2. Koordynator i korespondent ds. ochrony danych posiada niezbędne umiejętności i zdobywa wiedzę na temat ochrony danych. Przechodzi on szkolenie wprowadzające na temat ochrony danych oraz może uczestniczyć w sesjach informacyjnych i spotkaniach sieci koordynatorów i korespondentów ds. ochrony danych.
3. Koordynator i korespondent ds. ochrony danych:
- a) bez uszczerbku dla obowiązków IOD pomaga administratorom danych w wypełnianiu ich obowiązków;
  - b) ułatwia komunikację między IOD a administratorami danych;
  - c) stanowi centralny punkt kontaktowy w swojej służbie w sprawach dotyczących ochrony danych i współpracuje z IOD;
  - d) informuje i wspiera swoich współpracowników w sprawach związanych z przetwarzaniem danych osobowych;
  - e) przekazuje personelowi informacje na temat organizowanych wydarzeń podnoszących świadomość i sesji szkoleniowych;
  - f) współpracuje z IOD w celu sporządzenia i aktualizacji spisu istniejących i nowych czynności w zakresie przetwarzania danych osobowych;
  - g) kontaktuje się z IOD i powiadamia go o wszelkim przetwarzaniu danych osobowych w danej służbie;
  - h) pomaga we wskazywaniu odpowiednich delegowanych administratorów danych i podmiotów przetwarzających;
  - i) opracowuje rejestry w swoich dziedzinach wiedzy fachowej;
  - j) wspiera administratorów danych w tworzeniu i dokonywaniu przeglądu rejestrów oraz opracowywaniu informacji o ochronie danych osobowych;
  - k) przyczynia się do sporządzania weryfikacji zgodności i ocen skutków;
  - l) zapewnia, by odpowiednie informacje o ochronie danych osobowych były publikowane i właściwie wykorzystywane przez jego służbę;

- m) powiadamia IOD o wszelkich naruszeniach ochrony danych;
- n) we współpracy z IOD przygotowuje odpowiedzi na wnioski od osób, których dane dotyczą, o wykonywanie przysługujących im praw, rozpatrywanie skarg i pytań dotyczących czynności w zakresie przetwarzania danych w jego służbie.
4. Koordynator i korespondent ds. ochrony danych ma prawo do uzyskania informacji niezbędnych do wskazania czynności w zakresie przetwarzania danych osobowych oraz do przeprowadzenia konsultacji z IOD w imieniu swojej służby. Nie obejmuje to prawa dostępu do danych osobowych przetwarzanych w ramach obowiązków administratora danych.

#### Artykuł 10

### Organ powołujący

Organ powołujący konsultuje się z IOD w sprawie każdego wniosku lub skargi na podstawie art. 90 regulaminu pracowniczego w odniesieniu do stosowania rozporządzenia.

#### Artykuł 11

### Personel ESDZ

1. Wszyscy członkowie personelu ESDZ stosują zasady poufności i bezpieczeństwa w odniesieniu do przetwarzania danych osobowych określone w art. 33, 34 i 35 rozporządzenia. Żaden członek personelu ESDZ posiadający dostęp do danych osobowych nie przetwarza danych inaczej niż na polecenie administratorów danych.
2. Wszyscy członkowie personelu ESDZ informują swojego bezpośredniego przełożonego, gdy muszą przetwarzać dane osobowe, tak aby administratorzy danych mogli udokumentować to przetwarzanie w swoich rejestrach dotyczących ochrony danych oraz opracować niezbędne informacje o ochronie danych osobowych.
3. Każdy członek personelu ESDZ może złożyć do IOD wniosek lub wyrazić zaniepokojenie, w tym w sprawie domniemanego naruszenia danych, lub złożyć skargę do EIOD w sprawie domniemanego naruszenia rozporządzenia lub niniejszej decyzji, bez konieczności informowania swoich przełożonych.
4. Jeżeli którykolwiek z członków personelu uzna, że państwo trzecie, terytorium lub określony(-e) sektor(-y) w państwie trzecim lub organizacja międzynarodowa nie zapewniają odpowiedniego poziomu ochrony w rozumieniu art. 45 ust. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 <sup>(3)</sup> lub art. 36 ust. 3 dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 <sup>(4)</sup>, informują o tym IOD.

#### SEKCJA 4

### ŚRODKI I PROCEDURY

#### Artykuł 12

### Środki bezpieczeństwa oraz ochrona danych w fazie projektowania i domyślna ochrona danych

1. Środki bezpieczeństwa, środki techniczne i organizacyjne w celu uniknięcia przypadków naruszenia danych, wycieku danych lub nieuprawnionego ujawnienia obejmują:
  - a) odpowiednie określenie ról, obowiązków i etapów proceduralnych;
  - b) bezpieczne środowisko elektroniczne, które uniemożliwia bezprawny lub przypadkowy dostęp lub przekazanie danych elektronicznych osobom nieupoważnionym, wraz ze środkami bezpieczeństwa wbudowanymi w różne wykorzystywane aplikacje informatyczne;

<sup>(3)</sup> 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).

<sup>(4)</sup> 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 uchyłająca decyzję ramową Rady 2008/977/WSiSW (Dz.U. L 119 z 4.5.2016, s. 89).

- c) bezpieczne przetwarzanie i przechowywanie dokumentów w formie papierowej;
- d) elektroniczny i fizyczny dostęp wyłącznie dla uprawnionych pracowników posiadających indywidualnie przyznane prawa dostępu.

2. Przed zaprojektowaniem czynności w zakresie przetwarzaniem danych administratorzy danych wdrażają ochronę danych już w fazie projektowania oraz domyślną ochronę danych, o czym mowa w art. 27 rozporządzenia. W celu wdrożenia ochrony danych już w fazie projektowania i domyślnej ochrony danych administrator danych może skonsultować się z IOD i innymi właściwymi służbami, w tym ze służbami informatycznymi i służbami bezpieczeństwa informatycznego.

### Artykuł 13

#### **Powiadomienia o naruszeniu ochrony danych**

Po stwierdzeniu jakiegokolwiek zdarzenia, w szczególności naruszenia bezpieczeństwa, prowadzącego do przypadkowego lub niezgodnego z prawem zniszczenia, utraty, zmiany, nieuprawnionego ujawnienia danych lub dostępu do danych osobowych przekazywanych, przechowywanych lub przetwarzanych w inny sposób („naruszenie ochrony danych osobowych”), administrator danych lub podmiot przetwarzający niezwłocznie powiadamia o tym IOD i w ciągu 72 godzin EIOD oraz odpowiednio dokumentuje to zdarzenie.

### Artykuł 14

#### **Dochodzenia oraz rozpatrywanie wniosków i skarg przez IOD**

1. IOD może z własnej inicjatywy lub na wniosek innej osoby wszcząć dochodzenie w sprawie domniemanego naruszenia obowiązków wynikających z rozporządzenia. Wnioski kierowane są do IOD na piśmie.
2. IOD może zwrócić się do administratora danych odpowiedzialnego za daną czynność w zakresie przetwarzania danych o pisemne oświadczenie w danej sprawie. Administrator danych przekazuje odpowiedź IOD w terminie 14 dni kalendarzowych od otrzymania takiego wniosku. IOD może zwrócić się o dostęp do informacji uzupełniających, dokumentów, nośników danych, centrów danych, pomieszczeń i systemów innych służb ESDZ, w szczególności działu informacyjnego, dyrekcji ds. bezpieczeństwa oraz dyrekcji generalnej zajmującej się dochodzeniami administracyjnymi i procedurami dyscyplinarnymi. IOD otrzymuje odnośne informacje lub opinię w terminie 14 dni kalendarzowych.
3. W przypadku wniosków w sposób oczywisty bezzasadnych, stanowiących nadużycie i nadmiernych, w szczególności wniosków o powtarzalnym charakterze składanych przez tę samą osobę, której dane dotyczą, IOD może odmówić podjęcia decyzji w sprawie wniosku zgodnie z art. 14 rozporządzenia. Wnioskodawca jest odpowiednio informowany.

### SEKCJA 5

#### **PROCEDURA KORZYSTANIA ZE SWOICH PRAW PRZEZ OSOBY, KTÓRYCH DANE DOTYCZĄ**

### Artykuł 15

#### **Przepisy ogólne**

1. Osoby, których dane dotyczą, mogą skontaktować się z administratorem danych lub z IOD w celu skorzystania ze swoich praw zgodnie z art. 14–24 rozporządzenia.
2. Wnioski o skorzystanie ze swoich praw od osób, których dane dotyczą, są sporządzane na piśmie. W razie konieczności IOD pomaga osobie, której dane dotyczą, w ustaleniu właściwego administratora danych. IOD przekazuje wszelkie otrzymane wnioski odpowiedniemu administratorowi danych, który może skonsultować się z IOD.
3. Administratorzy danych rozpatrują wniosek i udzielają odpowiedzi bezpośrednio osobie, której dane dotyczą.

### Artykuł 16

#### Rozpatrywanie wniosków o skorzystanie ze swoich praw od osób, których dane dotyczą

1. Administratorzy danych rozpatrują otrzymany wniosek wyłącznie po zweryfikowaniu tożsamości wnioskodawcy lub – w przypadku wniosku od przedstawiciela osoby, której dane dotyczą – po otrzymaniu upoważnienia od osoby, której dane dotyczą.
2. Administrator danych odpowiedzialny za przetwarzanie danych wysła wnioskodawcy potwierdzenie odbioru w terminie 14 dni kalendarzowych od otrzymania wniosku przez ESDZ. Jeżeli nie postanowiono inaczej, administrator danych udziela odpowiedzi na wniosek w terminie 1 miesiąca od rejestracji wniosku. Administrator danych udziela na wniosek pozytywnej odpowiedzi albo podaje na piśmie przyczyny całkowitej lub częściowej odmowy. Termin na udzielenie odpowiedzi może zostać przedłużony o kolejne 2 miesiące, biorąc pod uwagę złożoność sprawy i liczbę złożonych wniosków, zgodnie z art. 14 ust. 3 rozporządzenia.
3. Wniosek od osoby, której dane dotyczą, może zostać odrzucony, jeżeli:
  - a) wniosek nie jest uzasadniony;
  - b) zastosowanie ma wyjątek ustanowiony w rozporządzeniu;
  - c) zastosowanie ma ograniczenie zgodnie z zasadami wewnętrznymi <sup>(5)</sup> przyjętymi na podstawie art. 25 rozporządzenia.
4. W przypadku wniosków w sposób oczywisty bezzasadnych, stanowiących nadużycie i nadmiernych, w szczególności wniosków o powtarzalnym charakterze składanych przez tę samą osobę, której dane dotyczą, kontroler danych, po konsultacji z IOD, może odmówić podjęcia decyzji w sprawie wniosku zgodnie z art. 14 rozporządzenia. Wnioskodawca jest odpowiednio informowany.

### Artykuł 17

#### Zwolnienia i ograniczenia

Ograniczenia zgodnie z zasadami wewnętrznymi przyjętymi na podstawie art. 25 rozporządzenia oraz wyjątki ustanowione w art. 15–19 i art. 21–24 rozporządzenia mają zastosowanie dopiero po konsultacji z IOD.

#### SEKCJA 6

#### PRZEPISY KOŃCOWE

### Artykuł 18

#### Powiadomienie o niniejszej decyzji

1. Zgodnie z art. 41 rozporządzenia o niniejszej decyzji informuje się EIOD.
2. Niniejszą decyzję udostępnia się personelowi ESDZ za pomocą odpowiednich środków, w szczególności poprzez opublikowanie jej na wewnętrznej stronie internetowej ESDZ.

### Artykuł 19

#### Uchylenie

Niniejszym uchyla się decyzję PROC HR(2011) 016 Wysokiego Przedstawiciela Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa z dnia 8 grudnia 2011 r. w sprawie przepisów dotyczących ochrony danych.

<sup>(5)</sup> Decyzja Wysokiego Przedstawiciela Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa w sprawie wewnętrznych zasad dotyczących ograniczenia pewnych praw osób, których dotyczą dane, w związku z przetwarzaniem danych osobowych w ramach funkcjonowania Europejskiej Służby Działań Zewnętrznych (ADMIN(2019) 10).



*Artykuł 20*

**Wejście w życie**

Niniejsza decyzja wchodzi w życie następnego dnia po jej przyjęciu.

Sporządzono w Brukseli dnia 1 października 2019 r.

Federica MOGHERINI  
*Wysoki Przedstawiciel*

---