



ROZPORZĄDZENIE OGÓLNE W SPRAWIE OCHRONY DANYCH OSOBOWYCH

adw. dor. pod.
Bartosz Kubista



ZAGADNIENIA WPROWADZAJĄCE PODSTAWOWE POJĘCIA

ZAKRES REGULACJI

Art. 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.**

ZAKRES REGULACJI

Artykuł 2 Materialny 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.

ZAKRES REGULACJI

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.**

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.

DEFINICJE

Artykuł 4 Definicje

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;

DEFINICJE

Artykuł 4 Definicje

Na użytek niniejszego rozporządzenia:

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;

DEFINICJE

Artykuł 4 Definicje

Na użytek niniejszego rozporządzenia:

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;

DEFINICJE

Artykuł 4 Definicje

Na użytek niniejszego rozporządzenia:

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;

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;

DEFINICJE

Artykuł 4 Definicje

Na użytek niniejszego rozporządzenia:

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**;

DEFINICJE

Artykuł 4 Definicje

Na użytek niniejszego rozporządzenia:

9) "odbiorca" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, **któremu ujawnia się dane osobowe**, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania;

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**;

DEFINICJE

Artykuł 4 Definicje

Na użytek niniejszego rozporządzenia:

1 1) "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;

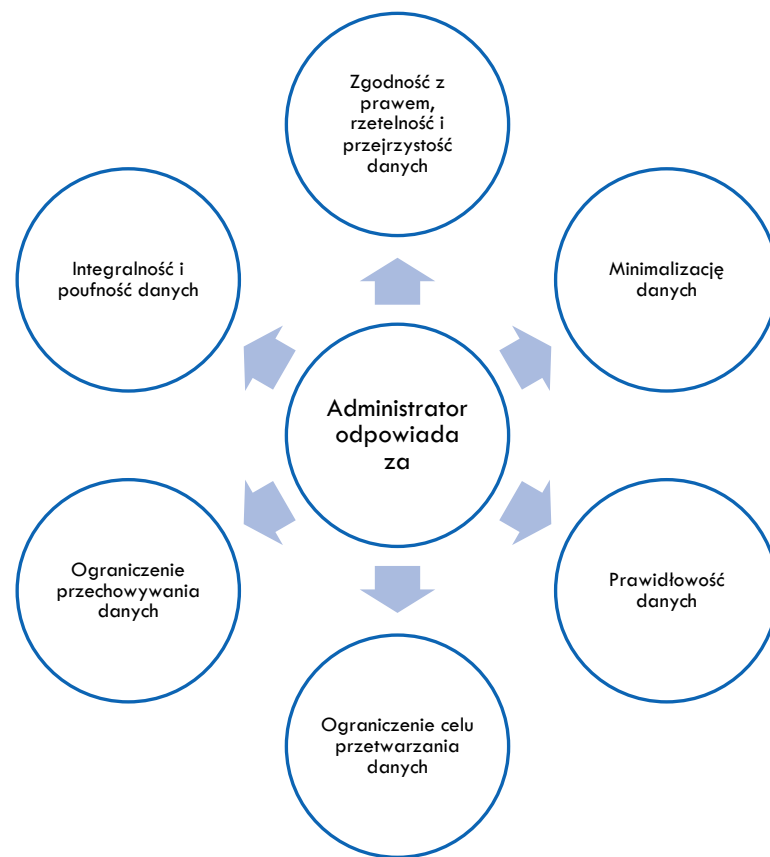
1 2) "naruszenie ochrony danych osobowych" oznacza **naruszenie bezpieczeństwa** prowadzące do **przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu** do danych osobowych przesyłanych, przechowywanych lub w inny sposób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



ZASADY DOTYCZĄCE PRZETWARZANIA DANYCH OSOBOWYCH

GDPR [GENERAL DATA PROTECTION RULE]

OGÓLNA ZASADA OCHRONY DANYCH OSOBOWYCH



ZASADY DOTYCZĄCE PRZETWARZANIA DANYCH

Artykuł 5 Zasady dotyczące przetwarzania danych osobowych

1. Dane osobowe muszą być:

- a) przetwarzane **zgodnie z prawem, rzetelnie i w sposób przejrzysty** dla osoby, której dane dotyczą ("zgodność z prawem, rzetelność i przejrzystość");
- b) zbierane **w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami**; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 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");

ZASADY DOTYCZĄCE PRZETWARZANIA DANYCH

Artykuł 5 Zasady dotyczące przetwarzania danych osobowych

1. Dane osobowe muszą być:

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");

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");

ZASADY DOTYCZĄCE PRZETWARZANIA DANYCH

Artykuł 5 Zasady dotyczące przetwarzania danych osobowych

1. Dane osobowe muszą być:

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").

ZGODNOŚĆ Z PRAWEM

Artykuł 6 Zgodność przetwarzania z prawem

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

- a) 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.

ZGODA NA PRZETWARZANIE DANYCH OSOBOWYCH

Artykuł 7 Warunki wyrażenia zgody

1. Jeżeli przetwarzanie odbywa się na podstawie zgody, **administrator musi być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych.**

2. Jeżeli osoba, której dane dotyczą, 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.**

ZGODA NA PRZETWARZANIE DANYCH OSOBOWYCH

Artykuł 7 Warunki wyrażenia zgody

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**.

PRZETWARZANIE DANYCH „WRAŻLIWYCH”

Artykuł 9 Przetwarzanie szczególnych kategorii danych osobowych

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

PRZETWARZANIE DANYCH „WRAŻLIWYCH”

Artykuł 9 Przetwarzanie szczególnych kategorii danych osobowych

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

- a) osoba, której dane dotyczą, **wyraziła wyraźną zgodę** na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach, chyba że prawo Unii 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;

PRZETWARZANIE DANYCH „WRAŻLIWYCH”

Artykuł 9 Przetwarzanie szczególnych kategorii danych osobowych

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

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**;

PRZETWARZANIE DANYCH „WRAŻLIWYCH”

Artykuł 9 Przetwarzanie szczególnych kategorii danych osobowych

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

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;

PRZETWARZANIE DANYCH „WRAŻLIWYCH”

Artykuł 9 Przetwarzanie szczególnych kategorii danych osobowych

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

- 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;
- 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.

DANE NIEZIDENTYFIKOWANE

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.



PRAWA OSOBY, KTÓREJ DANE DOTYCZĄ

INFORMOWANIE O OCHRONIE DANYCH OSOBOWYCH

Artykuł 12 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.

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 wykaze, iż nie jest w stanie zidentyfikować osoby, której dane dotyczą.

INFORMOWANIE O OCHRONIE DANYCH OSOBOWYCH

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 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 o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych.

INFORMOWANIE O OCHRONIE DANYCH OSOBOWYCH

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

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.

INFORMOWANIE O OCHRONIE DANYCH OSOBOWYCH

Artykuł 13 Informacje podawane w przypadku zbierania danych od 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.

INFORMOWANIE O OCHRONIE DANYCH OSOBOWYCH

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;
- 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 o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych.

INFORMOWANIE O OCHRONIE DANYCH OSOBOWYCH

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

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.

INFORMOWANIE O OCHRONIE DANYCH OSOBOWYCH

Artykuł 14 Informacje podawane w przypadku pozyskiwania danych osobowych w sposób inny niż od 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.

INFORMOWANIE O OCHRONIE DANYCH OSOBOWYCH

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

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.**

PRAWO DOSTĘPU DO 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.

PROSTOWANIE DANYCH

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.

PRAWO DO BYCIA ZAPOMNIANYM

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;
- 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;

PRAWO DO BYCIA ZAPOMNIANYM

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:

- 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.

PRAWO DO BYCIA ZAPOMNIANYM

Artykuł 17 Prawo do usunięcia danych ("prawo do bycia zapomnianym")

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.**

PRAWO DO BYCIA ZAPOMNIANYM

Artykuł 17 Prawo do usunięcia danych ("prawo do bycia zapomnianym")

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.

PRAWO DO OGRANICZENIA DANYCH OSOBOWYCH

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.

PRAWO DO OGRANICZENIA DANYCH OSOBOWYCH

Artykuł 18 Prawo do ograniczenia przetwarzania

2. Jeżeli na mocy ust. 1 przetwarzanie zostało ograniczone, takie dane osobowe można przetwarzać, z wyjątkiem przechowywania, wyłącznie za zgodą osoby, której dane dotyczą, lub w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii lub państwa członkowskiego.

3. Przed uchyleniem ograniczenia przetwarzania administrator informuje o tym osobę, której dane dotyczą, która żądała ograniczenia na mocy ust. 1.

PROSTOWANIE LUB USUWANIE DANYCH

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.

PRZENOSZENIE DANYCH

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.

PRAWO DO SPRZECIWU

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.**



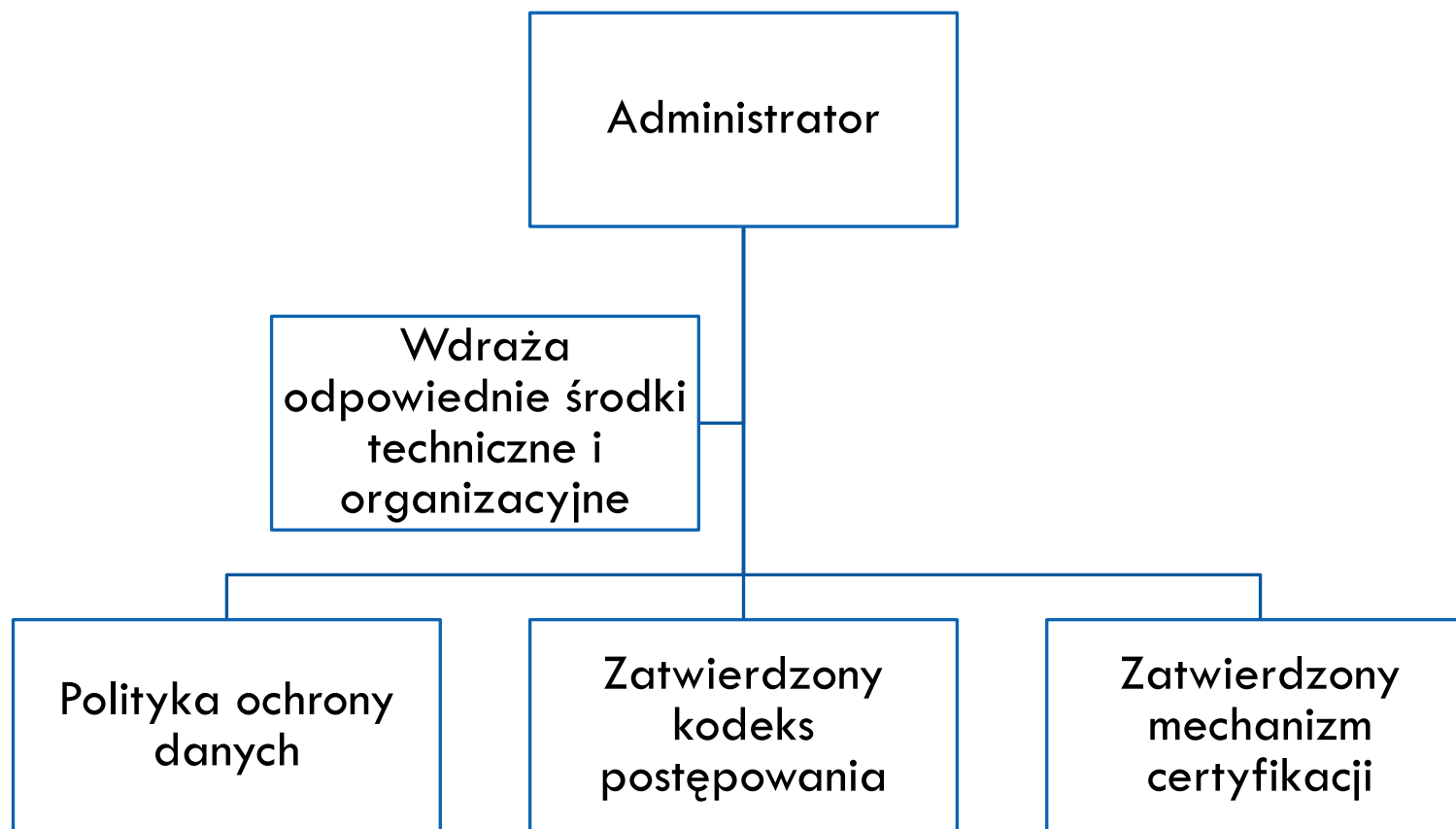
PRAWA I OBOWIĄZKI ADMINISTRATORA

OBOWIĄZKI ADMINISTRATORA

Artykuł 24 Obowiązki administratora

1. Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, 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 w art. 40, lub **zatwierdzonego mechanizmu certyfikacji**, o którym mowa w art. 42, może być wykorzystane jako element dla stwierdzenia przestrzegania przez administratora ciążących na nim obowiązków.

ŚRODKI TECHNICZNE I ORGANIZACYJNE



PRIVACY BY DESIGN

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.

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.

PRIVACY BY DEFAULT

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

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.

WSPÓŁADMINISTRATORZY

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.

PODMIOT PRZETWARZAJĄCY

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.

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.

PODMIOT PRZETWARZAJĄCY

Artykuł 28 Podmiot przetwarzający

3. Przetwarzanie przez podmiot przetwarzający odbywa się **na podstawie umowy lub innego instrumentu prawnego**, które podlegają prawu Unii lub prawu państwa członkowskiego i wiążą podmiot przetwarzający i administratora, **określają przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora**. Ta umowa lub inny 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** [[Bezpieczeństwo danych osobowych](#)];

PODMIOT PRZETWARZAJĄCY

Artykuł 28 Podmiot przetwarzający

3. Przetwarzanie przez podmiot przetwarzający odbywa się **na podstawie umowy lub innego instrumentu prawnego**, które podlegają prawu Unii lub prawu państwa członkowskiego i wiążą podmiot przetwarzający i administratora, **określają przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora**. Ta umowa lub inny instrument prawny stanowią w szczególności, że podmiot przetwarzający:

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 [\[Prawa i obowiązki\]](#);

f) uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga administratorowi wywiązać się z obowiązków określonych w art. 32-36 [\[Bezpieczeństwo danych osobowych\]](#);

PODMIOT PRZETWARZAJĄCY

Artykuł 28 Podmiot przetwarzający

3. Przetwarzanie przez podmiot przetwarzający odbywa się **na podstawie umowy lub innego instrumentu prawnego**, które podlegają prawu Unii lub prawu państwa członkowskiego i wiążą podmiot przetwarzający i administratora, **określają przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora**. Ta umowa lub inny instrument prawny stanowią w szczególności, że podmiot przetwarzający:

- 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.

PODMIOT PRZETWARZAJĄCY

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.

9. Umowa lub inny akt prawny, o których mowa w art. 3 i 4, **mają formę pisemną, w tym formę elektroniczną.**

REJESTROWANIE CZYNNOŚCI PRZETWARZANIA

Artykuł 30 Rejestrowanie czynności przetwarzania

1. Każdy administrator oraz - gdy ma to zastosowanie - przedstawiciel administratora prowadzą **rejestr czynności przetwarzania danych osobowych, 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**;
- 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 [[przekazanie poza terytorium UE](#)], 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 [[Bezpieczeństwo danych](#)].

REJESTROWANIE CZYNNOŚCI PRZETWARZANIA

Artykuł 30 Rejestrowanie czynności przetwarzania

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 [\[Dane wrażliwe\]](#), lub dane osobowe dotyczące wyroków skazujących i naruszeń prawa, o czym mowa w art. 10.

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;
- 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.

BEZPIECZEŃSTWO DANYCH OSOBOWYCH

Artykuł 32 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.

NARUSZENIE DANYCH OSOBOWYCH

Artykuł 33 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.

NARUSZENIE DANYCH OSOBOWYCH

Artykuł 33 Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorcemu

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

NARUSZENIE DANYCH OSOBOWYCH

Artykuł 33 Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorcemu

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**.

NARUSZENIE DANYCH OSOBOWYCH

Artykuł 34 Zawiadamywanie 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).

NARUSZENIE DANYCH OSOBOWYCH

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

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.

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.

OCENA SKUTKÓW DLA OCHRONY DANYCH I UPRZEDNIE KONSULTACJE

Artykuł 35 Ocena skutków dla ochrony danych

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**.

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.

OCENA SKUTKÓW DLA OCHRONY DANYCH I UPRZEDNIE KONSULTACJE

Artykuł 35 Ocena skutków dla ochrony danych

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.

OCENA SKUTKÓW DLA OCHRONY DANYCH I UPRZEDNIE KONSULTACJE

Artykuł 36 Uprzednie 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.



INSPEKTOR OCHRONY DANYCH

WYZNACZENIE INSPEKTORA

Artykuł 37 Wyznaczenie inspektora ochrony danych

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

- a) przetwarzania dokonują organ lub podmiot publiczny, 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** [\[Dane wrażliwe\]](#), oraz danych osobowych **dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10.**

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

WYZNACZENIE INSPEKTORA

Artykuł 37 Wyznaczenie inspektora ochrony danych

4. W przypadkach innych niż te, o których mowa w ust. 1, **administrator, podmiot przetwarzający, zrzeczenia 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 zrzeczeń i innych podmiotów reprezentujących administratorów lub podmioty przetwarzające.**

5. Inspektor ochrony danych jest wyznaczany **na podstawie kwalifikacji zawodowych**, a w szczególności **wiedzy fachowej na temat prawa i praktyk** w dziedzinie ochrony danych oraz umiejętności 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.**

INSPEKTOR OCHRONY DANYCH OSOBOWYCH

Artykuł 38 Status inspektora ochrony danych

1. Administrator oraz podmiot przetwarzający zapewniają, by inspektor ochrony danych **był właściwie i niezwłocznie włączany we wszystkie sprawy** dotyczące ochrony danych osobowych.

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**.

INSPEKTOR OCHRONY DANYCH OSOBOWYCH

Artykuł 38 Status inspektora ochrony danych

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.**

OBOWIĄZKI INSPEKTORA OCHRONY DANYCH OSOBOWYCH

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 **obowiązках spoczywających na nich na mocy niniejszego rozporządzenia** oraz innych przepisów Unii lub państw członkowskich o ochronie danych i **doradzanie im w tej sprawie**;
- 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 audyty;
- 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 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.



ZATWIERDZONY KODEKS POSTĘPOWANIA I ZATWIERDZONA CERTYFIKACJA

KODEKSY POSTĘPOWANIA

Artykuł 40 Kodeksy postępowania

1. Państwa członkowskie, organy nadzorcze, Europejska Rada Ochrony Danych oraz Komisja zachęcają do sporządzania kodeksów postępowania mających pomóc we właściwym stosowaniu niniejszego rozporządzenia - z uwzględnieniem specyfiki różnych sektorów dokonujących przetwarzania oraz szczególnych potrzeb mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw.

KODEKSY POSTĘPOWANIA

Artykuł 40 Kodeksy postępowania

2. Zrzeszenia i inne podmioty reprezentujące określone kategorie administratorów lub podmioty przetwarzające mogą opracowywać lub zmieniać kodeksy postępowania lub rozszerzać ich zakres, aby doprecyzować zastosowanie niniejszego rozporządzenia, między innymi w odniesieniu do:

- a) rzetelnego i przejrzystego przetwarzania;
- b) prawnie uzasadnionych interesów realizowanych przez administratorów w określonych kontekstach;
- c) zbierania danych osobowych;
- d) pseudonimizacji danych osobowych;
- e) informowania opinii publicznej i osób, których dane dotyczą;

KODEKSY POSTĘPOWANIA

Artykuł 40 Kodeksy postępowania

2. Zrzeszenia i inne podmioty reprezentujące określone kategorie administratorów lub podmioty przetwarzające mogą opracowywać lub zmieniać kodeksy postępowania lub rozszerzać ich zakres, aby doprecyzować zastosowanie niniejszego rozporządzenia, między innymi w odniesieniu do:

- f) wykonywania przez osoby, których dane dotyczą, przysługujących im praw;
- g) informowania i ochrony dzieci oraz sposobu pozyskiwania zgody osoby sprawującej władzę rodzicielską lub opiekę nad dzieckiem;
- h) środków i procedur, o których mowa w art. 24 i 25, oraz środków zapewniających bezpieczeństwo przetwarzania, o których mowa w art. 32;
- i) zgłaszania organowi nadzorcemu naruszeń ochrony danych osobowych oraz zawiadamiania o takich naruszeniach osób, których dane dotyczą;
- j) przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych; lub
- k) postępowań pozasądowych oraz innych trybów rozstrzygania sporów w celu rozstrzygania sporów między administratorami a osobami, których dane dotyczą, w zakresie przetwarzania, bez uszczerbku dla praw osób, których dane dotyczą, na mocy art. 77 i 79.

KODEKSY POSTĘPOWANIA

Artykuł 40 Kodeksy postępowania

4. Kodeks postępowania, o którym mowa w ust. 2 niniejszego artykułu, **przewiduje mechanizmy pozwalające podmiotowi, o którym mowa w art. 41 ust. 1, prowadzić obowiązkowe monitorowanie przestrzegania przepisów kodeksu przez administratorów lub podmioty przetwarzające, którzy podjęli się jego stosowania, bez uszczerbku dla zadań i uprawnień organów nadzorczych** właściwych na mocy art. 55 lub 56.

5. Zrzeszenia i inne podmioty, o których mowa w ust. 2 niniejszego artykułu, chcące opracować kodeks postępowania lub zmienić lub rozszerzyć zakres kodeksu już obowiązującego **przedkładają projekt kodeksu, zmiany lub rozszerzenia organowi nadzorcemu** właściwemu na mocy art. 55. Organ nadzorczy wydaje opinię o zgodności projektu kodeksu, zmiany lub rozszerzenia z niniejszym rozporządzeniem i zatwierdza taki projekt kodeksu, zmiany lub rozszerzenia, jeżeli uzna, że stanowią one odpowiednie zabezpieczenia.

6. W przypadku zatwierdzenia zgodnie z ust. 5 projektu kodeksu, zmiany lub rozszerzenia, organ nadzorczy rejestruje i publikuje ten kodeks, o ile nie dotyczy on czynności przetwarzania prowadzonych w kilku państwach członkowskich.

KODEKSY POSTĘPOWANIA

Artykuł 41 Monitorowanie zatwierdzonych kodeksów postępowania

1. Bez uszczerbku dla zadań i uprawnień właściwego organu nadzorczego wynikających z art. 57 i 58 monitorowaniem przestrzegania kodeksu postępowania na mocy art. 40 może się zajmować podmiot, który dysponuje odpowiednim poziomem wiedzy fachowej w dziedzinie będącej przedmiotem kodeksu i został akredytowany w tym celu przez właściwy organ nadzorczy.

2. Podmiot, o którym mowa w ust. 1, może zostać akredytowany w celu monitorowania przestrzegania kodeksu postępowania, jeżeli:

- a) w sposób satysfakcjonujący wykazał on właściwemu organowi nadzorczemu swoją niezależność i wiedzę fachową w dziedzinie będącej przedmiotem kodeksu;
- b) dysponuje procedurami, które pozwalają mu ocenić zdolność konkretnych administratorów i podmiotów przetwarzających do stosowania kodeksu, monitorować przestrzeganie przez nich jego przepisów oraz okresowo dokonywać przeglądu jego funkcjonowania;
- c) dysponuje procedurami i strukturami, które pozwalają rozpatrywać skargi na naruszenie kodeksu przez administratora lub podmiot przetwarzający lub na sposób wdrożenia lub wdrażania kodeksu przez administratora lub podmiot przetwarzający oraz które pozwalają zapewnić przejrzystość tych procedur i struktur dla osób, których dane dotyczą, i opinii publicznej; oraz
- d) w sposób satysfakcjonujący wykazał właściwemu organowi nadzorczemu, że jego zadania i obowiązki nie powodują konfliktu interesów.

CERTYFIKACJA

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.**

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.

CERTYFIKACJA

Artykuł 42 Certyfikacja

3. Certyfikacja jest **dobrowolna**, a proces jej uzyskania **musi być przejrzysty**.
4. Certyfikacja przewidziana w niniejszym artykule **nie wpływa na spoczywający na administratorze lub podmiocie przetwarzającym obowiązek przestrzegania niniejszego rozporządzenia** i pozostaje bez uszczerbku dla zadań i uprawnień organów nadzorczych właściwych na mocy art. 55 lub 56.
5. Certyfikacji przewidzianej w niniejszym artykule dokonują **podmioty certyfikujące**, o których mowa w art. 43, lub dokonuje **jej właściwy organ nadzorczy** - na podstawie kryteriów zatwierdzonych przez niego zgodnie z art. 58 ust. 3 lub przez Europejską Radę Ochrony Danych zgodnie z art. 63. W przypadku gdy kryteria są zatwierdzane przez Europejską Radę Ochrony Danych, może to skutkować wspólną certyfikacją, **europejskim znakiem jakości ochrony danych**.

CERTYFIKACJA

Artykuł 42 Certyfikacja

6. Administrator lub podmiot przetwarzający, którzy poddają swoje przetwarzanie mechanizmowi certyfikacji, **udzielają** podmiotowi certyfikującemu, o którym mowa w art. 43, lub gdy ma to zastosowanie - właściwemu organowi nadzorczemu **wszelkich informacji i wszelkiego dostępu do swoich czynności przetwarzania**, które to informacje i dostęp są niezbędne do przeprowadzenia procedury certyfikacji.

7. Certyfikacji administratora lub podmiotu przetwarzającego udziela się **na maksymalny okres 3 lat**; certyfikację **można przedłużyć na tych samych warunkach**, o ile nadal spełnione są stosowne wymogi. W stosownym przypadku organy certyfikujące, o których mowa w art. 43, lub właściwy organ nadzorczy cofają certyfikację, jeżeli jej wymogi nie są spełnione lub przestały być spełniane.

8. Europejska Rada Ochrony Danych gromadzi w rejestrze wszystkie mechanizmy certyfikacji oraz znaki jakości i oznaczenia w dziedzinie ochrony danych i udostępnia je opinii publicznej za pomocą odpowiednich środków.

CERTYFIKACJA

Artykuł 43 Podmiot certyfikujący

1. Bez uszczerbku dla zadań i uprawnień właściwego organu nadzorczego wynikających z art. 57 i 58 podmiot certyfikujący, który dysponuje odpowiednim poziomem wiedzy fachowej w dziedzinie ochrony danych dokonuje certyfikacji i jej przedłużenia po poinformowaniu organu nadzorczego w celu umożliwienia mu w razie potrzeby wykonywania uprawnień na mocy art. 58 ust. 2 lit. h) -. Państwa członkowskie zapewniają akredytację tych podmiotów certyfikujących przez:

- a) organ nadzorczy właściwy zgodnie z art. 55 lub 56; lub
- b) krajową jednostkę akredytującą określoną zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (WE) nr 765/2008 ²⁰ - zgodnie z EN-ISO/IEC 17065/2012 - oraz zgodnie z dodatkowymi wymogami określonymi przez organ nadzorczy właściwy zgodnie z. 55 lub 56.

CERTYFIKACJA

Artykuł 43 Podmiot certyfikujący

2. Podmioty certyfikujące, o których mowa w ust. 1, zostają akredytowane zgodnie z tym ustępem w przypadku gdy:

- a) w sposób satysfakcjonujący wykazały właściwemu organowi nadzorcemu swoją niezależność i wiedzę fachową w dziedzinie podlegającej certyfikacji;
- b) zobowiązały się do przestrzegania kryteriów, o których mowa w art. 42 ust. 5 i które zostały zatwierdzone przez organ nadzorczy właściwy zgodnie z art. 55 lub 56 lub przez Europejską Radę Ochrony Danych zgodnie z art. 63;
- c) dysponują procedurami wydawania, okresowego przeglądu i cofania certyfikacji, znaków jakości i oznaczeń w dziedzinie ochrony danych;
- d) dysponują procedurami i strukturami, które pozwalają rozpatrywać skargi na naruszenie warunków certyfikacji przez administratora lub podmiot przetwarzający lub na sposób wdrożenia lub wdrażania certyfikacji przez administratora lub podmiot przetwarzający, oraz które zapewniają przejrzystość tych procedur i struktur dla osób, których dane dotyczą, i opinii publicznej; oraz
- e) w sposób satysfakcjonujący pokażą właściwemu organowi nadzorcemu, że ich zadania i obowiązki nie powodują konfliktu interesów.

CERTYFIKACJA

Artykuł 43 Podmiot certyfikujący

3. Akredytacja podmiotów certyfikujących, o których mowa w ust. 1 i 2 niniejszego artykułu, jest dokonywana na podstawie kryteriów zatwierdzonych przez organ nadzorczy właściwy zgodnie z art. 55 lub 56 lub przez Europejską Radę Ochrony Danych zgodnie z art. 63. W przypadku akredytacji na mocy ust. 1 lit. c) niniejszego artykułu wymogi te są uzupełnieniem wymogów przewidzianych w rozporządzeniu (WE) nr 765/2008 oraz przepisów technicznych określających metody i procedury podmiotów certyfikujących.



SANKCJE

SKARGA DO ORGANU NADZORCZEGO

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.

OCHRONA PRZED SĄDAMI

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.

ODSZKODOWANIE

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.**

KARY ADMINISTRACYJNE

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 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.

KARY ADMINISTRACYJNE

Artykuł 83 Ogólne warunki nakładania administracyjnych kar pieniężnych

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;

KARY ADMINISTRACYJNE

Artykuł 83 Ogólne warunki nakładania administracyjnych kar pieniężnych

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.

KARY ADMINISTRACYJNE

Artykuł 83 Ogólne warunki nakładania administracyjnych kar pieniężnych

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.



DZIĘKUJĘ ZA UWAGĘ