MAZOWIECKIE CENTRUM POLITYKI SPOŁECZNEJ

Materiały szkoleniowe

Seminarium: **Ochrona danych osobowych w pomocy społecznej**

Warszawa, 20 listopada 2018 r.

Opracowanie

Monika Wieczorek

20 lat Mazowsze

SPIS TREŚCI

1. Źródła prawa w obszarze ochrony danych osobowych

Od 25 maja 2018 r. obowiązują przepisy Rozporządzenia 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 (*ang. General Data Protection Regulation, dalej jako: ogólne rozporządzenie o ochronie danych, RODO*). To nowe, jednolite dla całego Europejskiego Obszaru Gospodarczego przepisy, które wprowadzają **obowiązek zapewnienia wyższego, niż do tej pory poziomu ochrony danych osobowych.**

25 maja 2018 r. uchylona została ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, zastąpiona ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych (dalej: u.o.d.o.). Zgodnie z art. 1 ust. 1 u.o.d.o. „nową" ustawę stosuje się do ochrony osób fizycznych w związku z przetwarzaniem danych osobowych w zakresie określonym w art. 2 i 3 RODO. **Ustawa uzupełnia postanowienia rozporządzenia i określa (art. 1 ust. 2 u.o.d.o.):**

- podmioty publiczne obowiązane do wyznaczenia inspektora ochrony danych oraz tryb zawiadamiania o jego wyznaczeniu;
- warunki i tryb akredytacji podmiotu uprawnionego do certyfikacji w zakresie ochrony danych osobowych, akredytowanego przez Polskie Centrum Akredytacji, zwanego dalej "podmiotem certyfikującym", podmiotu monitorującego kodeks postępowania oraz certyfikacji;
- tryb zatwierdzenia kodeksu postępowania;
- organ właściwy w sprawie ochrony danych osobowych;
- postępowanie w sprawie naruszenia przepisów o ochronie danych osobowych;
- tryb europejskiej współpracy administracyjnej;
- kontrolę przestrzegania przepisów o ochronie danych osobowych;

- odpowiedzialność cywilną za naruszenie przepisów o ochronie danych osobowych i postępowanie przed sądem;
- odpowiedzialność karną i administracyjne kary pieniężne za naruszenie przepisów o ochronie danych osobowych.

W zakresie ochrony danych osobowych swoje zastosowanie znajdą także przepisy sektorowe, w tym stanowiące podstawy prawne przetwarzania. **Motyw 77** do rozporządzenia stanowi również, że *wskazówki co do tego, jak wdrożyć odpowiednie środki oraz wykazać przestrzeganie prawa przez administratora lub podmiot przetwarzający dane - w szczególności jeżeli chodzi o identyfikowanie ryzyka związanego z przetwarzaniem, o jego ocenę pod kątem źródła, charakteru, prawdopodobieństwa i wagi oraz o najlepsze praktyki pozwalające zminimalizować to ryzyko - mogą być przekazane w szczególności w formie zatwierdzonych kodeksów postępowania, zatwierdzonej certyfikacji, wytycznych Europejskiej Rady Ochrony Danych lub poprzez sugestie inspektora ochrony danych. Europejska Rada Ochrony Danych może wydawać wytyczne także w sprawie operacji przetwarzania, których nie uznaje się za mogące powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, i wskazywać, jakie środki mogą wystarczyć w takich przypadkach dla zaradzenia takiemu ryzyku.*

2. Ochrona danych osobowych w jednostkach pomocy społecznej

Przede wszystkim sięgnąć należy do **najważniejszych definicji występujących w treści rozporządzenia i wpływających na sposób prawidłowej realizacji jego wymogów przez placówki opieki społecznej:**

- **dane osobowe** to wszelkie 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 (art. 4 pkt. 1 RODO),

- **przetwarzanie** to operacja 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 (art. 4 pkt. 2 RODO),

- **administratorem** jest osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; (art. 4 pkt. 7 RODO),

- **podmiotem przetwarzającym** jest osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora (art. 4 pkt. 8 RODO),

- **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 (art. 4 pkt. 11 RODO),

- **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 (art. 4 pkt. 13 RODO),

- **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 (art. 4 pkt. 14 RODO),

- **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 (art. 4 ust. 15 RODO).

W każdym przypadku przetwarzanie danych osobowych musi **odbywać się zgodnie z zasadami** określonymi w art. 5 RODO:

- zgodności z prawem, rzetelności i przejrzystości,
- ograniczenia celu,
- minimalizacji danych,
- prawidłowości,
- ograniczenia przechowywania,
- integralności i poufności,
- rozliczalności.

Szczególne znaczenie ma tu **zasada rozliczalności**. Zgodnie z nią administrator musi być w stanie wykazać przestrzeganie przepisów rozporządzenia. Zasada ta, w połączeniu z podejściem opartym na ryzyku wynikającym z rozporządzenia stanowią novum w obszarze ochrony danych osobowych – rozporządzenie daje administratorowi wskazówki w zakresie ochrony, a nie nakazuje używanie konkretnych narzędzi. Tym samym administrator nie musi już posiadać, jak pod rządami poprzednio obowiązującej ustawy o ochronie danych osobowych, polityki bezpieczeństwa informacji i instrukcji zarządzania systemem informatycznym – może sam określić, w zależności od specyfiki swojej

organizacji, jakie środki będą dla niego wystarczające i odpowiednie do właściwej ochrony danych osobowych.

Jak przyjmuje się w literaturze *powszechnie przyjmuje się, że integralność danych oznacza właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany. Poufność danych to właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom, zaś rozliczalność to właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi* (Bielak-Jomaa Edyta (red.), Lubasz Dominik (red.), RODO. Ogólne rozporządzenie o ochronie danych. Opublikowano: WKP 2018).

Administrator musi zadbać nie tylko o bezpieczeństwo przetwarzanych danych, ale także o prawidłowość tego przetwarzania. W tym celu należy w szczególności **dokonać analizy** istniejących procesów przetwarzania przy uwzględnieniu:
- celu przetwarzania,
- podstawy przetwarzania,
- okresu przechowywania danych,
- odbiorców danych.

Niezbędne stanie się w tym względzie także dokonanie przeglądu istniejących procedur oraz umów i ich odpowiednia modyfikacja. Warto to wspomnieć, że w jednostkach pomocy społecznej do głównych grup, których dane są przetwarzane należą pracownicy jednostki i beneficjenci (interesanci).

Dla jednostek pomocy społecznej najbardziej użyteczną podstawą przetwarzania danych beneficjentów staje się podstawa określona w art. 6 ust. 1 lit. c RODO, tj. przetwarzanie danych odbywa się z uwagi na to, że jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze.

Wymienia się następujące akty prawne zawierające przepisy prawa nakładające na administratora **obowiązek prawny** tego rodzaju, że niezbędne staje się przetwarzanie danych osobowych:
- ustawa z dnia 26 października 1982 roku o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi;
- ustawa z 19 sierpnia 1994 r. o ochronie zdrowia psychicznego,
- ustawa z dnia 10 kwietnia 1997 roku prawo energetyczne,
- ustawa z dnia 21 czerwca 2001 r. o dodatkach mieszkaniowych,
- ustawa z dnia 28 listopada 2003 r. o świadczeniach rodzinnych,
- ustawa z dnia 12 marca 2004 r. o pomocy społecznej,

- ustawa z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych,
- ustawa z dnia 29 lipca 2005 r. o przeciwdziałaniu przemocy w rodzinie,
- ustawa z dnia 29 lipca 2005 roku o przeciwdziałaniu narkomanii,
- ustawa z dnia 7 września 2007 r. o pomocy osobom uprawnionym do alimentów,
- ustawa z dnia 9 czerwca 2011 r. o wspieraniu rodziny i systemie pieczy zastępczej,
- ustawa z dnia 4 kwietnia 2014 r. o ustaleniu i wypłacie zasiłków dla opiekunów,
- ustawa z dnia 5 grudnia 2014r o Karcie Dużej Rodziny,
- ustawa z dnia 11 lutego 2016r. o pomocy państwa w wychowywaniu dzieci,
- ustawa z dnia 4 listopada 2016r o wsparciu kobiet w ciąży i rodzin „Za życiem".

W kontekście danych osobowych przetwarzanych w pomocy społecznej warto zwrócić uwagę na opinię prezentowaną przez Prezesa Urzędu Ochrony Danych Osobowych, wedle której za niezgodne z prawem uznaje się oznaczanie strony postępowania administracyjnego numerem PESEL. W komunikacie dostępnym pod adresem https://uodo.gov.pl/pl/138/561 PUODO wskazuje m.in., że *numer PESEL to bowiem krajowy numer identyfikacyjny, który powinien podlegać szczególnej ochronie (art. 87 RODO). Jego używanie na potrzeby oznaczenia strony postępowania administracyjnego jest nadmiarowe i niezgodne z zasadą minimalizacji danych wyrażoną w art. 5 ust. 1 lit. c 1 RODO*. Prezes Urzędu Ochrony Danych Osobowych wskazuje również, że podanie numeru PESEL jest możliwe jedynie wówczas, gdy wynika to wprost z przepisów prawa – jest wówczas spełniona przesłanka legalizująca jego przetwarzanie określona w art. 6 ust. 1 lit. c RODO (przetwarzanie danych jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze). Jak wskazuje PUODO: *tak jest w przypadku zamieszczania numeru PESEL w tytule wykonawczym w przypadku prowadzenia przez organ administracji postępowania egzekucyjnego. Stanowi o tym art. 27 § 1 pkt 2 ustawy z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji. Zatem dopiero na etapie prowadzonego postępowania egzekucyjnego uzasadnione jest wskazanie numeru PESEL strony postępowania.*

3. Realizacja obowiązku informacyjnego

Rozporządzenie nakłada na administratora i podmiot przetwarzający obowiązek prawidłowego informowania osób, których dane dotyczą o przetwarzaniu ich danych osobowych. Sposób poinformowania określają art. 13 i 14 RODO.

Artykuł 13 RODO - 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 wszystkie 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;
c) cele przetwarzania danych osobowych, oraz podstawę prawną przetwarzania;
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 informację o sposobach uzyskania kopii tych zabezpieczeń lub o miejscu ich udostępnienia.

2. Poza informacjami, o których mowa w ust. 1, podczas pozyskiwania danych osobowych administrator podaje osobie, której dane dotyczą, następujące inne informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania:
a) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
b) informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub 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 RODO - 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;
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;
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 informację o sposobach uzyskania kopii tych zabezpieczeń lub o miejscu ich udostępnienia.

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. Techniczne i organizacyjne środki bezpieczeństwa oraz stosowanie polityki ochrony danych osobowych

Na gruncie RODO zniknął obowiązek wdrożenia konkretnych mechanizmów ochrony danych osobowych – rozporządzenie pozostawia administratorowi wybór w tym względzie, przy zachowaniu zasady rozliczalności oraz przy zastosowaniu podejścia opartego na ryzyku.

Jak wskazuje P. Fajgielski, przez pojęcie polityki ochrony danych *rozumieć można strategię ochrony danych, a więc przemyślany plan działań w dziedzinie ochrony danych, mający umożliwić osiągnięcie celu, jakim jest skuteczna ochrona danych. W tym rozumieniu polityka ochrony danych oznacza ogólny dokument wskazujący podstawowe założenia i cele, natomiast nie jest to akt normujący szczegółowe zagadnienia związane z technicznymi i organizacyjnymi środkami zabezpieczenia danych* (Fajgielski Paweł, Komentarz do rozporządzenia nr 2016/679 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), [w:] Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz)

Wdrożenie polityki ochrony danych osobowych będzie zatem niezbędne, gdy będzie to proporcjonalne do istniejącego przetwarzania.

Przy określeniu sposobów zabezpieczenia danych w szczególności należy uwzględnić specyfikę przetwarzania oceniając:
- charakter, zakres, kontekst i cele przetwarzania,
- oraz ryzyko naruszenia praw lub wolności osób fizycznych.

Przyjęte środki powinny być poddawane **cyklicznym przeglądom i uaktualniane**. W tym względzie można wdrożyć politykę monitorowania, w której znajdą się zasady monitorowania przestrzegania rozporządzenia. Zadanie to można również zlecić inspektorowi ochrony danych, który jest odpowiedzialny za monitorowanie przestrzegania rozporządzenia.

Artykuł 24 RODO - Obowiązki administratora

1. Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane.
2. Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki, o których mowa w ust. 1, obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych.
3. Stosowanie zatwierdzonych kodeksów postępowania, o których mowa wart. 40, lub zatwierdzonego mechanizmu certyfikacji, o którym mowa wart. 42, może być wykorzystane jako element dla stwierdzenia przestrzegania przez administratora ciążących na nim obowiązków.

Artykuł 32 RODO - 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, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym między innymi w stosownym przypadku:

a) pseudonimizację i szyfrowanie danych osobowych;
b) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;
c) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;
d) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

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

3. 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.

5. Prawa osób, których dane dotyczą

Każda osoba, **ma prawo zgłoszenia podmiotowi, który przetwarza jej dane żądań**: dostępu do swoich danych, ich sprostowania, usunięcia lub ograniczenia przetwarzania, sprzeciwu, a także prawo do przenoszenia tych danych w granicach wyznaczonych rozporządzeniem. Jeżeli jej prawa w zakresie

ochrony danych osobowych są naruszane, może również wnieść skargę do organu nadzorczego, którym jest Prezes Urzędu Ochrony Danych Osobowych.

Szczególną uwagę należy tu zwrócić na prawa, które w praktyce są najczęściej wykorzystywane przez podmioty danych, tj. prawo dostępu, prawo do bycia zapomnianym oraz sprzeciw wobec przetwarzania danych.

Artykuł 15 - Prawo dostępu przysługujące osobie, której dane dotyczą

1. Osoba, której dane dotyczą, jest uprawniona do uzyskania od administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz następujących informacji:
   a) cele przetwarzania;
   b) kategorie odnośnych danych osobowych;
   c) informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;
   d) w miarę możliwości planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
   e) informacje o prawie do żądania od administratora sprostowania, 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 w powszechnie stosowanej formie elektronicznej.
4. Prawo do uzyskania kopii, o której mowa w ust. 3, nie może niekorzystnie wpływać na prawa i wolności innych.

Artykuł 17 RODO - 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;
   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 21 RODO - 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, wniesie sprzeciw wobec przetwarzania do celów marketingu bezpośredniego, danych osobowych nie wolno już przetwarzać do takich celów.

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.

W szczególności zwrócić tu uwagę należy, że nie zawsze realizacja powyższych praw będzie konieczna. Na przykład, w zakresie dostępu do danych trzeba podkreślić, że *jeżeli administrator nie przetwarza danych dotyczących osoby, która zwraca się z żądaniem udzielenia informacji, to działanie administratora ogranicza się do odpowiedzi przeczącej i nie ma on obowiązku podawać podmiotowi danych innych informacji. W sytuacji gdy administrator wcześniej przetwarzał dane wnioskodawcy, ale zaprzestał ich przetwarzania (usunął albo zanonimizował dane), to – w miarę możliwości – powinien poinformować o tym fakcie osobę, której dane dotyczą* (Fajgielski Paweł, Komentarz do rozporządzenia nr 2016/679 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), [w:] Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz).

Odnosząc się do innej istotnej tu kwestii należy pamiętać, że – jak podkreśla się w piśmiennictwie - *przy realizacji żądania usunięcia danych powinna być stosowana ogólna reguła określona w art. 12 ust. 3, zgodnie z którą administrator ma obowiązek udzielić osobie, której dane dotyczą, informacji o działaniach podjętych w związku z żądaniem, bez zbędnej zwłoki – a w każdym razie w terminie miesiąca od otrzymania żądania, przy czym w razie potrzeby termin ten może być przedłużony o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań, o czym należy powiadomić wnioskodawcę, jeżeli taka sytuacja zachodzi, podając przyczyny opóźnienia dotyczą* (Fajgielski Paweł, Komentarz do rozporządzenia nr 2016/679 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), [w:] Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz).

6. Naruszenie ochrony danych osobowych

Jak wynika z treści art. 4 pkt. 11 RODO **naruszeniem ochrony danych osobowych** jest 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.

Jak wskazuje się w piśmiennictwie *wszystkie postaci operacji, które zostały wymienione w komentowanym przepisie, muszą dotyczyć danych osobowych. Jest to oczywisty i wprost wynikający z przepisu element pojęcia naruszenia ochrony danych osobowych. Jeżeli zatem dojdzie do naruszenia zasad bezpieczeństwa w rozumieniu przepisu art. 4 pkt 12 rozporządzenia ogólnego, jednak w jego konsekwencji zostaną utracone dane, które nie są danymi osobowymi, wówczas nie dojdzie do spełnienia przesłanek omawianego tu pojęcia* (Bielak-Jomaa Edyta (red.), Lubasz Dominik (red.), RODO. Ogólne rozporządzenie o ochronie danych. Opublikowano: WKP 2018).

W szczególności należy pamiętać, że naruszenie ochrony danych osobowych musi zostać zgłoszone Prezesowi Urzędu Ochrony Danych Osobowych w terminie 72 godzin stwierdzenia naruszenia – chyba, że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. W przypadku stwierdzenia, że naruszenie może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zobowiązany jest zawiadomić o naruszeniu również osobę, której prawa lub wolności mogły zostać naruszone.

Artykuł 33 RODO Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu

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 nadzorczemu weryfikowanie przestrzegania niniejszego artykułu.

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

1. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.
2. Zawiadomienie, o którym mowa w ust. 1 niniejszego artykułu, jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki, o których mowa w art. 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.

7. Odpowiedzialność odszkodowawcza

Każda osoba, której prawa wynikające z rozporządzenia zostały naruszone ma prawo do żądania od administratora lub podmiotu przetwarzającego **odszkodowania na drodze cywilnoprawnej**. Jak stanowi art. 93 ustawy o ochronie danych osobowych sprawy o roszczenia tego rodzaju, tj. z art. 79 i 82 RODO **rozpoznawane są przez właściwy sąd okręgowy.**

Artykuł 79 RODO - Prawo do skutecznego środka ochrony prawnej przed sądem przeciwko administratorowi lub podmiotowi przetwarzającemu

1. Bez uszczerbku dla dostępnych administracyjnych lub pozasądowych środków ochrony prawnej, w tym prawa do wniesienia skargi do organu nadzorczego zgodnie z art. *77,* każda osoba, której dane dotyczą, ma prawo do skutecznego środka ochrony prawnej przed sądem, jeżeli uzna ona, że prawa przysługujące jej na mocy niniejszego rozporządzenia zostały naruszone w wyniku przetwarzania jego danych osobowych z naruszeniem niniejszego rozporządzenia.

2. Postępowanie przeciwko administratorowi lub podmiotowi przetwarzającemu wszczyna się przed sądem państwa członkowskiego, w którym administrator lub podmiot przetwarzający posiadają jednostkę organizacyjną. Ewentualnie postępowanie takie może zostać wszczęte przed sądem państwa członkowskiego, w którym osoba, której dane dotyczą, ma miejsce zwykłego pobytu,

chyba że administrator lub podmiot przetwarzający są organami publicznymi państwa członkowskiego wykonującymi swoje uprawnienia publiczne.

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.

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

Warto zauważyć, że odpowiedzialność odszkodowawczą poniesie administrator lub podmiot przetwarzający **jedynie przy jednoczesnym spełnieniu przesłanek:**

- zaistnienie szkody,

- naruszenie przepisów rozporządzenia,

- związek przyczynowo – skutkowy pomiędzy szkodą a naruszeniem,

- wystąpienie winy w naruszeniu rozporządzenia (Bielak-Jomaa Edyta (red.), Lubasz Dominik (red.), RODO. Ogólne rozporządzenie o ochronie danych. Opublikowano: WKP 2018).

Naruszenie rozporządzenia, zgodnie z motywem 146 do RODO oznacza naruszenia wszelkich aktów prawnych przyjętych na mocy rozporządzenia.

8. Sankcje administracyjne za naruszenie przepisów rozporządzenia

Za naruszenie przepisów rozporządzenia możliwe jest także nałożenie administracyjnej kary pieniężnej, o której mowa w art. 83 RODO. Rozporządzenie wymaga, aby kara była nałożona indywidualnie i była skuteczna, proporcjonalna i odstraszająca. Administracyjną karę pieniężną nakłada Prezes Urzędu Ochrony Danych Osobowych w drodze decyzji administracyjnej. Jej wysokość w stosunku do jednostek sektora finansów publicznych została ograniczona kwotowo do 100 000 zł.

Artykuł 83 RODO - 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 należytą 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;

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 odstraszające. 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.

Art. 102 ustawy z 10.05.2018 r. o ochronie danych osobowych - Nałożenie administracyjnej kary pieniężnej na jednostki sektora finansów publicznych, instytuty badawcze lub NBP

1. Prezes Urzędu może nałożyć, w drodze decyzji, administracyjne kary pieniężne w wysokości do 100 000 złotych, na:
1) jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 1-12 i 14 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych;
2) instytut badawczy;
3) Narodowy Bank Polski.

3. Prezes Urzędu może nałożyć, w drodze decyzji, administracyjne kary pieniężne w wysokości do 10 000 złotych na jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 13 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych.

3. Administracyjne kary pieniężne, o których mowa w ust. 1 i 2, Prezes Urzędu nakłada na podstawie i na warunkach określonych w art. 83 rozporządzenia 2016/679.

NOTATKI

NOTATKI

NOTATKI

NOTATKI