

MATERIAŁ DYDAKTYCZNY

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/679

z dnia **27 kwietnia 2016 r.** w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Tekst mający znaczenie dla EOG)

PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ, uwzględniając
PRZYJMUJĄ NINIEJSZE ROZPORZĄDZENIE:

Niniejsze rozporządzenie ma zastosowanie od dnia 25 maja 2018 r.



ROZDZIAŁ I Przepisy ogólne

Artykuł 1 Przedmiot i cele

1. W niniejszym rozporządzeniu ustanowione zostają przepisy o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych oraz przepisy o swobodnym przepływie danych osobowych.
2. Niniejsze rozporządzenie chroni podstawowe prawa i wolności osób fizycznych, w szczególności ich prawo do ochrony danych osobowych.
3. Nie ogranicza się ani nie zakazuje swobodnego przepływu danych osobowych w Unii z powodów odnoszących się do ochrony osób fizycznych w związku z przetwarzaniem danych osobowych.

Artykuł 2 Materiałny zakres stosowania

1. Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany oraz do przetwarzania w sposób inny niż zautomatyzowany danych osobowych stanowiących część zbioru danych lub mających stanowić część zbioru danych.
2. Niniejsze rozporządzenie **nie ma zastosowania** do przetwarzania danych osobowych:
 - a) w ramach działalności nieobjętej zakresem prawa Unii;
 - b) przez państwa członkowskie w ramach wykonywania działań wchodzących w zakres tytułu V rozdział 2 TUE;
 - c) przez osobę fizyczną w ramach czynności o czysto osobistym lub domowym charakterze;
 - d) przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom.
3. Do przetwarzania danych osobowych przez instytucje, organy i jednostki organizacyjne Unii zastosowanie ma rozporządzenie (WE) nr 45/2001. Rozporządzenie (WE) nr 45/2001 oraz inne unijne akty prawne mające zastosowanie do takiego przetwarzania danych osobowych zostają dostosowane do zasad i przepisów niniejszego rozporządzenia zgodnie z art. 98.
4. Niniejsze rozporządzenie pozostaje bez uszczerbku dla stosowania dyrektywy 2000/31/WE, w szczególności dla zasad odpowiedzialności usługodawców będących pośrednikami, o których to zasadach mowa w art. 12–15 tej dyrektywy.

Artykuł 3 Terytorialny zakres stosowania

1. Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych w związku z działalnością prowadzoną przez jednostkę organizacyjną administratora lub podmiotu przetwarzającego w Unii, niezależnie od tego, czy przetwarzanie odbywa się w Unii. 4.5.2016 L 119/32 Dziennik Urzędowy Unii Europejskiej PL
2. Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych osób, których dane dotyczą, przebywających w Unii przez administratora lub podmiot przetwarzający niemających jednostek organizacyjnych w Unii, jeżeli czynności przetwarzania wiążą się z: a) oferowaniem

towarów lub usług takim osobom, których dane dotyczą, w Unii – niezależnie od tego, czy wymaga się od tych osób zapłaty; lub b) monitorowaniem ich zachowania, o ile do zachowania tego dochodzi w Unii.

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

Artykuł 4 Definicje [UODO art.6]

Na użytek niniejszego rozporządzenia:

1) **„dane osobowe”** oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

2) **„przetwarzanie”** oznacza **!!!! operację lub zestaw operacji wykonywanych** na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak **zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;**

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

4) **„profilowanie”** oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;

5) **„pseudonimizacja”** oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej; **pseudonimizacji** (z gr. *pseudōnymos* – fałszywie nazwany), czyli użyciu w miejsce rzeczywistej nazwy procesu bądź osoby, nazwy przybranej tj. pseudonimu¹¹⁰.

6) **„zbiór danych”** oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;

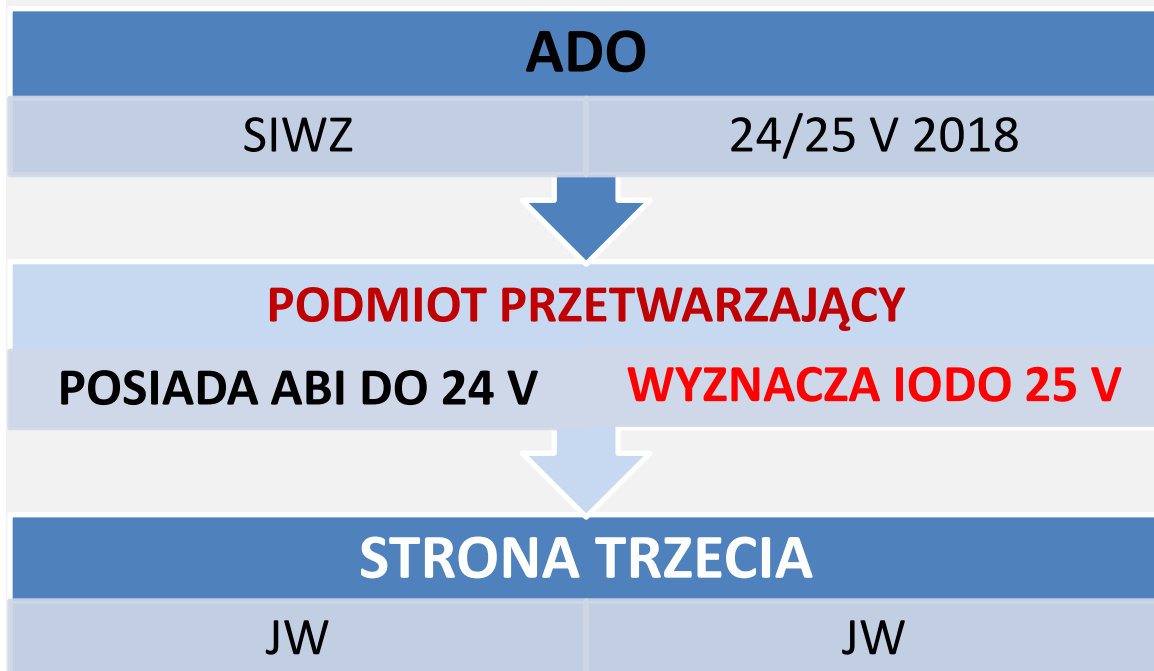
7) **„administrator”** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego,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

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

9) **„odbiorca”** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe **[ZUS WNIOSEK]**, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane 4.5.2016 L 119/33 Dziennik Urzędowy Unii Europejskiej PL osobowe w ramach konkretnego postępowania **[POLICJA]** zgodnie z prawem Unii lub prawem państwa członkowskiego, **nie są jednak uznawane za odbiorców;** przetwarzanie tych

danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania;

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



11) „zgoda” osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych; [UODO art. 7]

12) „naruszenie ochrony danych osobowych” oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;

13) „dane genetyczne” oznaczają dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej; [UODO art. 27 ust 1]

14) „dane biometryczne” oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne; [jw.]

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

16) „główna jednostka organizacyjna” oznacza:

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

to za główną jednostkę organizacyjną uznaje się jednostkę organizacyjną, w której zapadają takie decyzje;

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

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

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

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

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

21) „organ nadzorczy” [Prezes Urzędu Ochrony Danych Osobowych] oznacza niezależny organ publiczny ustanowiony przez państwo członkowskie zgodnie z art. 51; 4.5.2016 L 119/34 Dziennik Urzędowy Unii Europejskiej PL [UODO art. 8 – 22a]

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

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

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

c) wniesiono do niego skargę;

23) „transgraniczne przetwarzanie” oznacza:

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

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

24) „mający znaczenie dla sprawy i uzasadniony sprzeciw” oznacza sprzeciw wobec projektu decyzji dotyczącej tego, czy doszło do naruszenia niniejszego rozporządzenia lub czy planowane działanie wobec administratora lub podmiotu przetwarzającego jest zgodne z niniejszym rozporządzeniem,



który to sprzeciw musi jasno wskazywać wagę wynikającego z projektu decyzji ryzyka naruszenia podstawowych praw lub wolności osób, których dane dotyczą, oraz gdy ma to zastosowanie – wagę ryzyka zakłócenia swobodnego przepływu danych osobowych w Unii;

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

26) „organizacja międzynarodowa” oznacza organizację i organy jej podlegające działające na podstawie prawa międzynarodowego publicznego lub inny organ powołany w drodze umowy między co najmniej dwoma państwami lub na podstawie takiej umowy.

ROZDZIAŁ II Zasady

Art. 23
UODO

Artykuł 5 Zasady dotyczące przetwarzania danych osobowych

PRZESŁANKI PRZETWARZANIA WG KRYTERIÓW

5

1. Dane osobowe muszą być:

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

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

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

d) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („**prawidłowość**”); 4.5.2016 L 119/35 Dziennik Urzędowy Unii Europejskiej PL (1) Dyrektywa (UE) 2015/1535 Parlamentu Europejskiego i Rady z dnia 9 września 2015 r. ustanawiająca procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego (Dz.U. L 241 z 17.9.2015, s. 1).

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

f) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym **!!!! ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem**

oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub **organizacyjnych** („integralność i poufność”).

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

**Art. 23
UODO**

Artykuł 6 **Zgodność przetwarzania z prawem** [ART. 82]

6

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

- a) osoba, której dane dotyczą **wyraziła zgodę na przetwarzanie** swoich danych osobowych w jednym lub większej liczbie określonych celów;
- b) przetwarzanie jest **niezbędne do wykonania umowy**, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
- c) przetwarzanie jest niezbędne do **wypełnienia obowiązku prawnego** ciążącego na administratorze;
- d) przetwarzanie jest niezbędne do **ochrony żywotnych interesów** osoby, której dane dotyczą, lub innej osoby fizycznej;
- e) przetwarzanie jest niezbędne do wykonania **zadania realizowanego w interesie publicznym** lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
- f) przetwarzanie jest **niezbędne do celów wynikających z prawnie uzasadnionych** interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem. Akapit pierwszy lit. f) **nie ma zastosowania do przetwarzania, którego dokonują organy publiczne w ramach realizacji swoich zadań.**

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

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

- a) w prawie Unii; lub
- b) w prawie państwa członkowskiego, któremu podlega administrator. Cel przetwarzania musi być określony w tej podstawie prawnej lub, w przypadku przetwarzania, o którym mowa w ust. 1 lit. e) – musi być ono niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi. Podstawa prawna może zawierać przepisy szczegółowe dostosowujące stosowanie przepisów niniejszego rozporządzenia, w tym: ogólne warunki zgodności z prawem przetwarzania przez administratora; rodzaj danych podlegających

przetwarzaniu; osoby, których dane dotyczą; podmioty, którym można ujawnić dane osobowe; cele, w których można je ujawnić; **ograniczenia celu; okresy przechowywania; oraz operacje i procedury przetwarzania, w tym środki zapewniające zgodność z prawem i rzetelność przetwarzania**, 4.5.2016 L 119/36 Dziennik Urzędowy Unii Europejskiej PL w tym w innych szczególnych sytuacjach związanych z przetwarzaniem, o których mowa w rozdziale IX. Prawo Unii lub prawo państwa członkowskiego muszą służyć realizacji celu leżącego w interesie publicznym, oraz być proporcjonalne do wyznaczonego, prawnie uzasadnionego celu.

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

- a) wszelkie związki między celami, w których zebrano dane osobowe, a celami zamierzonego dalszego przetwarzania;
- b) kontekst, w którym zebrano dane osobowe, w szczególności relację między osobami, których dane dotyczą, a administratorem;
- c) **charakter danych osobowych, w szczególności czy przetwarzane są szczególne kategorie danych osobowych** zgodnie z art. 9 lub dane osobowe dotyczące wyroków skazujących i naruszeń prawa zgodnie z art. 10;
- d) ewentualne konsekwencje zamierzonego dalszego przetwarzania dla osób, których dane dotyczą;
- e) istnienie odpowiednich zabezpieczeń, w tym ewentualnie szyfrowania lub pseudonimizacji.

Artykuł 7 Warunki wyrażenia zgody [ART. 82]

7

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. /sposób i forma??? - udowodnienia nie jest jasna/

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

3. Osoba, której dane dotyczą, **ma prawo w dowolnym momencie wycofać zgodę**. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie

!!!zgody przed jej wycofaniem. **Osoba, której dane dotyczą, jest o tym informowana, zanim wyrazi zgodę.** Wycofanie zgody musi być równie łatwe jak jej wyrażenie.

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

Artykuł 8 Warunki wyrażenia zgody przez dziecko w przypadku usług społeczeństwa informacyjnego

1. Jeżeli zastosowanie ma art. 6 ust. 1 lit. a), w przypadku usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku, zgodne z prawem jest przetwarzanie danych osobowych dziecka, które ukończyło 16 lat. **Jeżeli dziecko nie ukończyło 16 lat, takie przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy zgodę wyraziła lub zaaprobowała ją osoba sprawująca władzę rodzicielską lub opiekę nad dzieckiem oraz wyłącznie w zakresie wyrażonej zgody.** Państwa członkowskie mogą przewidzieć w swoim prawie niższą granicę wiekową, która musi wynosić co najmniej 13 lat. 4.5.2016 L 119/37 Dziennik Urzędowy Unii Europejskiej PL

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

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

**Art. 27 /
1 UODO**

Artykuł 9 Przetwarzanie szczególnych kategorii danych osobowych WRAŻLIWE

8

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

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

**Art. 27 / 2
UODO**

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

b) przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, **zabezpieczenia społecznego i ochrony socjalnej**, o ile jest to dozwolone prawem Unii lub **prawem państwa członkowskiego**, lub

porozumieniem zbiorowym na mocy prawa państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą;
c) przetwarzanie jest niezbędne **do ochrony żywotnych interesów** osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody;

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

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

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

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

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

i) przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa Unii lub prawa państwa członkowskiego, które przewidują odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową; 4.5.2016 L 119/38 Dziennik Urzędowy Unii Europejskiej PL

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

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

również podlegającą obowiązkowi zachowania tajemnicy zawodowej na mocy prawa Unii lub prawa państwa członkowskiego, lub przepisów ustanowionych przez właściwe organy krajowe.

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

Artykuł 10

Przetwarzanie danych osobowych dotyczących wyroków skazujących i naruszeń prawa

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

Artykuł 11 Przetwarzanie niewymagające identyfikacji

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

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

ROZDZIAŁ III Prawa osoby, której dane dotyczą

Sekcja 1 Przejrzystość oraz tryb korzystania z praw

Artykuł 12

WZMOCNIENIE PRAW OSOBY

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

1. Administrator podejmuje odpowiednie środki, aby w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem – w szczególności gdy informacje są kierowane do dziecka – udzielić osobie, której dane dotyczą, wszelkich informacji, o których mowa w art. 13 i 14, **oraz prowadzić z nią wszelką**

komunikację na mocy art. 15–22 i 34 w sprawie przetwarzania. Informacji udziela się na piśmie lub w inny sposób, w tym w stosownych przypadkach – elektronicznie. **Jeżeli osoba, której dane dotyczą, tego zażąda, informacji można udzielić ustnie, o ile innymi sposobami potwierdzi się tożsamość** osoby, której dane dotyczą. 4.5.2016 L 119/39 Dziennik Urzędowy Unii Europejskiej PL

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

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

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

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

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

b) odmówić podjęcia działań w związku z żądaniem. Obowiązek wykazania, że żądanie ma ewidentnie nieuzasadniony lub nadmierny charakter, spoczywa na administratorze.

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

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

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

Sekcja 2 Informacje i dostęp do danych osobowych

[obowiązek informacyjny] o IODO

Artykuł 13 Informacje podawane w przypadku zbierania danych od osoby, której dane dotyczą

1. Jeżeli dane osobowe osoby, której dane dotyczą, zbierane są od tej osoby, administrator podczas pozyskiwania danych osobowych podaje jej **/w j. polskim - łącznie/** wszystkie następujące informacje:

10

BIP

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

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



c) cele przetwarzania danych osobowych, oraz podstawę prawną przetwarzania; 4.5.2016 L 119/40 Dziennik Urzędowy Unii Europejskiej PL

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

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

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

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

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

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



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

d) informacje o prawie wniesienia skargi do organu nadzorczego;

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

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

3. Jeżeli administrator planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym dane osobowe zostały zebrane, przed takim dalszym przetwarzaniem informuje on osobę, której dane dotyczą, o tym innym celu oraz udziela jej wszelkich innych stosownych informacji, o których mowa w ust. 2. 4. Ust. 1, 2 i 3 nie mają zastosowania, gdy – i w zakresie, w jakim – osoba, której dane dotyczą, dysponuje już tymi informacjami.

Artykuł 14 Informacje podawane w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą

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

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

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

11
IODO

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

d) kategorie odnośnych danych osobowych;

e) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją; 4.5.2016 L 119/41 Dziennik Urzędowy Unii Europejskiej PL

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

2. Poza informacjami, o których mowa w ust. 1, administrator podaje osobie, której dane dotyczą, następujące informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania wobec osoby, której dane dotyczą: **a) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;** b) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f) – prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią; c) informacje o prawie do **żądania od administratora dostępu** do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania oraz o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych; d) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem; e) informacje o prawie

wniesienia skargi do organu nadzorczego; f) źródło pochodzenia danych osobowych, a gdy ma to zastosowanie – czy pochodzą one ze źródeł publicznie dostępnych; g) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

3. Informacje, o których mowa w ust. 1 i 2, administrator podaje: a) w rozsądnym terminie po pozyskaniu danych osobowych – najpóźniej w ciągu miesiąca – mając na uwadze konkretne okoliczności przetwarzania danych osobowych; b) jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą – najpóźniej przy pierwszej takiej komunikacji z osobą, której dane dotyczą; lub c) jeżeli planuje się ujawnić dane osobowe innemu odbiorcy – najpóźniej przy ich pierwszym ujawnieniu.

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

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

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

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

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

d) dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianym w prawie Unii lub w prawie państwa członkowskiego, w tym ustawowym obowiązkiem zachowania tajemnicy. 4.5.2016 L 119/42 Dziennik Urzędowy Unii Europejskiej PL

Artykuł 15 Prawo dostępu przysługujące osobie, której dane dotyczą

12

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

a) cele przetwarzania;

b) kategorie odnośnych danych osobowych;

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

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

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

f) informacje o prawie wniesienia skargi do organu nadzorczego;

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

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

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

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

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

Sekcja 3 Sprostowanie i usuwanie danych

13

Artykuł 16 Prawo do sprostowania danych Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe. Z uwzględnieniem celów przetwarzania, osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.

Artykuł 17

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

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

- a) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane; 4.5.2016 L 119/43 Dziennik Urzędowy Unii Europejskiej PL
- b) osoba, której dane dotyczą, **cofnęła zgodę**, na której opiera się przetwarzanie zgodnie z art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a), i nie ma innej podstawy prawnej przetwarzania;
- c) osoba, której dane dotyczą, **wnosi sprzeciw na mocy** art. 21 ust. 1 wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania lub osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 2 wobec przetwarzania;
- d) dane osobowe były przetwarzane niezgodnie z prawem;
- e) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator;
- f) dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego, o których mowa w art. 8 ust. 1.

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

3. Ust. 1 i 2 nie mają zastosowania, w zakresie w jakim przetwarzanie jest niezbędne: a) do korzystania z prawa do wolności wypowiedzi i informacji; b) do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi; c) z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego zgodnie z art. 9 ust. 2 lit. h) oraz i) i art. 9 ust. 3; d) do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1, o ile prawdopodobne jest, że prawo, o którym mowa w ust. 1, uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania; lub e) do ustalenia, dochodzenia lub obrony roszczeń.

Artykuł 18 **Prawo do ograniczenia przetwarzania**

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

- a) osoba, której dane dotyczą, **kwestionuje** prawidłowość danych osobowych – **na okres pozwalający administratorowi sprawdzić prawidłowość** tych danych;
- b) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;
- c) **administrator nie potrzebuje już danych osobowych do celów przetwarzania**, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;

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

2. Jeżeli na mocy ust. 1 przetwarzanie zostało ograniczone, takie dane osobowe można przetwarzać, z wyjątkiem przechowywania, wyłącznie za zgodą osoby, której dane dotyczą, lub w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii lub państwa członkowskiego. 4.5.2016 L 119/44 Dziennik Urzędowy Unii Europejskiej PL 3. Przed uchYLENIEM ograniczenia przetwarzania administrator informuje o tym osobę, której dane dotyczą, która żądała ograniczenia na mocy ust. 1.

Artykuł 19 Obowiązek powiadomienia o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania

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

Artykuł 20 Prawo do przenoszenia danych

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

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

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

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

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

Sekcja 4 Prawo do sprzeciwu oraz zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach

Artykuł 21 Prawo do sprzeciwu

1. Osoba, której dane dotyczą, **ma prawo w dowolnym momencie wnieść sprzeciw** – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych opartego na art. 6 ust. 1 lit. e) lub f), w tym profilowania na podstawie tych przepisów.

Administratorowi **nie wolno już przetwarzać** tych danych osobowych, chyba że wykaże on istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.

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

3. Jeżeli osoba, której dane dotyczą, wnieśli sprzeciw **wobec przetwarzania do celów marketingu** bezpośredniego, danych osobowych nie wolno już przetwarzać do takich celów. 4.5.2016 L 119/45 Dziennik Urzędowy Unii Europejskiej PL

4. Najpóźniej przy okazji pierwszej komunikacji z osobą, której dane dotyczą, wyraźnie informuje się ją o prawie, o którym mowa w ust. 1 i 2, oraz przedstawia się je jasno i odrębnie od wszelkich innych informacji. 5. W związku z korzystaniem z usług społeczeństwa informacyjnego i bez uszczerbku dla dyrektywy 2002/58/WE osoba, której dane dotyczą, może wykonać prawo do sprzeciwu za pośrednictwem zautomatyzowanych środków wykorzystujących specyfikacje techniczne. 6. Jeżeli dane osobowe są przetwarzane do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, osoba, której dane dotyczą, ma prawo wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.

Artykuł 22 Zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach, w tym profilowanie

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

2. Ust. 1 nie ma zastosowania, jeżeli ta decyzja: a) jest niezbędna do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a administratorem; b) jest dozwolona prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator i które przewiduje właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą; lub c) opiera się na wyraźnej zgodzie osoby, której dane dotyczą.

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

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

Sekcja 5 Ograniczenia

Artykuł 23 Ograniczenia

1. Prawo Unii lub prawo państwa członkowskiego, któremu podlegają administrator danych lub podmiot przetwarzający, może aktem prawnym ograniczyć zakres obowiązków i praw przewidzianych w art. 12–22 i w art. 34, a także w art. 5 – o ile jego przepisy odpowiadają prawom i obowiązkom przewidzianym w art. 12–22 – jeżeli ograniczenie takie nie narusza istoty podstawowych praw i wolności oraz jest w demokratycznym społeczeństwie środkiem niezbędnym i proporcjonalnym, służącym: a) bezpieczeństwu narodowemu; b) obronie; c) bezpieczeństwu publicznemu; 4.5.2016 L 119/46 Dziennik Urzędowy Unii Europejskiej PL d) zapobieganiu przestępczości, prowadzeniu postępowań przygotowawczych, wykrywaniu lub ściganiu czynów zabronionych lub wykonywaniu kar, w tym ochronie przed zagrożeniami dla bezpieczeństwa publicznego i zapobieganiu takim zagrożeniom; e) innym ważnym celom leżącym w ogólnym interesie publicznym Unii lub państwa członkowskiego, w szczególności ważnemu interesowi gospodarczemu lub finansowemu Unii lub państwa członkowskiego, w tym kwestiom pieniężnym, budżetowym i podatkowym, zdrowiu publicznemu i zabezpieczeniu społecznemu; f) ochronie niezależności sądów i postępowania sądowego; g) zapobieganiu naruszeniom zasad etyki w zawodach regulowanych, prowadzeniu postępowań w takich sprawach, ich wykrywaniu oraz ściganiu; h) funkcjom kontrolnym, inspekcyjnym lub regulacyjnym związanym, nawet sporadycznie, ze sprawowaniem władzy publicznej w przypadkach, o których mowa w lit. a) – e) oraz g); i) ochronie osoby, której dane dotyczą, lub praw i wolności innych osób; j) egzekucji roszczeń cywilnoprawnych. 2. W szczególności akt prawny, o którym mowa w ust. 1, musi zawierać szczegółowe przepisy przynajmniej – w stosownym przypadku – o: a) celach przetwarzania lub kategorii przetwarzania; b) kategoriach danych osobowych; c) zakresie wprowadzonych ograniczeń; d) zabezpieczeniach zapobiegających nadużyciom lub niezgodnemu z prawem dostępowi lub przekazywaniu; e) określeniu administratora lub kategorii administratorów; f) okresach przechowywania oraz mających zastosowanie zabezpieczeniach z uwzględnieniem charakteru, zakresu i celów przetwarzania lub kategorii przetwarzania; g) ryzyka naruszenia praw lub wolności osoby, której dane dotyczą; oraz h) prawie osób, której dane dotyczą, do uzyskania informacji o ograniczeniach, o ile nie narusza to celu ograniczenia.

ROZDZIAŁ IV Administrator i podmiot przetwarzający

Sekcja 1 Obowiązki ogólne

Artykuł 24 **Obowiązki administratora**

15

1. Uwzględniając **charakter**, zakres, kontekst i **cele** przetwarzania **oraz ryzyko** naruszenia praw lub wolności osób fizycznych **o różnym prawdopodobieństwie i wadze zagrożeń**, 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 przeglądowi i uaktualniane.

2. Jeżeli jest to proporcjonalne w stosunku do czynności

przetwarzania, środki, o których mowa w ust. 1, obejmują wdrożenie **przez administratora odpowiednich polityk ochrony danych.**

[!!! - POD] - DZISIEJSZA PBI

3. Stosowanie zatwierdzonych kodeksów postępowania, o których mowa w art. 40, lub zatwierdzonego mechanizmu certyfikacji, o którym mowa w art. 42, **może być wykorzystane** jako element dla stwierdzenia przestrzegania przez administratora ciężących na nim obowiązków. 4.5.2016 L 119/47 Dziennik Urzędowy Unii Europejskiej PL

Artykuł 25 Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych

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

15a

2. Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. W szczególności środki te zapewniają, by domyślnie dane osobowe nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych. 3. Wywiązywanie się z obowiązków, o których mowa w ust. 1 i 2 niniejszego artykułu, można wykazać między innymi poprzez wprowadzenie zatwierdzonego mechanizmu certyfikacji określonego w art. 42.

Artykuł 26 Współadministratorzy

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

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

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

Artykuł 27 Przedstawiciele administratorów lub podmiotów przetwarzających niemających jednostki organizacyjnej w Unii

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

2. Obowiązek ustanowiony w ust. 1 niniejszego artykułu nie ma zastosowania w przypadku: a) przetwarzania, które ma charakter sporadyczny, nie obejmuje – na dużą skalę – przetwarzania szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1, ani przetwarzania danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10, i jest mało prawdopodobne, by ze względu na swój charakter, kontekst, zakres i cele powodowało ryzyko naruszenia praw lub wolności osób fizycznych; lub b) organu lub podmiotu publicznego. 4.5.2016 L 119/48 Dziennik Urzędowy Unii Europejskiej PL 3. Przedstawiciel musi mieć siedzibę w państwie członkowskim, w którym przebywają osoby, których dane dotyczą, których dane osobowe są przetwarzane w związku z oferowaniem im towarów lub usług lub których zachowanie jest monitorowane. 4. Przedstawiciel zostaje upoważniony przez administratora lub podmiot przetwarzający, by do celów zapewnienia przestrzegania niniejszego rozporządzenia mogły się do niego zwracać – oprócz lub zamiast do administratora lub podmiotu przetwarzającego – w szczególności organy nadzorcze i osoby, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem. 5. Wyznaczenie przedstawiciela przez administratora lub podmiot przetwarzający pozostaje bez uszczerbku dla postępowań, które mogą zostać wszczęte przeciwko samemu administratorowi lub podmiotowi przetwarzającemu.

Artykuł 28 Podmiot przetwarzający

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

15b

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

3. Przetwarzanie przez podmiot przetwarzający odbywa się na podstawie umowy lub innego instrumentu prawnego /Instrumentem prawnym, poprzez który uzewnętrznia się w sposób najbardziej charakterystyczny władczy charakter działania organów administracji publicznej (możliwość określenia praw lub nałożenia obowiązków na strony postępowania), jest akt administracyjny (decyzja administracyjna, postanowienie)./, **które podlegają prawu Unii lub prawu państwa członkowskiego i wiążą podmiot przetwarzający i administratora, określają przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora**. Ta umowa lub inny instrument prawny stanowią w szczególności, że podmiot przetwarzający:

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

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

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

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

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

f) uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga administratorowi wywiązać się z obowiązków określonych w art. 32–36; g) po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji administratora usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych;

h) udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w niniejszym artykule oraz umożliwia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich. 4.5.2016 L 119/49 Dziennik Urzędowy Unii Europejskiej PL W związku z obowiązkiem określonym w akapicie pierwszym lit. h) podmiot przetwarzający niezwłocznie informuje administratora, jeżeli jego zdaniem wydane mu polecenie stanowi naruszenie niniejszego rozporządzenia lub innych przepisów Unii lub państwa członkowskiego o ochronie danych.

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

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

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

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

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

9. Umowa lub inny akt prawny, o których mowa w art. 3 i 4, mają formę pisemną, w tym formę elektroniczną. 10. Bez uszczerbku dla art. 82, 83 i 84, jeżeli podmiot przetwarzający naruszy niniejsze rozporządzenie przy określaniu celów i sposobów przetwarzania, uznaje się go za administratora w odniesieniu do tego przetwarzania.

Artykuł 29 Przetwarzanie z upoważnienia administratora lub podmiotu przetwarzającego

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

Artykuł 30 Rejestrowanie czynności przetwarzania

16
klasyfikacja

1. Każdy administrator oraz – gdy ma to zastosowanie – przedstawiciel administratora prowadzi rejestr czynności przetwarzania danych osobowych [KLASYFIKACJA PRZEPISÓW, KATEGORIE DANYCH, KATEGORIE ZBIORÓW I KLASYFIKACJA OPERACJI] za które odpowiadają. W rejestrze tym zamieszcza się wszystkie następujące informacje:

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

b) cele przetwarzania;

c) opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych; 4.5.2016 L 119/50 Dziennik Urzędowy Unii Europejskiej PL

d) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione,

w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;

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

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

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

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

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

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

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

d) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1. 3. Rejestry, o których mowa w ust. 1 i 2, mają formę pisemną, w tym formę elektroniczną.

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

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

Artykuł 31 Współpraca z organem nadzorczym Administrator i podmiot przetwarzający oraz – gdy ma to zastosowanie – ich przedstawiciele na żądanie współpracują z organem nadzorczym w ramach wykonywania przez niego swoich zadań.

Sekcja 2 Bezpieczeństwo danych osobowych

Artykuł 32 Bezpieczeństwo przetwarzania

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

a) pseudonimizację i szyfrowanie danych osobowych; 4.5.2016 L 119/51 Dziennik Urzędowy Unii Europejskiej PL

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

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

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

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

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

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

Artykuł 33 Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu

/organizacyjne – techniczne lub utrata/

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

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

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

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

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

c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;

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

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

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

Artykuł 34 Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych

1.Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, **administrator bez zbędnej zwłoki zawiadamia osobę,**

której dane dotyczą, o takim naruszeniu. 4.5.2016 L 119/52 Dziennik Urzędowy Unii Europejskiej PL 2.Zawiadomienie, o którym mowa w ust. 1 niniejszego artykułu, jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki, o których mowa w art. 33 ust. 3 lit. b), c) i d).

3.Zawiadomienie, o którym mowa w ust. 1, nie jest wymagane, w następujących przypadkach: a) administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych; b) administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w ust. 1; c) wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

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

Sekcja 3 **Ocena skutków** dla ochrony danych i uprzednie konsultacje*Artykuł 35* **Ocena skutków dla ochrony danych**

1. Jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym **prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych**, administrator przed rozpoczęciem przetwarzania **dokonuje oceny skutków** planowanych **operacji przetwarzania** dla ochrony danych osobowych. Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę.

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

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

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

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

c) systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.
- CCTV

4. Organ nadzorczy ustanawia i podaje do publicznej wiadomości wykaz rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny skutków dla ochrony danych na mocy ust.

1. Organ nadzorczy przekazuje te wykazy Europejskiej Radzie Ochrony Danych, o której mowa w art. 68.

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

6. Jeżeli wykazy, o których mowa w ust. 4 i 5, obejmują czynności przetwarzania związane z oferowaniem towarów lub usług osobom, których dane dotyczą, lub z monitorowaniem ich zachowania w kilku państwach członkowskich lub mogące znacznie wpłynąć na swobodny przepływ danych osobowych w Unii, przed przyjęciem takich wykazów właściwy organ nadzorczy stosuje mechanizm spójności, o którym mowa w art. 63. 4.5.2016 L 119/53 Dziennik Urzędowy Unii Europejskiej PL

7. Ocena zawiera co najmniej:

- a) systematyczny opis planowanych **operacji przetwarzania** i **celów przetwarzania**, w tym, gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez administratora;
- b) ocenę, czy operacje przetwarzania są **niezbędne oraz proporcjonalne** w stosunku do celów;
- c) ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą, o którym mowa w ust. 1; oraz
- d) środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie niniejszego rozporządzenia, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy.

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

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

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

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

Artykuł 36 Upřednie konsultacje

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

2. Jeżeli organ nadzorczy jest zdania, że zamierzone przetwarzanie, o którym mowa w ust. 1, stanowiłoby naruszenie niniejszego rozporządzenia – w szczególności gdy administrator niedostatecznie zidentyfikował lub zminimalizował ryzyko – organ nadzorczy w terminie **do ośmiu tygodni od wpłynięcia wniosku** o konsultację udziela administratorowi, a gdy ma to zastosowanie także podmiotowi przetwarzającemu pisemnego zalecenia i może skorzystać z dowolnego ze swoich uprawnień, o których mowa w art. 58.

Okres ten można przedłużyć o sześć tygodni ze względu na złożony charakter zamierzonego przetwarzania. Organ nadzorczy informuje administratora, a gdy ma to zastosowanie także podmiot przetwarzający, o takim przedłużeniu w terminie miesiąca od wpłynięcia wniosku o konsultację, z podaniem przyczyn tego opóźnienia. Bieg tych terminów można zawiesić, do czasu aż organ nadzorczy uzyska wszelkie informacje, których zażądał do celów konsultacji.

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

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

b) cele i sposoby zamierzonego przetwarzania;

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

d) gdy ma to zastosowanie – dane kontaktowe inspektora ochrony danych; 4.5.2016 L 119/54 Dziennik Urzędowy Unii Europejskiej PL

e) ocenę skutków dla ochrony danych, o której mowa w art. 35; oraz f) wszelkie inne informacje, których żąda organ nadzorczy. 4. Państwa członkowskie konsultują się z organem nadzorczym, przygotowując projekt aktu prawnego przyjmowanego przez parlament narodowy lub aktu wykonawczego opartego na takim akcie prawnym, jeżeli projekt dotyczy przetwarzania.

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

Sekcja 4 Inspektor ochrony danych

18

Artykuł 37 Wyznaczenie inspektora ochrony danych



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

a) przetwarzania dokonują organ lub **podmiot publiczny** [JST, OPS, SZKOŁY, PRZEDSZKOLA, BIBLIOTEKI], z wyjątkiem sądów **w zakresie sprawowania** przez nie wymiaru sprawiedliwości;

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

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

/OCENA SKUTKÓW DZIAŁANIA ADO - ABI/

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

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

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

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

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

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

BIP

Artykuł 38 Status inspektora ochrony danych

19

1. **Administrator oraz podmiot przetwarzający zapewniają, by inspektor ochrony danych był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych.** 4.5.2016 L 119/55 Dziennik Urzędowy Unii Europejskiej PL

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

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

administratora lub podmiotu przetwarzającego. STATUT / SCHEMAT ORGANIZACYJNY DO UZUPEŁNIENIA

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

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

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

Artykuł 39 Zadania inspektora ochrony danych

1. Inspektor ochrony danych **ma następujące zadania:**

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

20

b) monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych **oraz polityk administratora** lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, **działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach** przetwarzania oraz powiązane z **tym audyty¹**;



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

d) współpraca z organem nadzorczym;

e) **pełnienie funkcji punktu kontaktowego** dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o

¹ Audyt – ocena danej osoby, organizacji, systemu, procesu, projektu lub produktu. Audyt jest przeprowadzany w celu upewnienia się co do prawdziwości i rzetelności informacji, a także oceny systemu kontroli wewnętrznej. Celem audytu jest wyrażenie opinii na temat osoby / organizacji / systemu itd. w ramach oceny w oparciu o przeprowadzone testy. Ze względów praktycznych, celem audytu jest dostarczenie tylko racjonalnego zapewnienia, o braku istotnych błędów, dlatego w audycie stosowane są często statystyczne metody doboru próby do badania. Audyt polega na ocenie przez kompetentny i niezależny zespół audytujący czy dany przedmiot audytu spełnia wymagania. Zespół audytujący składa się z jednego lub więcej audytorów. Celem audytu może być weryfikacja, czy cel wyznaczony przez organizację audytowaną został osiągnięty lub czy jej działania są zgodne z zaakceptowanymi standardami, statusem czy praktykami. Audyt ocenia także procedury kontrolne celem stwierdzenia, czy przedmiot audytu także w przyszłości będzie odpowiadał uzgodnionym do stosowania wymaganiom. Oprócz oceny wskazuje także zalecenia zmian w procedurach, w tym sprawdzających oraz w politykach.

których mowa w art. 36, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

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

Sekcja 5 Kodeksy postępowania i certyfikacja

Artykuł 40 Kodeksy postępowania – JST NIE SĄ WYMAGANE

[.....]

Artykuł 42 Certyfikacja

1. Państwa członkowskie, organy nadzorcze, Europejska Rada Ochrony Danych oraz Komisja zachęcają – w szczególności na szczeblu Unii – do ustanawiania mechanizmów **certyfikacji oraz znaków jakości i oznaczeń w zakresie ochrony danych osobowych mających świadczyć o zgodności z niniejszym rozporządzeniem operacji przetwarzania** prowadzonych przez administratorów i podmioty przetwarzające. Przy tym uwzględnia się szczególne potrzeby mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw. 4.5.2016 L 119/58 Dziennik Urzędowy Unii Europejskiej PL

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

[.....]

ROZDZIAŁ VIII Środki ochrony prawnej, odpowiedzialność i sankcje

Artykuł 77 **Prawo do wniesienia skargi do organu nadzorczego 1. Bez uszczerbku dla innych administracyjnych lub środków ochrony prawnej przed sądem każda osoba, której dane dotyczą, ma prawo wnieść skargę do organu nadzorczego, w szczególności w państwie członkowskim swojego zwykłego pobytu, swojego miejsca pracy lub miejsca popełnienia domniemanego naruszenia, jeżeli sądzi, że przetwarzanie danych osobowych jej dotyczące narusza niniejsze rozporządzenie.**

2. Organ nadzorczy, do którego wniesiono skargę, informuje skarżącego o postępach i efektach rozpatrywania skargi, w tym o możliwości skorzystania z sądowego środka ochrony prawnej na mocy art. 78.

Artykuł 78 Prawo do skutecznego środka ochrony prawnej przed sądem przeciwko organowi nadzorczemu 1.Bez uszczerbku dla innych administracyjnych lub pozasądowych środków ochrony prawnej każda osoba fizyczna lub prawna ma prawo do skutecznego środka ochrony prawnej przed sądem przeciwko prawnie wiążącej decyzji organu nadzorczego jej dotyczącej. 2.Bez uszczerbku dla innych administracyjnych lub pozasądowych środków ochrony prawnej każda osoba, której dane dotyczą, ma prawo do skutecznego środka ochrony prawnej przed sądem, jeżeli organ nadzorczy właściwy zgodnie z art. 55 i 56 nie rozpatrzył skargi lub nie poinformował osoby, której dane dotyczą, w terminie trzech miesięcy o postępach lub efektach rozpatrywania skargi wniesionej zgodnie z art. 77. 3.Postępowanie przeciwko organowi nadzorczemu zostaje wszczęte przed sądem państwa członkowskiego, w którym organ nadzorczy ma siedzibę. 4.Jeżeli postępowanie zostało wszczęte przeciwko decyzji organu nadzorczego, którą poprzedziła opinia lub decyzja Europejskiej Rady Ochrony Danych w ramach mechanizmu spójności, organ nadzorczy przekazuje sądowi tę opinię lub decyzję.

[.....]

Artykuł 82 Prawo do odszkodowania i odpowiedzialność

1.Każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia niniejszego rozporządzenia, ma prawo uzyskać od administratora lub podmiotu przetwarzającego odszkodowanie za poniesioną szkodę.

2.Każdy administrator uczestniczący w przetwarzaniu odpowiada za szkody spowodowane przetwarzaniem naruszającym niniejsze rozporządzenie. Podmiot przetwarzający odpowiada za szkody spowodowane przetwarzaniem wyłącznie, gdy nie dopełnił obowiązków, które niniejsze rozporządzenie nakłada bezpośrednio na podmioty przetwarzające, lub gdy działał poza zgodnymi z prawem instrukcjami administratora lub wbrew tym instrukcjom.

3.Administrator lub podmiot przetwarzający zostają zwolnieni z odpowiedzialności wynikającej z ust. 2, jeżeli udowodnią, że w żaden sposób nie ponoszą winy za zdarzenie, które doprowadziło do powstania szkody.

4.Jeżeli w tym samym przetwarzaniu uczestniczy więcej niż jeden administrator lub podmiot przetwarzający lub uczestniczy w nim zarówno administrator jak i podmiot przetwarzający i zgodnie z ust. 2 i 3 odpowiadają za szkodę spowodowaną przetwarzaniem, ponoszą oni odpowiedzialność solidarną za całą szkodę, tak by zapewnić osobie, której dane dotyczą, rzeczywiste uzyskanie odszkodowania.

5.Administrator lub podmiot przetwarzający, który zgodnie z ust. 4 zapłacił odszkodowanie za całą wyrządzoną szkodę, ma prawo żądania od pozostałych administratorów lub podmiotów przetwarzających, którzy uczestniczyli w tym samym przetwarzaniu, zwrotu części odszkodowania odpowiadającej części szkody, za którą ponoszą odpowiedzialność, zgodnie z warunkami określonymi w ust. 2. 4.5.2016 L 119/81 Dziennik Urzędowy Unii Europejskiej PL 6.Postępowanie sądowe

dotyczące odszkodowania jest wszczynane przed sądem właściwym na mocy prawa państwa członkowskiego, o którym mowa w art. 79 ust. 2.

Artykuł 83 Ogólne warunki nakładania administracyjnych kar pieniężnych

1. Każdy organ nadzorczy zapewnia, by stosowane na mocy niniejszego artykułu za naruszenia niniejszego rozporządzenia administracyjne kary pieniężne, o których mowa w ust. 4, 5 i 6, były w każdym indywidualnym przypadku skuteczne, proporcjonalne i odstraszające.

2. Administracyjne kary pieniężne nakłada się, zależnie od okoliczności każdego indywidualnego przypadku, oprócz lub zamiast środków, o których mowa w art. 58 ust. 2 lit. a)–h) oraz j). Decydując, czy nałożyć administracyjną karę pieniężną, oraz ustalając jej wysokość, zwraca się w każdym indywidualnym przypadku należyta uwagę na:

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

b) umyślny lub nieumyślny charakter naruszenia;

c) działania podjęte przez administratora lub podmiot przetwarzający w celu zminimalizowania szkody poniesionej przez osoby, których dane dotyczą;

d) stopień odpowiedzialności administratora lub podmiotu przetwarzającego z uwzględnieniem środków technicznych i organizacyjnych wdrożonych przez nich na mocy art. 25 i 32;

e) wszelkie stosowne wcześniejsze naruszenia ze strony administratora lub podmiotu przetwarzającego;

f) stopień współpracy z organem nadzorczym w celu usunięcia naruszenia oraz złagodzenia jego ewentualnych negatywnych skutków;

g) kategorie danych osobowych, których dotyczyło naruszenie; h) sposób, w jaki organ nadzorczy dowiedział się o naruszeniu, w szczególności, czy i w jakim zakresie administrator lub podmiot przetwarzający zgłosili naruszenie; i) jeżeli wobec administratora lub podmiotu przetwarzającego, których sprawa dotyczy, zostały wcześniej zastosowane w tej samej sprawie środki, o których mowa w art. 58 ust. 2 – przestrzeganie tych środków; j) stosowanie zatwierdzonych kodeksów postępowania na mocy art. 40 lub zatwierdzonych mechanizmów certyfikacji na mocy art. 42; oraz k) wszelkie inne obciążające lub łagodzące czynniki mające zastosowanie do okoliczności sprawy, takie jak osiągnięte bezpośrednio lub pośrednio w związku z naruszeniem korzyści finansowe lub uniknięte straty.

3. Jeżeli administrator lub podmiot przetwarzający narusza umyślnie lub nieumyślnie w ramach tych samych lub powiązanych operacji przetwarzania kilka przepisów niniejszego rozporządzenia, całkowita wysokość administracyjnej kary pieniężnej nie przekracza wysokości kary za najpoważniejsze naruszenie.

4. Naruszenia przepisów dotyczących następujących kwestii podlegają zgodnie z ust. 2 administracyjnej karze pieniężnej w wysokości do 10 000 000 EUR, a w przypadku przedsiębiorstwa – w wysokości do 2 % jego

całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa:

a) obowiązków administratora i podmiotu przetwarzającego, o których mowa w art. 8, 11, 25 –39 oraz 42 i 43; b) obowiązków podmiotu certyfikującego, o których mowa w art. 42 oraz 43;

c) obowiązków podmiotu monitorującego, o których mowa w art. 41 ust.

4; 4.5.2016 L 119/82 Dziennik Urzędowy Unii Europejskiej PL

5.Naruszenia przepisów dotyczących następujących kwestii podlegają zgodnie z ust. 2 administracyjnej karze pieniężnej w wysokości do 20 000 000 EUR, a w przypadku przedsiębiorstwa – w wysokości do 4 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa:

a) podstawowych zasad przetwarzania, w tym warunków zgody, o których to zasadach i warunkach mowa w art. 5, 6, 7 oraz 9; b) praw osób, których dane dotyczą, o których mowa w art. 12–22; c) przekazywania danych osobowych odbiorcy w państwie trzecim lub organizacji międzynarodowej, o którym to przekazywaniu mowa w art. 44–49; d) wszelkich obowiązków wynikających z prawa państwa członkowskiego przyjętego na podstawie rozdziału IX; e) nieprzestrzegania nakazu, tymczasowego lub ostatecznego ograniczenia przetwarzania lub zawieszenia przepływu danych orzeczonego przez organ nadzorczy na podstawie art. 58 ust. 2 lub niezapewnienia dostępu skutkującego naruszeniem art. 58 ust. 1.

6.Nieprzestrzeganie nakazu orzeczonego przez organ nadzorczy na podstawie art. 58 ust. 2 podlega na mocy ust. 2 niniejszego artykułu administracyjnej karze pieniężnej w wysokości do 20 000 000 EUR, a w przypadku przedsiębiorstwa – w wysokości do 4 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa.

7.Bez uszczerbku dla uprawnień naprawczych organu nadzorczego, o których mowa w ust. 58 ust. 2, każde państwo członkowskie może określić, czy i w jakim zakresie administracyjne kary pieniężne można nakładać na organy i podmioty publiczne ustanowione w tym państwie członkowskim.

8.Wykonywanie przez organ nadzorczy uprawnień powierzonych mu na mocy niniejszego artykułu podlega odpowiednim zabezpieczeniom proceduralnym zgodnie z prawem Unii i prawem państwa członkowskiego, obejmującym prawo do skutecznego sądowego środka ochrony prawnej i rzetelnego procesu.

9.Jeżeli ustrój prawny państwa członkowskiego nie przewiduje administracyjnych kar pieniężnych, niniejszy artykuł można stosować w ten sposób, że o zastosowanie kary pieniężnej wnosi właściwy organ nadzorczy, a nakłada ją właściwy sąd krajowy, o ile zapewniona zostaje skuteczność tych rozwiązań prawnych i równoważność ich skutku względem administracyjnej kary pieniężnej nakładanej przez organ nadzorczy. Nakładane kary pieniężne muszą być w każdym przypadku skuteczne, proporcjonalne i odstrasżające. W terminie określonym w art. 91 ust. 2 takie państwa członkowskie zawiadamiają Komisję o przepisach swojego prawa, które przyjęły zgodnie z niniejszym ustępem do dnia 25 maja 2018 r., a następnie niezwłocznie o wszelkich późniejszych aktach zmieniających lub zmianach mających wpływ na te przepisy.

Artykuł 84 Sankcje 1.Państwa członkowskie przyjmują przepisy określające inne sankcje za naruszenia niniejszego rozporządzenia, w szczególności za naruszenia niepodlegające

administracyjnym karom pieniężnym na mocy art. 83, oraz podejmują wszelkie środki niezbędne do ich wykonania. Sankcje te muszą być skuteczne, proporcjonalne i odstraszające.

2. Do dnia 25 maja 2018 r. każde państwo członkowskie zawiadamia Komisję o swoich przepisach przyjętych zgodnie z ust. 1, a następnie niezwłocznie o każdej późniejszej ich zmianie.

[.....]

Artykuł 99 Wejście w życie i stosowanie

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

2. Niniejsze rozporządzenie ma zastosowanie od **dnia 25 maja 2018 r.** 4.5.2016 L 119/87 Dziennik Urzędowy Unii Europejskiej PL Niniejsze rozporządzenie wiąże w całości i jest bezpośrednio stosowane we wszystkich państwach członkowskich.

Sporządzono w Brukseli dnia 27 kwietnia 2016 r.