# OCHRONA DANYCH OSOBOWYCH

**r.pr. dr Michał Miłosz**

## Geneza regulacji ochrony danych osobowych

- Administracyjnoprawna ochrony danych osobowych ma swe źródła w ochronie prywatność, stanowiąc jednak odrębny i stosunkowo nowy reżim prawy.

- **Prawo do prywatności**
  - Konstytucja RP: art. 47 „Każdy ma prawo do ochrony prawnej życia prywatnego, [...]".
  - akty międzynarodowe: Powszechna Deklaracja Praw Człowieka (1948 r.); Konwencja o ochronie praw człowieka i podstawowych wolności (1950 r.); Międzynarodowy Pakt Praw Obywatelskich i Politycznych (1966 r.).

**Czynniki wprowadzenia regulacji:**

- rozszerzający się zakres przetwarzania danych

  a) przedmiotowy – powszechność i wielopłaszczyznowość zbierania informacji,

  b) podmiotowy - wykorzystywanie danych przez różne podmioty,
- zinformatyzowanie przetwarzania danych.

**Funkcje prawa ochrony danych osobowych**

- Przetwarzanie danych osobowych z jednej strony stanowi zagrożenie prywatności jednostki, a z drugiej przetwarzanie danych strony nie tylko może służyć jednostce ale w wielu wypadkach jest niezbędne dla funkcjonowania współczesnego społeczeństwa.
- Przepisy regulujące ochronę danych osobowych starają się rozwiązać ten **konflikt między prawem do prywatności w zakresie danych osobowych a prawem do informacji** i koniecznością przetwarzania danych w życiu codziennym.

## Ochrona danych osobowych w prawie europejskim

Prawa krajowe

- lata 70': Szwecja, Austria, Francja, Luksemburg, Norwegia i Dania;
- lata 80' i wczesne 90': Wlk. Brytania, Irlandia, Islandia, Finlandia oraz Węgry.

Konwencje międzynarodowe

- Konwencja nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych z 1981 r. (Polska: 2002 r.).

Prawo unijne

- **Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679** z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) [dalej skrótem jako „r.o.d.o."] – stosowanie od dnia 25 maja 2018 r.

  *R.o.d.o. zastąpiło dyrektywę 95/46/WE z 1995 w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych.*

- **Rozporządzenie (WE) nr 45/2001** Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych

- **Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680** z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW

  Zgodnie z art. 1 ust. 1 dyrektywy ustanawia ona przepisy o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom.

  Dyrektywa ma zastosowanie do przetwarzania danych osobowych przez właściwe organy do powyżej określonych celów.

- **Dyrektywa 2002/58/WE** z 2002 w sprawie przetwarzania danych osobowych oraz ochrony prywatności w sektorze komunikacji elektronicznej („Dyrektywa o ochronie prywatności i komunikacji elektronicznej").
- Inne akty unijne

Karta Praw Podstawowych UE

Artykuł 8
Ochrona danych osobowych

1. Każdy ma prawo do ochrony danych osobowych, które go dotyczą.
2. Dane te muszą być przetwarzane rzetelnie w określonych celach i za zgodą osoby zainteresowanej lub na innej uzasadnionej podstawie przewidzianej ustawą. Każdy ma prawo dostępu do zebranych danych, które go dotyczą, i prawo do dokonania ich sprostowania.
3. Przestrzeganie tych zasad podlega kontroli niezależnego organu.

## Ochrona danych osobowych w prawie polskim

Konstytucyjne gwarancje ochrony danych osobowych

Zgodnie z art. 51 ust. 1 Konstytucji RP:

- nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawnienia informacji dotyczących jego osoby.
- władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym.
- każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych. Ograniczenie tego prawa może określić ustawa.
- każdy ma prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą.

Ustawowe gwarancje ochrony danych osobowych

- Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych [dalej skrótem jako „u.o.d.o.”].

  ”Każdy ma prawo do ochrony dotyczących go danych osobowych” (art. 1 ust. 1 u.o.d.o.).

  Przetwarzanie danych osobowych może mieć miejsce ze względu na dobro publiczne, dobro osoby, której dane dotyczą, lub dobro osób trzecich w zakresie i trybie określonym ustawą (art. 1 ust. 2 u.o.d.o.).

- Projekt nowej ustawy o ochronie danych osobowych.

- Regulacje szczególne.

# Pojęcie danych osobowych

## Pojęcie danych osobowych

**„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;

art. 4 pkt 1 r.o.d.o.

Dla zakwalifikowania określonej informacji do kategorii danych osobowych nie ma znaczenia m.in. status prawny określonej osoby fizycznej (np. to, czy posiada zdolność do czynności prawnych, czy przysługują jej prawa publiczne, jakie ma obywatelstwo), wiek, płeć itp.

## Pojęcie danych sensytywnych (wrażliwych)

Pewne kategorie danych przetwarzane są na szczególnych zasadach, w odniesieniu do tych danych stosowane bywa pojęcie danych „sensytywnych” lub „wrażliwych”.

**Dane sensytywne (wrażliwe)** to dane osobowe ujawniające 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 [art. 9 r.o.d.o.].

Definicje: „dane genetyczne" (art. 4 pkt 13 r.o.d.o.), "dane biometryczne" (art. 4 pkt 14 r.o.d.o.), "dane dotyczące zdrowia„ (art. 4 pkt 15 r.o.d.o.).

Ogólne rozporządzenie o ochronie danych osobowych zawiera szczególną regulację odnoszącą się do danych osobowych dotyczących wyroków skazujących i naruszeń prawa [art. 10 r.o.d.o.].

„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 r.o.d.o.).

"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 r.o.d.o.).

"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 pkt 15 r.o.d.o.).

# Przedmiot i zakres stosowania przepisów r.o.d.o.

**Przedmiot i cele r.o.d.o.**

Rozporządzenie ustanawia przepisy o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych oraz przepisy o swobodnym przepływie danych osobowych.

Rozporządzenie chroni podstawowe prawa i wolności osób fizycznych, w szczególności ich prawo do ochrony danych osobowych.

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.

[art. 1 r.o.d.o.]

**Zakres przedmiotowy stosowania r.o.d.o.**

- Rozporządzenie dotyczy wyłącznie danych o osobach fizycznych - nie chroni więc informacji o osobach prawnych.

- 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 *[pojęcie przetwarzania danych obejmuje także zbieranie]*.
    [art. 2 ust. 1 r.o.d.o.]

- Innymi słowy rozporządzanie ma zastosowanie do przetwarzania danych osobowych:
  - **w zbiorach danych**,
  - oraz poza zbiorami danych jeżeli jest dokonywane **w systemach informatycznych**.

**Przetwarzanie danych** - „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 [art. 4 pkt 2 r.o.d.o.].

**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 [art. 4 pkt 6 r.o.d.o.].

- zbiorami danych są przykładowo kartoteki, skorowidze, wykazy, inne zbiory ewidencyjne.
- zbiór danych to zestaw danych osobowych uporządkowanych w sposób pozwalający na bezpośredni dostęp do poszukiwanej informacji.
- ustawa nie obejmuje swoim zakresem zastosowania zestawów danych osobowych, gdy nie zostały one uporządkowane przynajmniej według jednego kryterium.

**Zakres podmiotowy stosowania r.o.d.o.**

Przepisy ustawy o ochronie danych osobowych stosuje się do:
- **podmiotów publicznych**
- **podmiotów prywatnych**

Rozporządzenie nie ma zastosowania do przetwarzania danych osobowych przez osobę fizyczną w ramach czynności o czysto osobistym lub domowym charakterze [art. 3a ust. 2 lit. c r.o.d.o. ].

Do przetwarzania danych osobowych przez instytucje, organy i jednostki organizacyjne Unii zastosowanie ma rozporządzenie (WE) nr 45/2001.

Administrator danych – **oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobow**ych; 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 (art. 4 pkt 6 r.o.d.o.).

- ustalanie celów i sposobów przetwarzania oznacza faktyczne podejmowanie, we własnym imieniu, decyzji co do przetwarzanych danych.
- na administratorach danych spoczywają określone prawem obowiązki związane z przetwarzaniem danych.

podmiot przetwarzający - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny **podmiot, który przetwarza dane osobowe w imieniu administratora** (art. 4 pkt 8 r.o.d.o.)

- odbiorca - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią (art. 4 pkt 9 r.o.d.o.).

  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

- 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 (art. 4 pkt 10 r.o.d.o.)

**Zakres terytorialny stosowania przepisów r.o.d.o.**

[art. 3 r.o.d.o.]

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

***Zakres terytorialny stosowania dyrektywy o.d.o. (art. 4)***

1. Każde Państwo Członkowskie stosuje, w odniesieniu do przetwarzania danych osobowych, przepisy prawa krajowego przyjmowane na mocy niniejszej dyrektywy wówczas, gdy:

a) **przetwarzanie danych odbywa się w kontekście prowadzenia przez administratora danych działalności gospodarczej na terytorium Państwa Członkowskiego;** jeżeli ten sam administrator danych prowadzi działalność gospodarczą na terytorium kilku Państw Członkowskich, musi on podjąć niezbędne działania, aby zapewnić, że każde z tych przedsiębiorstw wywiązuje się z obowiązków przewidzianych w odpowiednich przepisach prawa krajowego;

b) administrator danych nie prowadzi działalności gospodarczej na terytorium Państwa Członkowskiego, lecz w miejscu, gdzie jego prawo krajowe obowiązuje na mocy międzynarodowego prawa publicznego;

c) administrator danych nie prowadzi działalności gospodarczej na terytorium Wspólnoty a do celów przetwarzania danych osobowych wykorzystuje środki, zarówno zautomatyzowane jak i inne, znajdujące się na terytorium wymienionego Państwa Członkowskiego, o ile środki te nie są wykorzystywane wyłącznie do celów tranzytu przez terytorium Wspólnoty.

2. W okolicznościach określonych w ust. 1 lit. c), administrator danych musi wyznaczyć swojego przedstawiciela na terytorium tego Państwa Członkowskiego, bez uszczerbku dla postępowań sądowych, jakie mogłyby być podjęte przeciwko samemu administratorowi danych.

---

Wyrok TS UE (wielka izba) z dnia 13 maja 2014 r. w sprawie C-131/12

Sprawa Google Spain SL, Google Inc. Przeciwko Agencia de Protección de Datos (AEPD), Mario Costeja González [orzeczenie w trybie prejudycjalnym]

Regulacja
ogólnego rozporządzenia o ochronie danych osobowych

wyłączenia

uregulowania szczególne

- wyłączenia i uregulowania szczególne mogą mieć podstawę w przepisach unijnych oraz prawa międzynarodowego,
- wyłączenia i uregulowania szczególne mogą wynikać z przepisów krajowych (uregulowania te nie mogą naruszać prawa unijnego).

**Wyłączenia z zakresu zastosowania r.o.d.o. (art. 2 ust. 2-4 r.o.d.o.)**

- 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.
- Do przetwarzania danych osobowych przez instytucje, organy i jednostki organizacyjne Unii zastosowanie ma rozporządzenie (WE) nr 45/2001. Rozporządzenie (WE) nr 45/2001 oraz inne unijne akty prawne mające zastosowanie do takiego przetwarzania danych osobowych zostają dostosowane do zasad i przepisów niniejszego rozporządzenia zgodnie z art. 98.
- Rozporządzenie pozostaje bez uszczerbku dla stosowania dyrektywy 2000/31/WE, w szczególności dla zasad odpowiedzialności usługodawców będących pośrednikami, o których to zasadach mowa w art. 12-15 tej dyrektywy.

**Przepisy r.o.d.o. dotyczące szczególnych sytuacji związanych z przetwarzaniem – podstawa do wprowadzenia regulacji szczególnych w prawie krajowym**

- art. 85 r.o.d.o. - Przetwarzanie a wolność wypowiedzi i informacji
  Państwa członkowskie przyjmują przepisy pozwalające pogodzić prawo do ochrony danych osobowych na mocy niniejszego rozporządzenia z wolnością wypowiedzi i informacji, w tym do przetwarzania dla potrzeb dziennikarskich oraz do celów wypowiedzi akademickiej, artystycznej lub literackiej.
- art. 86 r.o.d.o. - Przetwarzanie a publiczny dostęp do dokumentów urzędowych
- art. 87 r.o.d.o. - Przetwarzanie krajowego numeru identyfikacyjnego
- art. 88 r.o.d.o. - Przetwarzanie w kontekście zatrudnienia
- art. 89 r.o.d.o. - Zabezpieczenia i wyjątki mające zastosowanie do przetwarzania do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych
- art. 90 r.o.d.o. - Obowiązek zachowania tajemnicy
- art. 91 r.o.d.o. - Istniejące zasady ochrony danych obowiązujące kościoły i związki wyznaniowe
- por. też art. 23 r.o.d.o. zgodnie, z którym przepisy unijne oraz przepisy prawa krajowego mogą ograniczyć zakres obowiązków i praw przewidzianych w art. 12–22 i w art. 34, a także w art. 5.

# Zasady ogólne przetwarzania danych osobowych

Ogólne zasady dotyczące przetwarzania danych osobowych określa art. 5 RODO.

Katalog zasad ogólnych obejmuje:

- zasadę zgodność z prawem, rzetelność i przejrzystość;
- zasadę ograniczenia celu;
- zasadę adekwatności ("minimalizacji danych");
- zasadę prawidłowości;
- zasadę ograniczonego czasu ("ograniczenie przechowywania");
- zasadę zapewnienia odpowiedniego bezpieczeństwa ("integralność i poufność");
- zasadę rozliczalności.

Zasady ogólne ochrony danych osobowych, sformułowane w RODO mają charakter normatywny.

- W literaturze wskazuje się, że zasady ogólne wynikające z art. 5 RODO mają charakter podstawowy dla całej regulacji rozporządzenia.

  P. Drobek, *Komentarz do art. 5 „Zasady dotyczące przetwarzania danych osobowych"* [w:] *Ogólne rozporządzenie o ochronie danych. Komentarz*, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2018, s. 324.

- Zasady mają nadrzędną moc w stosunku do pozostałych przepisów o ochronie danych osobowych.

  P. Drobek, *tamże*. Por. też P. Fajgielski, *Zasady ogólne przetwarzania i ochrony danych osobowych* [w:] *Prawna ochrona danych osobowych w Polsce na tle europejskich standardów. X-lecie polskiej ustawy o ochronie danych osobowych*, red. G. Goździewicz, M. Szabłowska, Toruń 2008, s. 17.

- Zasady ogólne należy traktować jako dyrektywy interpretacyjne, służące do dokonywania wykładni poszczególnych przepisów rozporządzenia.

  T. A. J. Banyś, *Zasady prawa ochrony danych osobowych* [w:] *Prawo ochrony danych osobowych. Podręcznik dla studentów i praktyków*, T. A. J. Banyś, E. Bielak-Jomaa, M. Kuba, J. Łuczak, Warszawa 2016, s. 22; P. Drobek, *Zasada celowości w dobie wielkich zbiorów danych (big data)*, M. Praw 2014, nr 9, dodatek, s. 22; P. Fajgielski, *Zasady ogólne przetwarzania* …, s. 17.

### (1) Zasada zgodności z prawem, rzetelności i przejrzystości

- Dane osobowe muszą być przetwarzane **zgodnie z prawem, rzetelnie i w sposób przejrzysty** dla osoby, której dane dotyczą ("zgodność z prawem, rzetelność i przejrzystość") [art. 5 ust. 1 lit. a].

- Obowiązkiem wyjściowym administratora danych jest przetwarzane danych zgodnie z prawem, tj. zgodnie nie tylko z postanowieniami u.o.d.o., ale i w sposób nie naruszający innych przepisów.
- Wynikająca z art. 5 ust. 1 lit a r.o.d.o. ogólna zasada przejrzystości przetwarzania danych doznaje rozwinięcia i konkretyzacji w art. 12 r.o.d.o.
- Zgodnie z art. 12 ust. 1 r.o.d.o. 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) Zasada związania celem**

- Dane osobowe muszą być przetwarzane 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") [art. 5 ust. 1 lit. b].

  [zob. art. 6 ust. 4 RODO]

- Zgodnie z art. 11 ust. 1 RODO 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. [dodatkowo por. 11 ust. 1 RODO dot. przekazywania dodatkowych danych w celu identyfikacji na potrzeby realizacji art. 15-20 RODO]

**(3) Zasada ograniczenia czasowego**

- Dane osobowe muszą być 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").

  [art. 5 ust. 1 lit. e]

## (4) Zasada adekwatności danych

- Dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane ("minimalizacja danych") [art. 5 ust. 1 lit. c].


PRZYKŁADY SPRAW

*Stanowisko GIODO w sprawie art. 21 § 1 k.p.k.*

Zgodnie z art. 21 § 1 k.p.k. o ukończeniu postępowania toczącego się z urzędu przeciw osobom zatrudnionym w instytucjach państwowych, samorządowych i społecznych, uczniom i słuchaczom szkół oraz żołnierzom należy bezzwłocznie zawiadomić przełożonych tych osób. Przepis ten nakłada na sąd, przed którym postępowanie zostało zakończone, obowiązek przekazania informacji w tej sprawie lecz nie precyzuje zakresu danych, które mają być przekazane.

W kwestii tej należy kierować się m.in. zasadą adekwatności.

Celem zawiadomienia wskazanego w art. 21 § 1 k.p.k. jest przekazanie pracodawcy informacji, na podstawie których będzie on w stanie stwierdzić, czy w związku z zakończeniem postępowania zasadne jest podejmowanie w stosunku do pracownika określonych kroków (takich jak np. ukaranie go lub rozwiązanie z nim umowy o pracę).
W ocenie GIODO, przekazanie pracodawcy takich informacji o sposobie zakończenia postępowania, jak kwalifikacja prawna czynu, za który pracownik został skazany, wymierzona kara oraz data uprawomocnienia się orzeczenia nie wykraczają poza zakres niezbędny do zrealizowania celu, jakiemu przetwarzanie danych ma służyć.

**(5) Zasada poprawności danych**

- Dane osobowe muszą być 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"). [art. 5 ust. 1 lit. d]

**(6) Zasada odpowiedniego zabezpieczenia danych**

- Dane osobowe muszą być 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"). [art. 5 ust. 1 lit. f]

**(7) Zasada rozliczalności**

- Administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie ("rozliczalność"). [art. 5 ust. 2] *[por. np. art. 7 ust. 1 dot. zgody]*

# Przesłanki legitymizujące przetwarzanie danych osobowych

## Przesłanki legitymizujące przetwarzanie danych osobowych

Przepisy RODO enumeratywnie określają **przesłanki warunkujące dopuszczalność przetwarzania danych osobowych.**

Administrator danych powinien wykazać się co najmniej jedną z przesłanek legitymizujących przetwarzanie danych osobowych, aby jego działanie polegające na przetwarzaniu danych w danej formie mogło być uznane za zgodne z prawem.


Przesłanki przetwarzania danych zwykłych, co do zasady, reguluje art. 6 r.o.d.o., zaś danych szczególnych art. 9.

### Artykuł 6 r.o.d.o. - 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.

Akapit pierwszy lit. f) nie ma zastosowania do przetwarzania, którego dokonują organy publiczne w ramach realizacji swoich zadań.

## Przesłanki przetwarzania danych zwykłych

### ① Przesłanka zgody

- Przetwarzanie jest zgodne z prawem, gdy osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów.

[art. 6 ust. 1 lit a RODO]

- Definicja zgody z art. 4 pkt 11 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.
- artykuł 7 RODO - Warunki wyrażenia zgody (zob. uregulowania dot. **możliwości cofnięcia zgody**).

- **Kryterium dobrowolności zgody**
- Dobrowolność zgody oznacza możliwość rzeczywistego wyboru; zgoda nie może być wymuszona; zgoda nie może być uznana za dobrowolną, jeżeli osoba, której dane dotyczą, nie ma możliwości odmówienia lub wycofania swojej zgody bez niekorzystnych konsekwencji (por. opinie w sprawie zgody WP187 oraz WP 259);

*Wymóg odrębności zgód na różne cele*

- „Jeżeli administrator połączył kilka celów przetwarzania i nie próbował uzyskać odrębnej zgody dla każdego celu, nie ma dobrowolności. Ta szczegółowość jest ściśle powiązana z koniecznością, aby zgoda była konkretna" - opinia WP 259.
- Motyw 43 RODO: […] Zgody nie uważa się za dobrowolną, jeżeli nie można jej wyrazić z osobna na różne operacje przetwarzania danych osobowych, mimo że w danym przypadku byłoby to stosowne […].
- Motyw 32 RODO: […] Zgoda powinna dotyczyć wszystkich czynności przetwarzania dokonywanych w tym samym celu lub w tych samych celach. Jeżeli przetwarzanie służy różnym celom, potrzebna jest zgoda na wszystkie te cele. […].

*Brak uwarunkowania realizacji umowy lub usługi wyrażeniem zgody*

- Art. 7 ust. 4 RODO: 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.

- Art. 7 ust. 4 RODO ma na celu zapewnienie, że cel przetwarzania danych osobowych nie będzie ukryty ani połączony z realizacją umowy lub usługi, do czego dane osobowe nie są konieczne. (opinia WP259)
- Niezbędność musi być interpretowana ściśle. Przetwarzanie musi być niezbędne do wypełnienia umowy z każdą indywidualną osobą, której dane dotyczą. (opinia WP259).
- Motyw 43 r.o.d.o.: […] Zgody nie uważa się za dobrowolną, jeżeli […] jeżeli od zgody uzależnione jest wykonanie umowy - w tym świadczenie usługi - mimo że do jej wykonania zgoda nie jest niezbędna.

*Niemożność odmowy lub wycofania zgody bez niekorzystnych konsekwencji jako sytuacja wyłączająca dobrowolność*:

- Motyw 42 RODO: „[…] Wyrażenia zgody nie należy uznawać za dobrowolne, jeżeli osoba, której dane dotyczą, nie ma rzeczywistego lub wolnego wyboru oraz nie może odmówić ani wycofać zgody bez niekorzystnych konsekwencji."

*Brak równowagi jako sytuacja wyłączająca dobrowolność:*

- Aby zapewnić dobrowolność, zgoda nie powinna stanowić ważnej podstawy prawnej przetwarzania danych osobowych w szczególnej sytuacji, w której istnieje wyraźny brak równowagi między osobą, której dane dotyczą, a administratorem, w szczególności gdy administrator jest organem publicznym i dlatego jest mało prawdopodobne, by w tej konkretnej sytuacji zgodę wyrażono dobrowolnie we wszystkich przypadkach […]. [motyw 43 RODO].
- Sytuacja braku równowagi w szczególności może występować w odniesieniu do organów publicznych oraz pracodawcy.

- **Kryterium konkretności zgody**

- **Konkretność okazania zgody** oznacza przede wszystkim określać precyzyjnie cel przetwarzania danych oraz wskazywać zakres danych (por. brzmienie art. 6 ust. 1 lit a). Niedopuszczalne jest zbieranie zgód blankietowych. Należy też wyraźnie oddzielić informacje związane z uzyskaniem zgody od informacji dotyczących innych kwestii.

- Zgodnie z zasadą związania celem (ograniczenia celu) dane osobowe muszą być przetwarzane zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami […] - art. 5 ust. 1 lit. b RODO.
- „Wymóg, że zgoda musi być `konkretna` ma na celu zapewnienie stopnia kontroli użytkownika oraz przejrzystości dla osoby, której dane dotyczą. Wymóg ten nie został zmieniony przez RODO i nadal jest ściśle związany z wymogiem `szczegółowości' w celu uzyskania `dobrowolnej` zgody." – opinia WP259.

- Art. 7 ust. 2 r.o.d.o.: 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.

- Por. motywy 32 i 43 RODO.

- Patrz też opinia GR Art. 29 3/2013 w sprawie ograniczenia celu (WP203)

- **Kryterium świadomości zgody**

- Kryterium świadomości zgody wiąże się z wymogiem przekazania niezbędnych informacji osobom, których dane dotyczą, aby umożliwić im podejmowanie świadomych decyzji i zrozumienie, na co wyrażają zgodę. Kryterium te wiąże się ściśle z zasadą przejrzystości.
- Zdaniem GR Art. 29 (opinia WP 259, s. 16-17) aby zgoda była świadoma, wymagane jest podanie co najmniej następujących informacji:
- tożsamość administratora,
- cel każdej operacji przetwarzania, dla której prosi się o zgodę,
- zakres przetwarzanych danych,
- istnienie prawa do wycofania zgody,
- *informacje na temat wykorzystywania danych do decyzji opartych jedynie na zautomatyzowanym przetwarzaniu, w tym profilowaniu (zgodnie z artykułem 22 ust. 2),*
- *jeżeli zgoda dotyczy przekazywania – informacje na temat możliwych zagrożeń związanych z przekazywaniem danych do krajów trzecich w przypadku braku decyzji stwierdzającej odpowiedni stopień ochrony oraz odpowiednich zabezpieczeń.*

- W przypadku, gdy na wnioskowanej zgodzie ma bazować wielu (wspólnych) administratorów lub gdy dane mają być przekazane innym administratorom lub przetwarzane przez innych administratorów, którzy chcą polegać na pierwotnej zgodzie, wszystkie te organizacje powinny być wymienione. (opinia WP 259, s. 17)

- W ramach wymogów zgody nie trzeba wymieniać przetwarzających, aczkolwiek w celu zapewnienia zgodności z artykułami 13 i 14 RODO administratorzy będą musieli przedstawić pełną listę odbiorców lub kategorii odbiorców, w tym przetwarzających. (opinia WP 259, s. 17)

- **Kryterium jednoznaczności zgody**

- Jednoznaczność zgody oznacza, że ważna zgoda wymaga jednoznacznego okazania w formie oświadczenia lub wyraźnego działania potwierdzającego, co oznacza, że osoba, której dane dotyczą, musi podjąć celowe działanie w celu wyrażenia zgody na określone przetwarzanie.
- „Wyraźnie działanie potwierdzające" oznacza, że osoba, której dane dotyczą, musiała podjąć celowe działanie w celu wyrażenia zgody na określone przetwarzanie. (opinia WP259, s. 20)
- „zgoda nie może być uzyskana poprzez takie samo działanie jak zgoda na umowę lub akceptacja ogólnych warunków usługi. Ukryta akceptacja ogólnych warunków nie może być uznana za jasne działanie potwierdzające w celu wyrażenia zgody na wykorzystywanie danych osobowych. (opinia WP 259, s. 20-21)

- Motyw 32 RODO: […] Milczenie, okienka domyślnie zaznaczone lub niepodjęcie działania nie powinny zatem oznaczać zgody. […]

**Wymóg uzyskania zgody wyraźnej**

Konieczność uzyskania zgody „wyraźniej" wiążę się z przetwarzaniem danych szczególnych (art. 9), przekazywaniem danych do państw trzecich lub organizacji międzynarodowych w przypadku braku odpowiednich zabezpieczeń (art. 49), zautomatyzowanego podejmowania decyzji (art. 22).

„RODO przewiduje, że `wyraźne potwierdzające działanie` jest warunkiem wstępnym `zwykłej` zgody. […] Termin *wyraźna* odnosi się do sposobu, w jaki zgoda jest wyrażona przez osobę, której dane dotyczą. Oznacza to, że osoba, której dane dotyczą, musi wyrazić oświadczenie zgody.„ – z opinii WP259, s. 23.

RODO nie przewiduje wymogu pisemnego oświadczenia woli w odniesieniu do zgody „wyraźniej".

*Z orzecznictwa (u.o.d.o. z 1997):*

- *„Zgoda musi mieć charakter wyraźny, a jej wszystkie aspekty muszą być jasne dla podpisującego w momencie jej wyrażania. Czynności takiej nie konwaliduje późniejsze poinformowanie o treści regulaminu ani możliwość zgłoszenia zastrzeżeń wobec pewnych form przetwarzania danych."* - wyrok NSA z 4 kwietnia 2003 r., II SA 2135/02
- *„Zgoda na przetwarzanie danych osobowych musi być wyraźna. Nie spełnia tego wymagania podpisanie oświadczenia o wyrażeniu zgody na przetwarzanie danych, stanowiącego dodatkowy element innego zobowiązania niezawierającego informacji o celach i zakresie przetwarzania tych danych."* - wyrok NSA z 4 kwietnia 2003 r., II SA 2135/02
- *„Zgoda na przetwarzanie danych osobowych musi być sformułowana w sposób wyraźny i jednoznaczny i wyróżniać się spośród innych pochodzących od tej osoby informacji i oświadczeń. Nie może mieć charakteru abstrakcyjnego, lecz powinna odnosić się do skonkretyzowanego stanu faktycznego, obejmując tylko określone dane oraz sprecyzowany sposób i cel ich przetwarzania. […] Dlatego też w przypadku oświadczenia woli dotyczącego **różnych celów** przetwarzania, np. celu przynależności do klubu czy przekazywania przesyłek reklamowych innych firm, **zgoda powinna być wyrażona wyraźnie pod każdym z tych celów przetwarzania**."* - wyrok NSA z 11 kwietnia 2003 r., II SA 3942/02; por. też wyrok NSA z 10 stycznia 2013, I OSK 2029/11

*Zapis o zgodzie jako klauzula niedozwolona (u.o.d.o.):*

Do rejestru niedozwolonych klauzul wpisane są zapisy, w których klient nieświadomie wyraża zgodę na przetwarzanie danych osobowych w celach niezwiązanych z realizacją zawieranej umowy.

Do rejestru wpisano klauzule, w których klient akceptując regulamin jednocześnie zgadza się na przetwarzanie danych w innych celach, np. w celach marketingowych.

Numer wpisu 3522, data wpisu 06.08.2012: *Udostępnione dane osobowe będą przechowywane w bazie danych administratora i będą wykorzystywane w celu prawidłowej realizacji umowy sprzedaży oraz w celach marketingowych w szczególności w celu informowania o nowych produktach, usługach oraz promocjach oferowanych przez sklep.*

**Wycofanie zgody**

- Zgodnie z art. 7 ust. 3 r.o.d.o.: 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.

- Zgodnie z art. 7 ust. 3 zd. 3 RODO osoba, której dane dotyczą, musi zostać poinformowana o prawie do wycofania zgody w dowolnym momencie, zanim wyrazi zgodę. Por. też art. 13 ust. 2 lit. c) RODO. Obowiązek poinformowania o prawie do wycofania zgody ma charakter szczególny, gdyż został sformułowany w artykule regulującym „warunki wyrażenia zgody".
- W art. 7 ust. 3 RODO wyraźnie sformułowana została konieczność zapewnienia tego, aby wycofanie zgody było równie łatwe, jak jej wyrażenie. Oznacza to, że jeśli zgoda była pozyskana przy użyciu interfejsu użytkownika (na przykład za pośrednictwem strony internetowej, aplikacji, strony logowania, poczty elektronicznej), jej odwołanie powinno być możliwe za pomocą tego samego interfejsu elektronicznego.

**Zasada rozliczalności w odniesieniu do zgody (wykazanie zgody)**

Zasadę rozliczalności konstytuuje art. 5 ust. 2 r.o.d.o., zgodnie z nią administrator musi być w stanie wykazać przestrzeganie przepisów regulujących ochronę danych osobowych.

Zgodnie z art. 7 ust. 1 r.o.d.o.: 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.**

„Dopóki dane są przetwarzane, istnieje obowiązek wykazania prawidłowo wyrażonej zgody. Po zakończeniu czynności przetwarzania, dowód na wyrażenie zgody nie powinien być przechowywany dłużej niż jest to wymagane do wywiązania się z obowiązku prawnego, ustalenia, dochodzenia lub obrony roszczeń, zgodnie z art. 17 ust. 3b i 3e)." – z opinii WP259, s. 25.

„Administrator danych musi również być w stanie wykazać, że osoba, której dane dotyczą, była poinformowana, a procedura zastosowana przez administratora spełnia wszystkie istotne kryteria dotyczące ważnej zgody." – z opinii WP259, s. 25.

***Przykład klauzuli zgody na przetwarzanie danych osobowych dla celów marketingowych***

Niniejszy wyrażam zgodę na przetwarzanie moich danych osobowych [zawartych w ……] / [obejmujących …] przez [nazwa i adres podmiotu] z siedzibą ……., jako administratora danych, w celu marketingu produktów i usług …….. [np. własnych / nazwa podmiotu] zgodnie z przepisami o ochronie danych osobowych.
Jednocześnie oświadczam, że dane podałem dobrowolnie i zapoznałem się z informacjami, o których mowa w art. 13 ogólnego rozporządzenia o ochronie danych osobowych oraz przyjmuję do wiadomości, że przysługuje mi prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem.

**Treść powyższej klauzuli nie stanowi wypełnienia obowiązków informacyjnych z art. 13 r.o.d.o. - informacje te muszą być podane osobie wyrażającej zgodę**

***Klauzula zgody na przesyłanie informacji handlowej***

Zgodnie z art. 10 u.s.u.d.e. zakazane jest przesyłanie niezamówionej informacji handlowej skierowanej do oznaczonego odbiorcy będącego osobą fizyczną za pomocą środków komunikacji elektronicznej, w szczególności poczty elektronicznej. Informację handlową uważa się za zamówioną, jeżeli odbiorca wyraził zgodę na otrzymywanie takiej informacji, w szczególności udostępnił w tym celu identyfikujący go adres elektroniczny.

*informacja handlowa - każdą informację przeznaczoną bezpośrednio lub pośrednio do promowania towarów, usług lub wizerunku przedsiębiorcy lub osoby wykonującej zawód, której prawo do wykonywania zawodu jest uzależnione od spełnienia wymagań określonych w odrębnych ustawach, z wyłączeniem informacji umożliwiającej porozumiewanie się za pomocą środków komunikacji elektronicznej z określoną osobą oraz informacji o towarach i usługach niesłużącej osiągnięciu efektu handlowego pożądanego przez podmiot, który zleca jej rozpowszechnianie, w szczególności bez wynagrodzenia lub innych korzyści od producentów, sprzedawców i świadczących usługi*

W wyrok z 31 stycznia 2012 r., I OSK 1317/11 Naczelny Sąd Administracyjny stanął na stanowisku, że zgodę na wysyłanie informacji handlowej drogą elektroniczną (wyrażaną na podstawie u.s.u.d.e.) należy wyodrębnić od zgody na przetwarzanie danych w celach marketingowych.

Por. też stanowisko GIODO: http://www.giodo.gov.pl/pl/259/10003

*Przykładowa klauzula:*

Wyrażam zgodę na przesyłanie środkami komunikacji elektronicznej informacji handlowej, na podany przeze mnie adres poczty elektronicznej przez _____ [nazwa i adres podmiotu]

Wyrażam zgodę na otrzymywanie na mój adres poczty elektronicznej informacji handlowych przesyłanych środkami komunikacji elektronicznej przez _____ [nazwa i adres podmiotu]

… *i wykorzystywanie w tym zakresie dla celów marketingu bezpośredniego telekomunikacyjnych urządzeń końcowych, których jestem użytkownikiem.*

***Klauzula zgody telekomunikacyjnej***

Zakazane jest używanie telekomunikacyjnych urządzeń końcowych i automatycznych systemów wywołujących dla celów marketingu bezpośredniego, chyba że abonent lub użytkownik końcowy uprzednio wyraził na to zgodę (art. 172 PT).

*Telekomunikacyjnymi urządzeniami końcowymi są urządzenie telekomunikacyjne przeznaczone do podłączenia bezpośrednio lub pośrednio do zakończeń sieci. Zatem urządzeniami telekomunikacyjnymi mogą być: telefony stacjonarne, telefony komórkowe, tablety, faksy, komputery.*

*Przykładowe klauzule:*

Wyrażam zgodę na używanie przez [nazwa i adres podmiotu] telekomunikacyjnych urządzeń końcowych, których jestem użytkownikiem, dla celów marketingu bezpośredniego zgodnie z art. 172 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne.

Wyrażam zgodę na używanie przez [nazwa i adres podmiotu] telekomunikacyjnych urządzeń końcowych, których jestem użytkownikiem i otrzymywanie telefonicznych połączeń przychodzących w celach marketingu bezpośredniego zgodnie z art. 172 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne.

**Problem ważności zgód zebranych przed wejściem w życie r.o.d.o.**

- Zgoda, która została pozyskana na gruncie obowiązywania starej u.o.d.o., jest nadal ważna, jeżeli jest zgodna z warunkami ważności zgody określonymi w ogólnym rozporządzeniu o ochronie danych osobowych.
- Motyw 171 r.o.d.o.: *„jeżeli przetwarzanie ma za podstawę zgodę w myśl dyrektywy 95/46/WE, osoba, której dane dotyczą, nie musi ponownie wyrażać zgody, jeżeli pierwotny sposób jej wyrażenia odpowiada warunkom niniejszego rozporządzenia; dzięki temu administrator może kontynuować przetwarzanie po dacie rozpoczęcia stosowania niniejszego rozporządzenia”.*
- Aby zgody zebrane uprzednio zachowały ważność, muszą spełniać kryteria dobrowolności, konkretności, świadomości i jednoznaczności. Ponadto przepis określający warunki wyrażenia zgody nakłada na administratora obowiązek poinformowania osoby, której dane dotyczą, o możliwości odwołania zgody, zanim ta zgoda zostanie wyrażona – również to kryterium warunkuje ważność uprzednio zebranych zgód.
- W ostatnich Wytycznych Grupy Roboczej Art. 29 dotyczących zgody (WP 259) wskazano, że art. 13 ust. 2 RODO należy rozumieć w sposób, który nie wyklucza ważności zebranych zgód w sytuacji kiedy nie wszystkie informacje określone w tym przepisie zostały przekazane osobie, której dane dotyczą w momencie pozyskiwania zgody. *„Jako że nie wszystkie elementy wymienione w artykułach 13 i 14 muszą zawsze występować jako warunek świadomej zgody, rozszerzone obowiązki informacyjne na mocy RODO niekoniecznie przeciwstawiają się ciągłości zgody wyrażonej przed wejściem w życie RODO”.*

**Artykuł 8 RODO**

**Warunki wyrażenia zgody przez dziecko w przypadku usług społeczeństwa informacyjnego**

1. Jeżeli zastosowanie ma art. 6 ust. 1 lit. a), w przypadku usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku, zgodne z prawem jest przetwarzanie danych osobowych dziecka, które ukończyło 16 lat. Jeżeli dziecko nie ukończyło 16 lat, takie przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy zgodę wyraziła lub zaaprobowała ją osoba sprawująca władzę rodzicielską lub opiekę nad dzieckiem oraz wyłącznie w zakresie wyrażonej zgody.

Państwa członkowskie mogą przewidzieć w swoim prawie niższą granicę wiekową, która musi wynosić co najmniej 13 lat.

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

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

② **Przesłanka niezbędności dla realizacji lub zawarcia umowy**

Przetwarzanie jest zgodne z prawem, gdy 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.
[art. 6 ust. 1 lit b RODO]

③ **Przesłanka niezbędności dla realizacji prawnego obowiązku**

Przetwarzanie jest zgodne z prawem, gdy jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze.
[art. 6 ust. 1 lit c RODO]
[ zob. też art. 6 ust. 3 RODO, por. też motyw 45 RODO]

④ **Przesłanka niezbędności do ochrony żywotnych interesów osoby**

Przetwarzanie jest zgodne z prawem, gdy jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej. [art. 6 ust. 1 lit d RODO]

- Motyw 46 RODO: Przetwarzanie danych osobowych należy uznać za zgodne z prawem również w przypadkach, gdy jest niezbędne do ochrony interesu, który ma istotne znaczenie dla życia osoby, której dane dotyczą, lub innej osoby fizycznej. Żywotny interes innej osoby fizycznej powinien zasadniczo być podstawą przetwarzania danych osobowych wyłącznie w przypadkach, gdy ewidentnie przetwarzania tego nie da się oprzeć na innej podstawie prawnej. Niektóre rodzaje przetwarzania mogą służyć zarówno ważnemu interesowi publicznemu, jak i żywotnym interesom osoby, której dane dotyczą, na przykład gdy przetwarzanie jest niezbędne do celów humanitarnych, w tym monitorowania epidemii i ich rozprzestrzeniania się lub w nadzwyczajnych sytuacjach humanitarnych, w szczególności w przypadku klęsk żywiołowych i katastrof spowodowanych przez człowieka.

### ⑤ Przesłanka wykonywania zadań publicznych

- Przetwarzanie jest zgodne z prawem, gdy jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.

[art. 6 ust. 1 lit e RODO]
[ zob. też art. 6 ust. 3 RODO, por też. motyw 45 RODO]

### ⑥ Przesłanka prawnie uzasadnionego celu (usprawiedliwionego celu)

- Przetwarzanie jest zgodne z prawem, gdy 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.

[art. 6 ust. 1 lit f RODO]

Akapit pierwszy lit. f) nie ma zastosowania do przetwarzania, którego dokonują organy publiczne w ramach realizacji swoich zadań.

Art. 51 ust. 2 Konstytucji RP: Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym.

- Podstawa ta ma charakter dopełniający w stosunku do pozostałych przesłanek przetwarzania danych, przesłanka ta jest wypełniona jeśli:

a) przetwarzanie danych jest niezbędne do wypełnienia celu wynikającego z prawnie uzasadnionych interesów administratora danych lub odbiorcy danych;

b) powyższy interes jest nadrzędny w stosunku do interesów lub podstawowych praw i wolności osoby, której dane dotyczą.

- Na gruncie tej przesłanki zachodzi konieczność wyważania interesów dwóch stron – z jednej uzasadnionego interesu administratora danych (lub odbiorcy danych), a z drugiej, interesów lub podstawowych praw i wolności osoby, której dane dotyczą.

*Na gruncie starej u.o.d.o. „wyważenie tych interesów jest warunkiem koniecznym przy stosowaniu art. 23 […], z uwzględnieniem rangi tych interesów w realiach konkretnej sprawy*" – wyrok NSA z 6 VI 2001 r., I OPS 2/05. (na grucie u.o.d.o.)

a)

- cel, który zamierza osiągnąć administrator nie może być sprzeczny z prawem, przy czym nie oznacza to, że musi mieć podstawę w szczególnym przepisie prawa.
- uzasadniony cel powinien się mieścić w ramach prowadzonej działalności, tj. cel ten zasadniczo powinien mieć jakieś uzasadnienie: prawne, gospodarcze, społeczne, czy organizacyjne.
- powołanie się na tę przesłankę możliwe, w zakresie w jakim wykorzystywanie danych jest konieczne dla osiągnięcia oznaczonego celu (→ zasada adekwatności).

b)

- przyjmuje się, że przez pojęcie podstawowych praw i wolności w rozumieniu tego przepisu chodzi o prawa chronione na podstawie norm kształtujących podstawowe zasady funkcjonowania jednostki w społeczeństwie, znajdujących swoje źródła przede wszystkim w normach konstytucyjnych oraz konwencjach międzynarodowych w szczególności odnoszących się do wolności i praw osobistych (dotyczących ochrony prywatności, życia rodzinnego, dobrego imienia, decydowania o swoim życiu, tajemnicy komunikowania itp.) oraz odnoszących się do wolności i praw politycznych oraz ekonomicznych.

PRZYKŁAD – dochodzenie roszczeń

Za prawnie usprawiedliwiony cel uważa się w szczególności dochodzenie roszczeń z tytułu prowadzonej działalności gospodarczej.

Stanowisko GIODO (na gruncie u.o.d.o.):
Skoro spółka poniosła szkodę wyrządzoną jej przez skazanych (która nie została przez nich naprawiona w ustalonym przez sąd terminie) i na podstawie sądowego tytułu egzekucyjnego jest uprawniona do dochodzenia swej wierzytelności na drodze egzekucji komorniczej, to do jej wszczęcia niezbędne jest wskazanie adresów zamieszkania skazanych. Sąd, jako administrator danych zawartych w aktach sprawy, powinien udostępnić dane adresowe skazanych zawartych w aktach sprawy, na podstawie art. 23 ust. 1 pkt 5, gdyż dane te są spółce niezbędne do dochodzenia roszczeń związanych z jej działalnością gospodarczą.
Aby spółka mogła skorzystać z przysługującego jej prawa do dochodzenia swoich roszczeń musi posiadać dane osobowe dłużników. Niezbędnym bowiem elementem do wszczęcia egzekucji wobec dłużnika jest oznaczenie miejsca jego zamieszkania.

- Motyw 47 RODO: Podstawą prawną przetwarzania mogą być prawnie uzasadnione interesy administratora, w tym administratora, któremu mogą zostać ujawnione dane osobowe, lub strony trzeciej, o ile w świetle rozsądnych oczekiwań osób, których dane dotyczą, opartych na ich powiązaniach z administratorem nadrzędne nie są interesy lub podstawowe prawa i wolności osoby, której dane dotyczą. Taki prawnie uzasadniony interes może istnieć na przykład w przypadkach, gdy zachodzi istotny i odpowiedni rodzaj powiązania między osobą, której dane dotyczą, a administratorem, na przykład gdy osoba, której dane dotyczą, jest klientem administratora lub działa na jego rzecz. Aby stwierdzić istnienie prawnie uzasadnionego interesu, należałoby w każdym przypadku przeprowadzić dokładną ocenę, w tym ocenę tego, czy w czasie i w kontekście, w którym zbierane są dane osobowe, osoba, której dane dotyczą, ma rozsądne przesłanki by spodziewać się, że może nastąpić przetwarzanie danych w tym celu. Interesy i prawa podstawowe osoby, której dane dotyczą, mogą być nadrzędne wobec interesu administratora danych w szczególności w przypadkach, gdy dane osobowe są przetwarzane w sytuacji, w której osoby, których dane dotyczą, nie mają rozsądnych przesłanek, by spodziewać się dalszego przetwarzania. Ponieważ dla organów publicznych podstawę prawną przetwarzania danych osobowych powinien określić ustawodawca, prawnie uzasadniony interes administratora nie powinien mieć zastosowania jako podstawa prawna do przetwarzania, którego dokonują organy publiczne w ramach realizacji swoich zadań. Prawnie uzasadnionym interesem administratora, którego sprawa dotyczy, jest również przetwarzanie danych osobowych bezwzględnie niezbędne do zapobiegania oszustwom. Za działanie wykonywane w prawnie uzasadnionym interesie można uznać przetwarzanie danych osobowych do celów **marketingu bezpośredniego**.

***Delegacja do ustanowienia szczegółowych regulacji w państwach członkowskich***

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

**Przesłanki przetwarzania danych szczególnych (sensytywnych)**

- Zgodnie z art. 9 RODO („Przetwarzanie szczególnych kategorii danych osobowych") ust. 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."
- Art. 9 ust. 2 RODO określa **wyjątki od zakazu**.
- Zgodnie z art. 9 ust. 4 RODO państwa członkowskie mogą zachować lub wprowadzić dalsze warunki, w tym ograniczenia w odniesieniu do przetwarzania danych genetycznych, danych biometrycznych lub danych dotyczących zdrowia.

Wyjątki od zakazu

Przetwarzanie szczególnych kategorii danych osobowych określonych w art. 9 ust. 1 jest dopuszczane w następujących przypadkach:

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

b) przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem Unii lub prawem państwa członkowskiego, lub porozumieniem zbiorowym na mocy prawa państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą;

c) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody;

[…]

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

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

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

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

[…]

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

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

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.

## Pozostałe uregulowania RODO dotyczące szczególnych sytuacji przetwarzania danych

- **Art. 10 RODO dot. przetwarzanie danych osobowych dotyczących wyroków skazujących i naruszeń prawa**

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

- **Art. 44 – 50 (rozdział V RODO) - przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych**

Przepisy rozdziału IX RODO odnoszą się do przepisów dotyczących szczególnych sytuacji związanych z przetwarzaniem:

- Art. 85 RODO – przetwarzanie a wolność wypowiedzi i informacji
  *[możliwe uregulowania szczególne dla przetwarzania do celów dziennikarskich lub do celów wypowiedzi akademickiej, artystycznej lub literackiej]*
- Art. 86 RODO - przetwarzanie a publiczny dostęp do dokumentów urzędowych
  *[konieczność pogodzenia publicznego dostępu do dokumentów urzędowych z prawem do ochrony danych osobowych na mocy RODO]*
- Art. 87 RODO - przetwarzanie krajowego numeru identyfikacyjnego
- Art. 89 RODO – dot. przetwarzania do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych
- Art. 88 RODO - dot. przyjmowania przepisów regulujących przetwarzanie w kontekście zatrudnienia
- Art. 91 RODO – dot. istniejących w państwach członkowskich zasad ochrony danych obowiązujących kościoły i związki wyznaniowe

# Prawa osób, których dane są przetwarzane

Prawa osób, których dane są przetwarzane uregulowane są w rozdziale III RODO (art. 12 – 23 RODO).

**Ogólne wymogi dotyczące informowania i komunikacji z podmiotami danych**

- Artykuł 12 **(Przejrzyste informowanie i przejrzysta komunikacja oraz tryb wykonywania praw przez osobę, której dane dotyczą)** formułuje ogólne wymogi dotyczące informowania i komunikacji z podmiotami danych
- 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. [art. 12 ust. 1 RODO]
- Administrator ułatwia osobie, której dane dotyczą, wykonanie praw przysługujących jej na mocy art. 15-22 […]. [art. 12 ust. 2 RODO]

*Istota i funkcje zasady*

- „dysponowanie odpowiednim zasobem informacji przez osoby, których dane dotyczą, jest warunkiem niezbędnym sprawowania faktycznej kontroli nad tym, kto, kiedy, w jaki sposób i w jakim celu pozyskuje informacje na ich temat, zmniejsza ryzyko nadużyć ze strony administratorów, a także pozwala na realne korzystanie z narzędzi ochrony" - J. Łuczak, *Komentarz do art. 12 „Przejrzyste informowanie i przejrzysta komunikacja oraz tryb wykonywania praw przez osobę, której dane dotyczą"* [w:] *Ogólne rozporządzenie o ochronie danych. Komentarz*, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2018, s. 467.
- Z motywu 39 RODO wynika, że jednostka powinna zawsze mieć jasność, co do tego, że dochodzi do zbierania ich danych osobowych, oraz iż dane te będą następnie wykorzystywane, a także co do tego w jakim stopniu te dane osobowe będą przetwarzane. W motywie tym podkreślono, że przejrzystość wymaga, by wszelkie informacje i wszelkie komunikaty związane z przetwarzaniem danych osobowych były łatwo dostępne i zrozumiałe oraz sformułowane jasnym i prostym językiem. W szczególności zaś osobom fizycznym, których dane są przetwarzane należy uświadomić ryzyka, zasady, zabezpieczenia i prawa związane z przetwarzaniem danych osobowych oraz sposoby wykonywania praw przysługujących im w związku z takim przetwarzaniem.

- Ustanowione w art. 12 ust. 1 r.o.d.o. wymogi należy traktować jako ogólną dyrektywę mająca zastosowania do formułowania przez administratora informacji i komunikatów kierowanych do osób, których dane są przetwarzane. Przyjęte w r.o.d.o. podejście powoduje, że obowiązki informacyjne administratora danych nie mogą być postrzegane tylko i wyłącznie na **płaszczyźnie formalnej** lecz uzyskują istotny **aspekt materialny**. Sprowadza się on do wymogu podejmowania działań informacyjnych w taki sposób, aby mogły one skutecznie doprowadzić do nabycia świadomości przez podmiot danych co do samego faktu przetwarzania jego danych oraz zakresu, celu i innych istotnych elementów dotyczących dokonywanych operacji przetwarzania danych.

- W motywie 58 r.o.d.o. zaznaczone zostało, że zasada przejrzystości wymaga, by wszelkie informacje kierowane do ogółu społeczeństwa lub osoby, której dane dotyczą, były zwięzłe, łatwo dostępne i zrozumiałe, by były formułowane jasnym i prostym językiem, a w stosownych przypadkach, dodatkowo wizualizowane.
- Konstrukcja komunikatu, sposób formułowania treści oraz sposób samego przekazania wymaganych informacji powinien być dostosowany do specyfiki potencjalnych odbiorów komunikatu i powinien uwzględniać charakterystykę danego przejawu przetwarzania danych.

*Forma udzielenie informacji*

- 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. [art. 12 ust. 1 r.o.d.o.]
- Wybór sposobu sformułowania i przekazania informacji każdorazowo spoczywa na administratorze danych, przy czym musi on uwzględnić to aby środki podejmowane w celu realizacji obowiązków informacyjnych było „odpowiednie" do osiągnięcia rezultatów określonych w art. 12 ust. 1 r.o.d.o.
- Znaki graficzne: Informacje, których udzielane przez administratora danych w związku z gromadzeniem danych osobowych (art. 13-14 RODO) mogą być dodatkowo opatrzone standardowymi znakami graficznymi (art. 12 ust. 7 RODO). Znaki te w sposób widoczny, zrozumiały i czytelny mają przedstawiać sens zamierzonego przetwarzania danych. Posługiwanie się takim znakami graficznymi w komunikatach kierowanych do podmiotów danych ma w zamierzeniu pomóc w przejrzystym przekazaniu treści a zarazem ułatwić ich przyswajanie przez odbiorców. Dodać należy że Komisji Europejska ma prawo na podstawie art. 12 ust. 7 w zw. z art. 92 r.o.d.o. przyjmować akty delegowane w celu określenia informacji przedstawianych za pomocą znaków graficznych i procedur ustanowienia standardowych znaków graficznych.

*Terminy udzielenie informacji, o podejmowanych działaniach lub odmowie podjęcia działań*

- Administrator bez zbędnej zwłoki - a w każdym razie w terminie miesiąca od otrzymania żądania - udziela osobie, której dane dotyczą, informacji o działaniach podjętych w związku z żądaniem na podstawie art. 15-22. W razie potrzeby termin ten można przedłużyć o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań. W terminie miesiąca od otrzymania żądania administrator informuje osobę, której dane dotyczą o takim przedłużeniu terminu, z podaniem przyczyn opóźnienia. Jeśli osoba, której dane dotyczą, przekazała swoje żądanie elektronicznie, w miarę możliwości informacje także są przekazywane elektronicznie, chyba że osoba, której dane dotyczą, zażąda innej formy. [art. 12 ust. 3 RODO]
- Jeżeli administrator nie podejmuje działań w związku z żądaniem osoby, której dane dotyczą, to niezwłocznie - najpóźniej w terminie miesiąca od otrzymania żądania - informuje osobę, której dane dotyczą, o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem. [art. 12 ust. 4 RODO]

*Zasada nieodpłatnego udzielania informacji i prowadzenia komunikacji*

Informacje podawane na mocy art. 13 i 14 oraz komunikacja i działania podejmowane na mocy art. 15–22 i 34 są wolne od opłat.

Jeżeli żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, administrator może:

a) pobrać rozsądną opłatę, uwzględniając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań; albo
b) odmówić podjęcia działań w związku z żądaniem. […] [art. 12 ust. 5]

Podanie informacji wynikających z art. 13 i 14 RODO nie może być uwarunkowane żądaniem uiszczenia opłaty.

*Identyfikacja osoby realizującej prawa*

- Zgodnie z art. 12 ust. 6 jeżeli administrator ma uzasadnione wątpliwości co do tożsamości osoby fizycznej składającej żądanie, o którym mowa w art. 15-21, może zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby, której dane dotyczą.

- Z kolei zgodnie z art. 11 ust. 2 jeżeli 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.

**Prawo do informacji**

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

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

*Artykuł 15* **Prawo dostępu przysługujące osobie, której dane dotyczą**

*Zakres podawanych danych*

A. *Informacje podawane w przypadku zbierania danych od osoby, której dane dotyczą - Artykuł 13*
B. *Informacje podawane w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą - Artykuł 14*

- Administrator danych w związku z gromadzeniem danych zobowiązany jest przekazać podmiotowi danych następujące informacje:
  - dane identyfikacyjne administratora (obejmujące tożsamość i dane kontaktowe administratora);
  - dane identyfikacyjne przedstawiciela administratora, jeżeli administrator ma przedstawiciela;
  - dane kontaktowe inspektora ochrony danych w razie jego powołania (zakres podawanych danych nie obejmuje imienia i nazwiska inspektora);
  - **cele przetwarzania danych osobowych**;
  - **podstawę prawną przetwarzania** danych osobowych, a także jeżeli przetwarzanie odbywa się na podstawie klauzuli usprawiedliwionego celu (art. 6 ust. 1 lit. f r.o.d.o.) - **prawnie uzasadnione interesy** realizowane przez administratora lub przez stronę trzecią;
  - **okres**, przez który dane osobowe będą przechowywane, a gdy nie jest możliwe bezwzględne określenie tego okresu, kryteria jego ustalania;

- informacje o przysługujących podmiotowi danych prawach: o prawie do żądania od administratora dostępu do danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania; o prawie do przenoszenia danych; o prawie do cofnięcia zgody jeżeli przetwarzanie odbywa się na podstawie zgody; a także o prawie wniesienia skargi do organu nadzorczego;
- informacje o odbiorcach danych osobowych lub o kategoriach odbiorców (o ile istnieją jacyś odbiorcy);
- w razie takiego zamiaru informacje o przekazywaniu danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję Europejską odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi r.o.d.o., wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych;
- informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, oraz istotne informacje o zasadach podejmowania takich decyzji, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą. [obowiązek informowani o profilowaniu, dotyczy tylko profilowaniu w celu automatycznego podjęcia decyzji, o którym mowa w art. 24 ust. 1 i 4 r.o.d.o.]

- W przypadku zbierania danych **bezpośrednio** od osoby, której one dotyczą należy podać 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 (wymóg ten wynika z art. 13 ust. 2 lit. e r.o.d.o.).

- Natomiast w sytuacji, w której dane są zbierane **niebezpośrednio** od osoby, której dane dotyczą należy podać kategorie odnośnych danych osobowych (art. 14 ust. 1 lit d r.o.d.o.) oraz źródło pochodzenia danych osobowych, a gdy ma to zastosowanie - czy pochodzą one ze źródeł publicznie dostępnych (art. 14 ust. 2 lit f r.o.d.o.).
- *„Firma, która nabyła zbiór danych osobowych od innego administratora danych, powinna powiadomić klientów, że posiada ich dane, oraz dać im czas, aby mieli szansę wnieść sprzeciw na ich przetwarzanie do celów marketingowych. Niedotrzymanie tych warunków łamie przepisy o ochronie danych osobowych."* [wyrok WSA w Warszawie z dnia 22 stycznia 2004 r., II SA 2665/2002]

- Zakres informacji podawanych w związku ze zbieraniem danych osobowych jest niezależny od tego jakie kategorie danych są zbierane, ani od tego w jakich celach mają być przetwarzane, ani też od formy w jakiej przekazanie informacji następuje.

- Doprecyzowanie obowiązków informacyjnych, w pewnym zakresie, może zostać doprecyzowane w kodeksach postępowania (art. 40 ust. 2)

- Osobie, której dane dotyczą, poza informacjami wskazanymi w art. 13 i 14 RODO administrator, w określonych przypadkach, przekazuje również i inne informacje, np. o wiążących regułach korporacyjnych (art. 47 ust. 2 lit g dot. przekazywania danych do państw trzecich).

*Wyjątki od obowiązku informacyjnego*

- W przypadku, w którym dane zostały zebrane od osoby, której dotyczą, obowiązek informacyjny wyłączony jest jedynie, gdy – oraz jedynie w zakresie, w jakim - osoba, której dane dotyczą, dysponuje już tymi informacjami (art. 13 ust. 4 r.o.d.o.).
- W przypadku pozyskiwania danych osobowych w inny sposób, obowiązek informacyjny wyłączone jest jedynie gdy i w zakresie w jakim:

– podmiot danych dysponuje już tymi informacjami
– udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku; 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;
– pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem unijnym lub prawem państwa członkowskiego, któremu podlega administrator;
– dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianym w prawie unijnym lub w prawie państwa członkowskiego, w tym ustawowym obowiązkiem zachowania tajemnicy.

- Ponadto prawodawca unijny dopuścił, w art. 23 RODO, możliwość ograniczenia zakres obowiązków informacyjnych przepisem szczególnym prawa unijnego lub prawa państwa członkowskiego.
- Ograniczenia obowiązków informacyjnych mogą potencjalnie także wynikać z przepisów szczególnych, których przyjęcie dopuszcza art. 85 ust. 2 RODO.

Radcowie prawni (z projektu)

- Do przetwarzania danych osobowych przez radców prawnych, w przypadku danych osobowych przetwarzanych w ramach wykonywania zawodu, przepisów art. 13-15 ust. 1 i 3, 18, 19 i 21 RODO - nie stosuje się.
- Wyłączenia te stosuje się w przypadku danych osobowych niezbędnych do zapewnienia prawidłowej realizacji zadań, obowiązków lub uprawnień.
- Przepisu art. 16 RODO rozporządzenia 2016/679 nie stosuje się, - o ile przepisy szczególne przewidują odrębny tryb sprostowania.

*Terminy spełnienia obowiązków informacyjnych*

- W przypadku zbierania danych wprost od osoby, której te dane dotyczą podanie wymaganych informacji powinno poprzedzić samą czynność zbierania danych.

- Spełnienie obowiązku informacyjnego w razie zbierania danych w inny sposób ma charakter następczy w stosunku do faktu ich pozyskania.
- Zgodnie z art. 14 ust. 3 r.o.d.o. administrator, w takich sytuacjach, podać informacje:
  - w rozsądnym terminie po pozyskaniu danych osobowych - najpóźniej w ciągu miesiąca;
  - w przypadku, w którym dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą, przekazanie informacji musi nastąpić najpóźniej przy pierwszej takiej komunikacji (por. też art. 21 ust. 4. r.o.d.o. dot. poinformowania o sprzeciwie);
  - jeżeli administrator danych planuje ujawnić dane osobowe innemu odbiorcy – przekazanie wymaganych informacji podmiotowi danych musi nastąpić najpóźniej przy ich pierwszym ujawnieniu.

*Obowiązek informacyjny w razie zmiany celu przetwarzania danych*

- Rozporządzenie reguluje kwestię przetwarzania danych osobowych w celach innych niż te dla których były pierwotnie zgromadzone, czyli w przypadku w którym administrator w trakcie przetwarzania zamierza zmienić cele przetwarzania. W przypadku takim administrator przed takim dalszym przetwarzaniem musi poinformować osobę, której dane dotyczą, o tym innym celu oraz udzielić jej wszelkich innych stosownych informacji, o których mowa w art. 13 ust. 3 lub art. 14 w ust. 2 r.o.d.o. – w zależności, czy pierwotnie dane zostały zebrane bezpośrednio od podmiotu danych czy w inny sposób. Przetwarzanie danych osobowych w innym celu niż pierwotny bez uprzedniego poinformowania o tym podmiotu danych jest niedopuszczalne.

## Prawo dostęp do danych (art. 15 RODO)

- Zgodnie z art. 15 ust. 1 r.o.d.o. osoba, której dane dotyczą, jest **uprawniona do uzyskania od administratora potwierdzenia**, czy przetwarzane są dane osobowe jej dotyczące.
- W przypadku, w którym administrator przetwarza dane jednostki ma ona:
  - **prawo dostępu do danych jej dotyczących** (można żądać dostępu do określonego zakresu danych),
  - **prawo do uzyskania określonych ww. przepisie informacji** (zakres przysługujących informacji koresponduje do pewnego stopnia z zakresem informacji przekazywanych podczas zbierania danych).

- Podmiot danych ma także **prawo do uzyskania kopii danych**.
  Administrator dostarcza bezpłatnie 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. [art. 15 ust. 3 r.o.d.o., por. też ust. 4]

- Art. 51 ust. 3 Konstytucji RP: Każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych. Ograniczenie tego prawa może określić ustawa.

## Prawo do sprostowania danych (art. 16 RODO)

- 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 sprostowania danych obejmuje prawo do żądania sprostowania nieprawidłowych danych oraz uzupełnienia danych niekompletnych.
- Art. 51 ust. 4 Konstytucji RP: Każdy ma prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą.
- Administrator może aktualizować dane z własnej inicjatyw, bez wniosku od podmiotu danych - zob. zasada prawidłowości danych [art. 5 ust. 1 lit. d RODO].
- Z prawa do sprostowania i uzupełnienia danych osobowych nie można wyprowadzać aktywnego obowiązku podmiotu danych sprawdzania danych na swój temat oraz korygowania i uzupełniania ich - por.: J. Barta, P. Fajgielski, R. Markiewicz, Ochrona danych osobowych. Komentarz, LEX 2015. W zakresie uzupełniania danych por. art. 51 ust. 1 Konstytucji RP: Nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby.

- żądanie sprostowania i uzupełnienia danych nie ma charakteru bezwzględnego, i w zależności od okoliczności, administrator może w pewnych przypadkach odmówić sprostowania danych;
- sprostowanie i uzupełnienie danych musi każdorazowo być zgodne z zasadami ogólnymi przetwarzania danych wynikającymi z art. 5 RODO, w szczególności uzupełnienie danych musi mieć związek z celem przetwarzania danych i uwzględniać zasady adekwatności i prawidłowości;
- zgodnie z art. 11 ust. 2 administrator nie musi uwzględniać żądania podmiotu danych w sytuacji, gdy może wykazać, że nie jest w stanie zidentyfikować osoby, której dane dotyczą;
- termin realizacji żądań reguluje zasadniczo art. 12 RODO;
- zgodnie z art. 19 administrator informuje o sprostowaniu każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie to wymagać niewspółmiernie dużego wysiłku. Administrator ma obowiązek poinformowania osoby, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.

Zob. „RODO. Ogólne rozporządzenie o ochronie danych. Komentarz", red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2018

Dla wystąpienia z żądaniami skierowanymi na korektę danych nie ma istotnego znaczenia:

a) czy niepoprawne (błędne, niekompletne) dane zostały wprowadzone do zbioru świadomie (przez administratora albo inną osobę, w tym samego zainteresowanego), czy też pomyłkowo lub przypadkowo, albo czy dane z upływem czasu straciły swoją aktualność (np. nazwisko kobiety w związku z zawarciem małżeństwa, adres w związku z przeprowadzką);

b) w jaki sposób (od kogo, na jakiej drodze) zainteresowany uzyskał wiadomość, że przetwarzane dane nie są poprawne;

c) "rozmiar" błędnych danych i znaczenie ich niepoprawności, czy i jakie wywołuje negatywne konsekwencje po stronie tego, kogo dane dotyczą (np. z jednej strony drobna pomyłka w adresie, z drugiej strony - mylna informacja o karalności osoby);

d) czy niepoprawność danych narusza prawa osobiste skarżącego; zainteresowany nie musi naruszenia praw osobistych wykazywać.

Barta Janusz, Fajgielski Paweł, Markiewicz Ryszard, Ochrona danych osobowych. Komentarz, LEX 2015

## Prawo do żądania usunięcia danych / 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;

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. *[dot. danych osobowych dzieci]*

## *Obowiązki informacyjne związane z realizacją prawa do usunięcia danych – przekazanie żądania innym administratorom*

Zgodnie z art. 17 ust. 2 RODO. **Jeżeli administrator upublicznił dane osobowe**, a na mocy art. 17 ust. 1 RODO 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.

- art. 17 ust. 2 RODO kreuje obowiązek przekazania, przez administratora danych, żądania podmiotu danych usunięcia danych dalszym administratorom, ;
- wydaje się, że podmiot danych, może wyrazić wolę, zgodnie z którą ogranicza żądanie usunięcia danych tylko do administratora, do którego bezpośrednio kieruje żądanie.
- zob. też: obowiązek powiadomienia przez administratora odbiorców, którym ujawniono dane osobowe, o usunięciu danych osobowych wynikający z art. 19 RODO.

*Ograniczenia prawa do usunięcia danych / do bycia zapomnianym*

Art. 17 ust. 3 RODO: ustępy 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* **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.

Prawo do sprzeciwu obejmuje trzy podstawy:

a) prawo do sprzeciwu wobec przetwarzania danych z przyczyn związanych z szczególną sytuacją podmiotu danych (art. 21 ust. 1)
b) prawo do sprzeciwu wobec przetwarzania danych osobowych na potrzeby marketingu bezpośredniego (art. 21 ust. 2)
c) prawo do sprzeciwu wobec przetwarzania danych osobowych do celów badań naukowych, historycznych lub do celów statystycznych (art. 21 ust. 6).

Jedynie sprzeciw wobec przetwarzania danych osobowych na potrzeby marketingu bezpośredniego jest bezwzględnie wiążący dla administratora w pozostałych przypadkach zachodzi zasadniczo konieczność dokonania ważenia podstaw przetwarzania danych i interesów związanych z przetwarzaniem, z jednej strony, oraz interesów praw i wolności osoby, której dane dotyczą, z drugiej strony.

Ogólne zasady realizacji prawa do sprzeciwu określa art. 12 RODO.

Obowiązek informacyjny – art. 21 ust. 4.

Prawo do wniesienia sprzeciwu drogą elektroniczną w przypadku sprzeciwu wiążącego się z korzystaniem z usług społeczeństwa informacyjnego – art. 21 ust. 5 (por. też motyw 59).

- Prawo do sprzeciwu wobec przetwarzania danych z przyczyn związanych z szczególną sytuacją podmiotu danych przysługuje wyłącznie jeżeli podstawą przetwarzania jest art. 6 ust. 1 lit. e) lub f).
- Administrator może nie uwzględnić takiego sprzeciwu jeżeli wykaże 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.

- Prawo do sprzeciwu wobec przetwarzania danych na potrzeby marketingu bezpośredniego nie ogranicza się do marketingu bezpośredniego własnych produktów lub usług, a zatem obejmuje także marketingu nie swoich produktów i usług.
- Motyw 70: Jeżeli dane osobowe są przetwarzane do celów marketingu bezpośredniego, osoba, której dane dotyczą, powinna mieć prawo wnieść w dowolnym momencie, bezpłatnie sprzeciw wobec tego przetwarzania, pierwotnego lub dalszego - w tym profilowania, o ile jest ono powiązane z marketingiem bezpośrednim. Prawo to powinno zostać wyraźnie podane do wiadomości osobie, której dane dotyczą, oraz powinno być przedstawione jasno i oddzielnie od wszelkich innych informacji.

***Sprzeciw wobec przetwarzania w celach marketingowych. Reklamy wyświetlane po zalogowaniu do serwisu internetowego***

- Teza: Złożony przez klienta Banku sprzeciw oznacza, że klient na swoim koncie internetowym (po zalogowaniu do niego za pomocą loginu i hasła) nie powinien otrzymywać jakichkolwiek informacji o marketingu Banku. W przeciwnym razie można uznać, że Bank nadal przetwarza dane osobowe klienta w celach marketingowych. Informowanie klienta na jego indywidualnym profilu o produktach Banku stanowi przetwarzanie jego danych w celach marketingowych. - wyrok WSA w Warszawie z dnia 12 sierpnia 2016 r., II SA/Wa 337/16

- Teza: Z chwilą ujawniania danych internauty (oczywiście w formie zalogowanej), zmienia się jego status odbiorcy reklamy: z anonimowego na znanego, spersonifikowanego klienta. Z chwilą takiej zmiany statusu internauty w przypadku, gdy administrator danych ma do czynienia z klientem, który zastrzegł sprzeciw przetwarzania swoich danych osobowych w celach marketingowych, system informacyjny administratora danych powinien natychmiast zaprzestać wyświetlania reklamy (art. 32 ust. 3 u.o.d.o.). Skoro tego nie czyni, tym samym nadal atakuje klienta swoim materiałem marketingowym, wbrew jego woli, narusza prawo. - wyrok WSA w Warszawie z dnia 9 stycznia 2017 r., II SA/Wa 878/16; wyrok WSA w Warszawie z dnia 15 czerwca 2010 r., II SA/Wa 556/10

## Prawo do ograniczenia przetwarzania

*Artykuł 18*

1. Osoba, której dane dotyczą, ma prawo żądania od administratora ograniczenia przetwarzania w następujących przypadkach: **a)** osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych – na okres pozwalający administratorowi sprawdzić prawidłowość tych danych; **b)** przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania; **c)** administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń; **d)** osoba, której dane dotyczą, wniosła sprzeciw na mocy art. 21 ust. 1 wobec przetwarzania – do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie administratora są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.

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

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

- żądanie ograniczonego przetwarzania dotyczyć może danych, osoby wnoszącej żądanie, tj. co do zasady, nie może dotyczyć danych innych osób;
- żądanie ograniczonego przetwarzania danych jest bez przedmiotowe, gdy przed jego zgłoszeniem administrator usunie dane danej osoby;
- należy uznać, że podmiot danych może cofnąć żądanie odgraniczonego przetwarzania danych;
- informacja o prawie do ograniczenia przetwarzania objęta jest zakresem obowiązków informacyjnych określonych w art. 13 i 14 RODO;
- zasady realizacji prawa określa art. 12 RODO (w tym terminy, brak odpłatności);
- przed uchyleniem ograniczenia przetwarzania administrator informuje o tym osobę, której dane dotyczą, która żądała ograniczenia (art. 18 ust. 3 RODO);
- zob. też: obowiązek powiadomienia przez administratora odbiorców, którym ujawniono dane osobowe, o usunięciu danych osobowych wynikający z art. 19 RODO.

- prawo do ograniczenia przetwarzania może podlegać ograniczeniom w prawie krajowym lub unijnym (art. 23 i 89);

## Obowiązek powiadomienia związany ze sprostowaniem, usunięciem i ograniczonym przetwarzaniem

*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.

- "odbiorca" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. […]
- "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
- Do realizacji obowiązku powiadomienia znajduje zastosowanie art. 12 RODO.
- Zgodnie z art. 58 ust. 2 lit. g organ nadzoru może nakazać administratorowi powiadomienie odbiorców, którym dane osobowe ujawniono, w przypadku, gdy administrator nie wywiązał się z obowiązku powiadomienia o sprostowaniu lub usunięciu danych osobowych lub o ograniczonym przetwarzaniu.

## Prawo do przenoszenia danych

*Artykuł 20*

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.

Elementy prawa do przenoszenia danych:

- prawo do otrzymania danych dostarczonych administratorowi w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego (w tym zakresie prawo do przenoszenie danych uzupełnia prawo dostępu),
- prawo przesłania ww. danych innemu administratorowi bez przeszkód ze strony administratora, któremu dane dostarczono,
- prawo żądania przeslania ww. danych przez administratora bezpośrednio innemu administratorowi (w razie, gdy jest to technicznie możliwe).

Zakres danych objętych prawem z art. 20 RODO.

- Na gruncie art. 20 RODO występuje problem zakresu danych, które są objęte zakresem przedmiotowym prawa do przeniesienia danych. W myśl opinii WP 242 za dane „dostarczone" przez osobę, której dane dotyczą można uznać: 1) dane aktywnie i świadomie przekazywane przez osobę, której dane dotyczą, 2) dane zaobserwowane przez administratora w związku z korzystaniem z usług lub urządzeń przez osobę, której dane dotyczą.

- W swej istocie przepis ten ma sprzyjać konkurencji i ułatwiać zmiany dostawców usług w konsumentom, przy czym art. 20 nie ogranicza danych podlegających przenoszeniu do tych, które są konieczne lub przydatne do zmiany usługi (por. opinia WP 242 rew.01).

*Przykłady do rozważenia (na gruncie RODO i przepisów szczególnych):*

- *przenoszenie danych z serwisów poczty elektronicznej (np. kontaktów,* wiadomości e-mail) [może przykładowo przejawiać się przekazaniem dostawcy analogicznych usług, jak i usług innego typu, np. archiwizacji danych];
- *przenoszenie list odtwarzania z serwisu muzycznego;*
- *przenoszenie listy zakupów (np. z karty lojalnościowej);*
- *przenoszenie blogów pomiędzy serwisami;*
- *przenoszenie zleceń, zdefiniowanych odbiorców, listy transakcji z konta bankowego;*

- „Przenoszenie danych może propagować kontrolowaną i ograniczoną wymianę danych osobowych przez użytkowników między organizacjami i w ten sposób wzbogacić usługi i doświadczenia konsumentów. Przenoszenie danych może ułatwić przesyłanie oraz ponowne wykorzystywanie danych dotyczących użytkowników między różnymi usługami, którymi są zainteresowani.„ (por. opinia WP 242 rew.01)

- Administrator otrzymujący dane odpowiada za zgodność przetwarzania z prawem. W konsekwencji należy uznać, że nie musi zatrzymać ani przyjąć wszystkich przekazywanych danych.
- W przypadku przeniesienia danych do nowego administratora ciążą na nim obowiązki informacyjne określone w RODO.
- Skorzystanie z prawa do przeniesienie danych samo w sobie nie delegitymizuje przetwarzania danych przez dotychczasowego administratora danych i nie wpływa na pierwotny okres przechowywania mający zastosowanie wobec danych, które zostały przesłane.
- Z art. 13 i ust. 2 lit. b) i art. 14 ust. 2 lit. c) wynika obowiązek informowania o prawie do przenoszenia danych.
- Ogólne zasady realizacji prawa do przenoszenia danych określa też art. 12 RODO.

- Realizacja prawa do przenoszenia danych nie może niekorzystnie wpływać na prawa i wolności innych. Kwestia tego wymogu w kontekście danych wykorzystywanych do celów osobistych a objętych prawem przenoszenia danych, z opinii WP 242 rew.01:
- „Operacje przetwarzania zainicjowane przez osobę, której dane dotyczą, w kontekście czynności o osobistym charakterze, które dotyczą i mają potencjalny wpływ na strony trzecie, pozostają w zakresie jej odpowiedzialności, w stopniu, w jakim o takim przetwarzaniu, w żaden sposób, nie decyduje administrator danych."
- „Na przykład usługa poczty e-mail może umożliwiać tworzenie książki osób kontaktowych, znajomych, krewnych, rodziny i szerszego otoczenia osoby, której dane dotyczą. Jako że dane te dotyczą możliwej do zidentyfikowania osobę osoby (i są przez nią tworzone), która chce realizować swoje prawo do przenoszenia danych, administratorzy danych powinni przesłać całą książkę e-maili przychodzących i wychodzących osobie, której dane dotyczą."
- „W związku z tym, aby zapobiec negatywnemu wpływowi na zaangażowane strony trzecie, przetwarzanie takich danych osobowych przez innego administratora jest dozwolone tylko w zakresie, w jakim dane są przechowywane pod wyłączną kontrolą wnioskującego użytkownika i są przetwarzane tylko na potrzeby o czysto osobistym lub domowym charakterze. Otrzymujący 'nowy' administrator danych […] nie może wykorzystywać przesłanych danych stron trzecich do własnych celów, np. w celu oferowania produktów i usług marketingowych […]. Na przykład informacji tych nie powinno się wykorzystywać do wzbogacenia profilu osoby, której dane dotyczą, będącej stroną trzecią i do odbudowy środowiska społecznego, bez jej wiedzy i zgody".

Pojęcie „ustrukturyzowanego, powszechnie używanego formatu nadającego się do odczytu maszynowego”.

Przyjmuje się, że do interpretacji ww. pojęcie pomocne może być odwołanie do dyrektywy 2013/37/UE (dot. ponownego wykorzystywania informacji sektora publicznego) - motyw 21: Dokument należy uznać za sporządzony **w formacie przeznaczonym do odczytu komputerowego**, jeżeli występuje w formacie pliku zorganizowanego w sposób umożliwiający aplikacjom komputerowym łatwe identyfikowanie, rozpoznawanie i pozyskiwanie z niego określonych danych. Dane zakodowane w plikach zorganizowanych w formacie przeznaczonym do odczytu komputerowego to dane przeznaczone do odczytu komputerowego. Formaty przeznaczone do odczytu komputerowego mogą być otwarte lub zastrzeżone; mogą one występować jako standardy formalne lub nie. Dokumentów zakodowanych w formacie pliku ograniczającym przetwarzanie automatyczne z powodu niemożności pozyskania danych lub utrudnień w ich pozyskaniu z tych dokumentów nie należy uznawać za sporządzone w formacie przeznaczonym do odczytu komputerowego […]

Motyw 68 RODO (68) osoba, której dane dotyczą, powinna także mieć możliwość otrzymywania dotyczących jej danych osobowych, których dostarczyła administratorowi, w ustrukturyzowanym, powszechnie używanym, nadającym się do odczytu maszynowego i interoperacyjnym formacie oraz przesyłania ich innemu administratorowi.

- Artykuł 20 ust. 1 RODO przewiduje, że osoby, których dane dotyczą, mają prawo do przesyłania danych do innego administratora bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe.
- Takie przeszkody można określić jako przeszkody prawne, techniczne lub finansowe tworzone przez administratora danych, aby powstrzymać lub spowolnić dostęp, przesyłanie lub ponowne wykorzystanie przez osobę, której dane dotyczą, lub przez innego administratora danych. Na przykład taką przeszkodę mogą stanowić: opłaty żądane za przesłanie danych, brak interoperacyjności lub dostępu do formatu danych lub API bądź zapewnianego formatu, nadmierna zwłoka lub złożoność w przypadku pozyskania pełnego zbioru danych, celowe zamaskowanie zbioru danych lub określone lub niewłaściwe bądź nadmierne żądania standaryzacji lub akredytacji. (z opinii WP 242 rew.01)
- Motyw 68 RODO: Administratorów danych należy zachęcać do opracowywania interoperacyjnych formatów, które umożliwiają przenoszenie danych. […] Przysługujące osobie, której dane dotyczą, prawo do przesłania lub otrzymania swoich danych osobowych nie powinno nakładać na administratorów obowiązku prowadzenia lub wprowadzenia kompatybilnych technicznie systemów przetwarzania.

- Prawo do przenoszenia poza ograniczeniami winiącymi z art. 20 RODO może podlegać ograniczeniom w prawie krajowym i unijnym (art. 23 oraz 89 ust. 3 dot. przetwarzania do celów archiwalnych w interesie publicznym).

Przykład (z projektu nowej u.o.d.o.)

Art. 10b. ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych

2. Instytucje płatnicze oraz instytucje pieniądza elektronicznego są uprawnione do ograniczenia prawa do przenoszenia danych, o którym mowa w art. 20 rozporządzenia nr 2016/679, i prawa do usunięcia danych, o którym mowa w art. 17 rozporządzenia nr 2016/679, gdy obowiązek lub uprawnienie do przetwarzania danych przez określony czas i określonym zakresie wynika z przepisów prawa.

3. Uprawnienie do przenoszenia danych, o którym mowa w art. 20 rozporządzenia nr 2016/679, nie dotyczy przenoszenia danych, które stanowią tajemnicę przedsiębiorstwa.

## Zautomatyzowane podejmowanie decyzji

*Artykuł 22*

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

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

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

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

- Art. 22 ust. 1 określa zakaz dot. wydawania decyzji opierające się wyłącznie na zautomatyzowanym przetwarzaniu danych osobowych i wywołujące wobec podmiotu danych skutki prawne lub w podobny sposób istotnie na nią wpływające mogą obejmować.
- Przykłady: ocena zdolności kredytowej; ocena spełniania warunków zawarcia umowy ubezpieczeniowej; elektroniczne metody rekrutacji, przyznawanie premii i inne decyzje z zakresu prawa pracy; różnicowanie kuponów promocyjnych w programie lojalnościowym. Kwestia dyskusyjna – reklama behawioralna.
- Art. 22 ust. 2 określa wyjątki od zakazu, a ust. 3 wymogi mające wówczas zastosowanie. Ograniczenie wyjątków przewiduje z kolei art. 22 ust. 4 (dot. szczególnych kategorii danych).

- "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;

- Por. też art. 13 ust. 2 lit. f) oraz art. 14 ust. 2 lit. g) dotyczące obowiązków informacyjnych.
- Por. też art. 35 ust. 3 lit. a) wprowadzający obowiązkową ocenę skutków dla ochrony danych w przypadku „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;”

- Prawo krajowe i unijne może wprowadzać rozwiązania szczególne odrębnymi przepisami.

  Z projektu ustawy wprowadzającej nową u.o.d.o.:

  W art. 70 Prawa bankowego po ust. 1 dodaje się ust. 1a w brzmieniu:

  „1a. W celu oceny zdolności kredytowej, o której mowa w ust. 1, oraz wykonania obowiązku, o którym mowa w art. 50 ust. 2, bank może przetwarzać dane osobowe w sposób zautomatyzowany, w tym poprzez profilowanie.”.

## Podstawa do ograniczenia praw osób, której dane dotyczą w przepisach unijnych oraz przepisach krajowych

Zgodnie art. 23 r.o.d..o. przepisy unijne oraz przepisy prawa krajowego mogą ograniczyć zakres obowiązków i praw przewidzianych w art. 12–22 i w art. 34, a także w art. 5 (**Zasady dotyczące przetwarzania danych osobowych)** – jeżeli ograniczenie takie nie narusza istoty podstawowych praw i wolności oraz jest w demokratycznym społeczeństwie środkiem niezbędnym i proporcjonalnym, służącym:

a) bezpieczeństwu narodowemu;
b) obronie;
c) bezpieczeństwu publicznemu;
d) zapobieganiu przestępczości, prowadzeniu postępowań przygotowawczych, wykrywaniu lub ściganiu czynów zabronionych lub wykonywaniu kar, w tym ochronie przed zagrożeniami dla bezpieczeństwa publicznego i zapobieganiu takim zagrożeniom;
e) innym ważnym celom leżącym w ogólnym interesie publicznym Unii lub państwa członkowskiego, w szczególności ważnemu interesowi gospodarczemu lub finansowemu Unii lub państwa członkowskiego, w tym kwestiom pieniężnym, budżetowym i podatkowym, zdrowiu publicznemu i zabezpieczeniu społecznemu;
f) ochronie niezależności sądów i postępowania sądowego;
g) zapobieganiu naruszeniom zasad etyki w zawodach regulowanych, prowadzeniu postępowań w takich sprawach, ich wykrywaniu oraz ściganiu;
h) funkcjom kontrolnym, inspekcyjnym lub regulacyjnym związanym, nawet sporadycznie, ze sprawowaniem władzy publicznej w przypadkach, o których mowa w lit. a) – e) oraz g);
i) ochronie osoby, której dane dotyczą, lub praw i wolności innych osób;
j) egzekucji roszczeń cywilnoprawnych.

## Środki ochrony prawnej przewidziane w RODO

**Prawo do wniesienia skargi do organu nadzorczego** (art. 77 RODO)

- Zgodnie z art. 77 RODO 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.

**Prawo do skutecznego środka ochrony prawnej przed sądem przeciwko organowi nadzorczemu** (art. 78 RODO, por. też art. 58 ust 4 RODO).

**Prawo do skutecznego środka ochrony prawnej przed sądem przeciwko administratorowi lub podmiotowi przetwarzającemu** (art. 79 RODO)

**Prawo do odszkodowania i odpowiedzialność odszkodowawcza administratora danych oraz podmiotu przetwarzającego** (art. 82 RODO)

(por. min. art. 87-91 projektu ustawy o ochronie danych osobowych)

# Administrator, współadministratorzy i podmiot przetwarzający

**ADMINISTRATOR**

"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.

**WSPÓŁADMINISTRATORZY (art. 26 RODO)**

- Jeżeli co najmniej dwóch administratorów wspólnie ustala cele i sposoby przetwarzania, są oni **współadministratorami**.

  *Przykładowo sytuacja taka może dotyczyć, w określonych relacjach, działania biur podróży, pośredników nieruchomości, agencje pracy.*

- **Współadministratorzy** są zobowiązani do tego aby w drodze wspólnych uzgodnień w przejrzysty sposób określić odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z niniejszego rozporządzenia.
- Dokonywane uzgodnienia powinny należycie odzwierciedlać odpowiednie zakresy obowiązków współadministratorów oraz relacje pomiędzy nimi a podmiotami, których dane dotyczą, w szczególności powinny odnosić się do wykonywania przez podmiot danych przysługujących jej praw, oraz obowiązków w odniesieniu do podawania informacji przy gromadzeniu danych. W uzgodnieniach można wskazać punkt kontaktowy dla osób, których dane dotyczą.
- Zasadnicza treść uzgodnień dokonanych przez współadministratorów jest udostępniana podmiotom, których dane dotyczą.
- Przypadające współadministratorom obowiązki mogą też określać przepisy prawa (potencjalnie dotyczy to w szczególności administratorów z sektora publicznego).
- Niezależnie od uzgodnień dokonanych przez współadministratorów osoba, której dane dotyczą, może wykonywać przysługujące jej prawa wynikające z niniejszego rozporządzenia wobec każdego z administratorów.

**PODMIOT PRZETWARZAJĄCY**

"podmiot przetwarzający" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora.

- administrator może powierzyć dokonywanie przetwarzania danych w określonym zakresie podmiotowi przetwarzającemu.
- administrator korzysta wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi r.o.d.o. i chroniło prawa osób, których dane dotyczą (art. 28 ust. 1, por. też 28 ust. 5).
- podpowierzenie: podmiot przetwarzający nie korzysta z usług innego podmiotu przetwarzającego bez uprzedniej zgody administratora (zob. art. 28 ust. 2, który określa warunki takiego podpowierzenia (por. też art. 28 ust. 4-5).
- jeżeli podmiot przetwarzający naruszy niniejsze rozporządzenie przy określaniu celów i sposobów przetwarzania, uznaje się go za administratora w odniesieniu do tego przetwarzania (art. 28 ust. 10).

- 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 (art. 28 ust. 3).
- Taka umowa lub inny instrument prawny mają formę pisemną, w tym formę elektroniczną (art. 28 ust. 9) – „sformułowania tego nie można wykładać przez pryzmat przepisów krajowych o formie czynności prawnych", „w konsekwencji należy opowiedzieć się za stanowiskiem, zgodnie, z którym wystarczające jest użycie formy, która odpowiadałby zakresowi pojęcia formy […] dokumentowej (art. 772 k.c.) z ograniczeniem jej zastosowania do utrwalenia tekstu" (K. Witkowska-Nowakowska [w:] RODO. Rozporządzenie ogólne o ochronie danych. Komentarz).

***Elementy umowy lub innego instrumentu prawnego***

Umowy lub innego instrumentu prawny, na podstawie których odbywa się przetwarzanie powinien określać (art. 28 ust. 3):

- przedmiot,
  [opis przedmiotu umowy czyli powierzonych procesów / operacji przetwarzania danych i wskazanie ich ewentualnej relacji do określonych usług]
- czas trwania przetwarzania,
  [czynności jednorazowe, przetwarzanie na czas nieokreślony lub określony bezwzględnie lub za pomocą określonych kryteriów ustalania tego okresu]
- charakter i cel przetwarzania,
- rodzaj danych osobowych,
- kategorie osób, których dane dotyczą,
- obowiązki i prawa administratora,
  [wiąże się to z koniecznością zapewnienia prawidłowej realizacji obowiązków administratora także w odniesieniu do danych powierzanych]

- Ponadto umowa lub inny instrumentu prawny, na podstawie których odbywa się przetwarzanie powinien stanowić, że podmiot przetwarzający (art. 28 ust. 3):

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 *[nie jest potrzebne ich określenie w umowie]*;przestrzega warunków korzystania z usług innego podmiotu przetwarzającego *[o warunkach tym mowa w ust. 2 i 4 art. 28]*;

c.d.n.

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;

[Może być koniecznym określenie w umowie czasu, zasad i sposób realizacji ww. obowiązku przez podmiot przetwarzający. Ma to szczególne znaczenie w przypadkach, w których administrator nie ma bezpośredniego dostępu do przetwarzanych danych]

f) uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga administratorowi wywiązać się z obowiązków określonych w art. 32-36;

[Przepisy te dotyczą bezpieczeństwa przetwarzania danych (art. 32), obowiązków notyfikacyjnych (art. 33-34), oceny skutków dla ochrony danych (art. 35-36)]

g) po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji administratora usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych;

h) udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w niniejszym artykule oraz umożliwia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich. Podmiot przetwarzający niezwłocznie informuje administratora, jeżeli jego zdaniem wydane mu polecenie stanowi naruszenie niniejszego rozporządzenia lub innych przepisów o ochronie danych.

- Elementy umowy powierzającej przetwarzanie danych określone w RODO nie stanowią katalogu zamkniętego, umowa taka może regulować też inne kwestie związane z powierzeniem przetwarzania danych.

- *Standardowe klauzule umowne:* umowa lub inny instrument prawny powierzający przetwarzanie mogą się opierać w całości lub w części na standardowych klauzulach umownych (art. 28 ust. 6): standardowe klauzule umowne może określić Komisja oraz organ nadzorczy (art. 28 ust. 7-8)

K. Witkowska-Nowakowska [w:] RODO. Ogólne rozporządzenie o ochronie danych. Komentarz, s. 646-647: „ W ramach takich ustaleń strony mogą uzgodnić także m.in. kwestie związane z:

1) ewentualnym regresem w przypadku naruszenia przez podmiot przetwarzający przepisów w zakresie ochrony danych osobowych i ustaleniem rozkładu odpowiedzialności w relacjach wewnętrznych pomiędzy administratorem a podmiotem przetwarzającym;
2) zastrzeżenia kar umownych w przypadku naruszenia przez podmiot przetwarzający postanowień umowy;
3) wprowadzenie szczegółowych zasad prowadzenia audytów lub inspekcji przez administratora;
4) skutecznością i mocą wiążącą zaleceń wydawanych w toku prowadzonych audytów lub inspekcji;
5) wspieraniem administratora w przypadku kontroli przestrzegania przepisów rozporządzenia 2016/679;
6) zasadami współpracy z inspektorem ochrony danych powołanym po stronie podmiotu przetwarzającego;
7) wynagrodzeniem z tytułu przetwarzania danych w imieniu administratora;
8) możliwymi sposobami zakończenia współpracy;
9) stosowanymi obostrzeniami lub konkretnymi rozstrzygnięciami w zakresie obligatoryjnych środków technicznych i organizacyjnych, których zastosowania żąda administrator;
10) ustaleniem prawa właściwego w relacjach transgranicznych”.

**PRZETWARZANIE Z UPOWAŻNIENIA ADMINISTRATORA LUB PODMIOTU PRZETWARZAJĄCEGO (art. 29 RODO)**

- każda osoba działająca z upoważnienia administratora lub podmiotu przetwarzającego i mająca dostęp do danych osobowych przetwarza je wyłącznie na polecenie administratora, chyba że wymaga tego prawo Unii lub prawo państwa członkowskiego.
- powyższe dotyczy także samego podmiotu przetwarzającego.

- zgodnie z art. 38 ust. 4 r.o.d.o. 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.

**PRZEDSTAWICIELE ADMINISTRATORÓW LUB PODMIOTÓW PRZETWARZAJĄCYCH NIEMAJĄCYCH JEDNOSTKI ORGANIZACYJNEJ W UNII (art. 27 RODO)**

- zgodnie z art. 27 ust. 1 jeżeli zastosowanie ma art. 3 ust. 2, administrator lub podmiot przetwarzający na piśmie wyznacza swojego przedstawiciela w Unii.
- art. 27 ust. 2 określa wyjątki od powyższego obowiązku.
- art. 27 ust. 3 reguluje kwestię siedziby przedstawiciela.

- przedstawiciel powinien zostać upoważniony, by do celów zapewnienia przestrzegania r.o.d.o. mogły się do niego zwracać - oprócz lub zamiast do administratora lub podmiotu przetwarzającego - w szczególności organy nadzorcze i osoby, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem.
- wyznaczenie przedstawiciela przez administratora lub podmiot przetwarzający pozostaje bez uszczerbku dla postępowań, które mogą zostać wszczęte przeciwko samemu administratorowi lub podmiotowi przetwarzającemu (art. 27 ust. 5 RODO).

# Obowiązki administratora i podmiotu przetwarzającego

❖ **Zasada zgodności z prawem**

- Z wynikającej z art. art. 5 ust. 1 lit. a RODO zasady zgodności z prawem wynika obowiązek przetwarzane danych zgodnie, nie tylko z postanowieniami RODO ale także z przepisami zawartymi w regulacjach szczególnych.
- W pierwszej kolejności obowiązek działania z prawem odnosi się do zachowania przesłanek legalności przetwarzania danych (art. 6 RODO) i przestrzegania ogólnych zasad przetwarzania danych osobowych (art. 5 RODO).
- W kontekście powyższego należy wskazać, że administrator jest odpowiedzialny za przestrzeganie zasad ogólnych oraz musi być w stanie wykazać ich przestrzeganie – jest to tzw. zasada rozliczalności (wynika ona z art. 5 ust. 2, por. też np. art. 7 ust. 1 dot. zgody).

❖ **Identyfikacja procesów przetwarzania danych osobowych a obowiązki administratora danych**

- W praktyce niemożliwe jest pełnie wypełnienie obowiązków ciążących na administratorze danych (podmiocie przetwarzającym) bez identyfikacji procesów przetwarzania danych w zbiorach danych oraz poza zbiorami w sposób zautomatyzowany oraz bez zinwentaryzowanych zasobów służących przetwarzaniu danych osobowych (zob. obowiązek prowadzenia rejestru czynności przetwarzania).

❖ **Ogólny obowiązek wdrażania środków technicznych i organizacyjnych zapewniających zgodność przetwarzania z postanowieniami RODO (art. 24 RODO)**

- 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.

✓ Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki te obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych.
✓ Stosowanie zatwierdzonych kodeksów postępowania, o których mowa w art. 40, lub zatwierdzonego mechanizmu certyfikacji, o którym mowa wart. 42, może być wykorzystane jako element dla stwierdzenia przestrzegania przez administratora ciążących na nim obowiązków.

❖ **Obowiązek uwzględniania ochrony danych w fazie projektowania oraz domyślna ochrona danych**
(tzw. „*privacy by design*" i „*privacy by default*" - artykuł 25 RODO)

- 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 **wdraża odpowiednie środki techniczne i organizacyjne, 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.
- 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.

❖ **Obowiązki informacyjne związane z gromadzeniem danych osobowych (art. 13 i 14 RODO)**

- *informacje podawane w przypadku zbierania danych od osoby, której dane dotyczą określa art. 13*
- *informacje podawane w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą określa art. 14*
- *administrator danych wypełniając obowiązki informacyjne powinien przestrzegać postanowień art. 12 formułującego zasady przejrzystego informowania*

❖ **Obowiązki stanowiące korelat wykonywania praw przez podmiot danych osobowych (art. 12, art. 15-22)**

❖ **Obowiązek współpracy z organem nadzorczym (art. 31)**

❖ **Obowiązek wyznaczenia inspektora ochrony danych (zob. 37-39 RODO) [zob. slajdy dot. inspektora ochrony danych]**

❖ **Obowiązek zapewnienia odpowiedniego stopnia bezpieczeństwa przetwarzania danych** *(artykuł 32 RODO)*

- 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** (art. 32 ust. 1).

- 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 (art. 32 ust. 2).

Normy z serii ISO/IEC 27001

• Niezależnie od mechanizmów przewidzianych w przepisach regulujących ochronę danych osobowych, do prawidłowego wdrożenia rozporządzenia może się przyczynić wdrożenie norm technicznych z serii ISO 27001. Są to międzynarodowe normy standaryzujące systemy zarządzania bezpieczeństwem informacji, regulują zasadniczo kwestie identyfikacji, zarządzania i monitorowania ryzykiem, ujawnienia informacji z wykorzystaniem analizy ryzyka.

• W związku z powyższym podmioty przetwarzających dane osobowe dostosowując się do wymogów rozporządzenia mogą, tworząc swoje system bezpieczeństwa informacji, także opierać się na normach z serii ISO 27001, gdyż te

• W Polsce normę ISO/IEC 27001 opublikowana jest obecnie jako PN-ISO/IEC 27001:2014-12.

❖ **Obowiązek dokonywania oceny skutków planowanych operacji przetwarzania danych (art. 35-36 RODO)**

**Ocena skutków dla ochrony danych (art. 35 RODO)**
**(*ang. Data Protection Impact Assessment - DPIA*)**

- Dokonywanie oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych jest nowym obowiązkiem, który ciąży na administratorze danych.
- Oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych administrator dokonuje przed rozpoczęciem przetwarzania dokonuje. [art. 35 ust. 1 RODO]
- Zasadniczo ocena ta dokonywana jest w razie zachodzenia wysokiego ryzyka naruszenia praw lub wolności osób fizycznych.
- Wyniki oceny należy uwzględnić przy określaniu odpowiednich środków, które należy zastosować by wykazać, że przetwarzanie danych osobowych odbywa się zgodnie z RODO.

## *Zakres obowiązku dokonania oceny skutków dla ochrony danych*

Przeprowadzenie ocena skutków dla ochrony danych jest wymagane:

- 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** [art. 35 ust. 1 RODO]

w szczególności przeprowadzenie ocena jest wymagane w przypadku:

- 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 [art. 35 ust. 3 lit a RODO];
- przetwarzania na dużą skalę szczególnych kategorii danych osobowych (art. 9 ust. 1 RODO) lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa (art. 10 RODO) [art. 35 ust. 3 lit b RODO];
- systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie [art. 35 ust. 3 lit c RODO].
- Gdy planowane przetwarzanie polega na wykonywaniu operacji uwzględnionych w wykazie prowadzonym i publikowanym przez organ nadzorczy [art. 35 ust. 4 RODO];

- Wyjątki od obowiązku przeprowadzenia oceny skutków dla ochrony danych określa art. 35 ust. 10 RODO.

- Zob. Wytyczne Grupy Roboczej Art. 29 dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko" do celów rozporządzenia 2016/679 – WP 248 rev.01
- Zob. Proponowany wykaz rodzajów przetwarzania, dla których wymagane jest przeprowadzenie oceny skutków - projekt ogłoszony przez GIODO, dostępny: https://www.giodo.gov.pl/pl/1520281/10430

*Z projektu ustawy*

**Art. 55.** 1. Prezes Urzędu:

1) ogłasza w komunikacie wykaz rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony, o którym mowa w art. 35 ust. 4 rozporządzenia 2016/679;

2) może ogłosić w komunikacie wykaz rodzajów operacji przetwarzania danych osobowych niewymagających oceny skutków przetwarzania dla ich ochrony, o którym mowa w art. 35 ust. 5 rozporządzenia 2016/679.

2. Komunikaty, o których mowa w ust. 1, ogłasza się w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski".

[podstawa prawna ogłaszania komunikatów w RODO – art. 35 ust. 4-6]

***Wyjątki od obowiązku przeprowadzenia oceny skutków dla ochrony danych (art. 35 ust. 10)***

- Obowiązek oceny skutków dla ochrony danych nie zachodzi, jeżeli łącznie spełnione są następujące przesłanki:

1) Przetwarzanie jest niezbędna do wypełnienia obowiązku prawnego ciążącego na administratorze (przetwarzanie dokonywane jest na mocy art. 6 ust. 1 lit. c) lub przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznych lub w ramach sprawowania władzy publicznej powierzonej administratorowi (przetwarzanie dokonywane jest na mocy art. 6 ust. 1 lit. e);
2) ma podstawę prawną w prawie Unii lub w prawie państwa członkowskiego, któremu podlega administrator;
3) prawo takie reguluje daną operację przetwarzania lub zestaw operacji,
4) oceny skutków dla ochrony danych dokonano już w ramach oceny skutków regulacji w związku z przyjęciem tej podstawy prawnej

(chyba że państwa członkowskie uznają za niezbędne, by przed podjęciem czynności przetwarzania dokonać oceny skutków dla ochrony danych).

***Elementy oceny skutków dla ochrony danych (DPIA):***

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,

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.

[art. 35 ust. 7 RODO]

***Zasady normatywne dokonywania oceny skutków dla ochrony danych*:**

- Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę [art. 35 ust. 1 RODO].
- Oceniając skutki operacji przetwarzania uwzględnia się przestrzeganie przez administratora lub podmiot przetwarzający **zatwierdzonych kodeksów postępowania** [art. art. 35 ust. 8 RODO].
- Dokonując oceny skutków dla ochrony danych, administrator **konsultuje się z inspektorem ochrony danych**, jeżeli został on wyznaczony [art. 35 ust. 2 RODO].
- W stosownych przypadkach administrator zasięga **opinii osób, których dane dotyczą, lub ich przedstawicieli** w sprawie zamierzonego przetwarzania [art. 35 ust. 9 RODO].
- W razie potrzeby, przynajmniej gdy zmienia się ryzyko wynikające z operacji przetwarzania, administrator dokonuje przeglądu, by stwierdzić, czy przetwarzanie odbywa się zgodnie z oceną skutków dla ochrony danych [**obowiązek aktualizacji oceny** - art. 35 ust. 11 RODO]

- Dokonanie oceny skutków dla ochrony danych w pewnych przypadkach może wymagać przeprowadzenia **uprzednich konsultacji** z organem nadzorczym.

– Instytucję uprzednich konsultacji reguluje art. 36 RODO oraz art. 58 projektu ustawy u.o.d.o.

– Zakres obowiązku przeprowadzenia uprzednich konsultacji z organem nadzorczym:

Administrator zobowiązany jest do podjęcia konsultacji z organem nadzorczym jeżeli po dokonania oceny skutków dla ochrony danych osobowych (zgodnie z art. 35) „stwierdzi, że bez podjęcia odpowiednich kroków w postaci zastosowania zabezpieczeń, środków bezpieczeństwa oraz mechanizmów minimalizujących ryzyko planowane przetwarzanie będzie powodować wysokie rysko naruszenia praw lub wolności, osób których dane dotyczą, i jednocześnie uzna, że ryzyka tego nie da się zminimalizować środkami rozsądnymi z punktu widzenia dostępnych technologii i kosztów wdrożenia” (K. Witkowska-Nowakowska [w:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*)

❖ **Obowiązki notyfikacyjne**

**Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu (artykuł 33 RODO)**

- W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki - w miarę możliwości, (co do zasady) nie później niż w terminie 72 godzin po stwierdzeniu naruszenia - zgłasza je właściwemu organowi nadzorczemu, 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. Por. też art. 33 ust. 4.
- podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi.
- art. 33 ust. 3 określa elementy zgłoszenia, a art. 33 ust. 5 obowiązek dokumentowania naruszeń ochrony danych osobowych
- *Z projektu ustawy u.o.d.o.: art. 56. Prezes Urzędu może prowadzić system teleinformatyczny umożliwiający administratorom dokonywanie zgłoszenia naruszenia ochrony danych osobowych, o którym mowa w art. 33 rozporządzenia 2016/679.*

**Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych** *(artykuł 34 RODO)*

- 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.
- Zawiadomienie nie jest wymagane, gdy:

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;

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.

❖ **Obowiązki dokumentacyjne (zbiorczo)**

**Rejestrowanie czynności przetwarzania (art. 30)**

- każdy administrator (przedstawiciel administratora) prowadzi **rejestr czynności przetwarzani**a danych osobowych, za które odpowiadają.
- każdy podmiot przetwarzający (jego przedstawiciel) prowadzi **rejestr wszystkich kategorii czynności przetwarzania** dokonywanych w imieniu administratora

- obowiązki powyższe nie mają zastosowania **do przedsiębiorcy lub podmiotu zatrudniającego mniej niż 250 osób**, chyba że przetwarzanie, którego dokonują, :

– może powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą,
– nie ma charakteru sporadycznego
– lub obejmuje szczególne kategorie danych osobowych, o których mowa w art. 9 ust. 1, lub dane osobowe dotyczące wyroków skazujących i naruszeń prawa, o czym mowa w art. 10.

W rejestrze **rejestr czynności przetwarzania** prowadzonym przez administratora zamieszcza się wszystkie następujące informacje:

a) imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz 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 przekazań, o których mowa w art. 49 ust. 1 akapit drugi, dokumentacja odpowiednich zabezpieczeń;
f) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;
g) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1.

W rejestrze **rejestr kategorii czynności przetwarzania** prowadzonym przez podmiot przetwarzający zawiera się następujące informacje:

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

b) kategorie przetwarzań dokonywanych w imieniu każdego z administratorów;

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

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

**Upoważnienia i polecenia co do przetwarzania danych osobowych**

- podmiot przetwarzający przetwarza dane, co do zasady, wyłącznie na polecenie administratora (por. art. 29);
- pracownicy administratora oraz podmiotu przetwarzającego powinni być upoważnieni do przetwarzania danych i przetwarzać dane, , co do zasady, wyłącznie na polecenie administratora (por. art. 29);
- kwestia dokumentacji upoważnień i poleceń;
- w rachubę wchodzi również prowadzenie ewidencji udzielonych upoważnień;
- zgodnie z art. 38 ust. 4 r.o.d.o. 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.

**Polityka ochrony danych**

- Zgodnie z art. 24 ust. 2, jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki służące zapewnieniu aby przetwarzanie odbywało się zgodnie z r.o.d.o. obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych.

**Dokumentacja ocena skutków planowanych operacji przetwarzania dla ochrony danych osobowych oraz uprzednich konsultacji** (art. 35-36)

**Uzgodnienia współadministratorów** (art. 26)

**Umowy lub inne instrumenty powierzenia przetwarzania danych** (art. 28)

**Rejestr naruszeń ochrony danych osobowych** (art. 33 ust. 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 obowiązku notyfikacyjnego.

**Pozostała dokumentacja umożliwiająca wykazanie przestrzeganie przepisów r.o.d.o.**

- przykładowo: zgody na przetwarzanie danych, dokumentacja wypełniania obowiązków informacyjnych, dokumentacja związana z powołaniem (lub niepowołaniem inspektora ochrony danych).

# Inspektor ochrony danych

- Instytucję inspektora ochrony danych regulują art. 37- 39 r.o.d.o.
- Obowiązek wyznaczenia **inspektora ochrony danych,** określa art. 37 ust. 1, administrator i podmiot przetwarzający obligatoryjnie 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 (art. 9 ust. 1) oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa.

*Z projektu u.o.d.o.*

Art. 8. Administrator i podmiot przetwarzający jest obowiązany do wyznaczenia inspektora ochrony danych, zwanego dalej „inspektorem”, w przypadkach i na zasadach określonych w art. 37 rozporządzenia 2016/679.

Art. 9. Przez organy i podmioty publiczne obowiązane do wyznaczenia inspektora, o których mowa w art. 37 ust. 1 lit. a rozporządzenia 2016/679, rozumie się:

1) **jednostki sektora finansów publicznych**, o których mowa w art. 9 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych;

2) instytuty badawcze, o których mowa w ustawie z dnia 30 kwietnia 2010 r. o instytutach badawczych (Dz. U. z 2017 r. poz. 1158, 1452 i 2201);

3) Narodowy Bank Polski.

Art. 9 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych:

Sektor finansów publicznych tworzą:

1) organy władzy publicznej, w tym organy administracji rządowej, organy kontroli państwowej i ochrony prawa oraz sądy i trybunały;

2) jednostki samorządu terytorialnego oraz ich związki;

2a) związki metropolitalne;

3) jednostki budżetowe;

4) samorządowe zakłady budżetowe;

5) agencje wykonawcze;

6) instytucje gospodarki budżetowej;

7) państwowe fundusze celowe;

8) Zakład Ubezpieczeń Społecznych i zarządzane przez niego fundusze oraz Kasa Rolniczego Ubezpieczenia Społecznego i fundusze zarządzane przez Prezesa Kasy Rolniczego Ubezpieczenia Społecznego;

9) Narodowy Fundusz Zdrowia;

10) samodzielne publiczne zakłady opieki zdrowotnej;

11) uczelnie publiczne;

12) Polska Akademia Nauk i tworzone przez nią jednostki organizacyjne;

13) państwowe i samorządowe instytucje kultury;

14) inne państwowe lub samorządowe osoby prawne utworzone na podstawie odrębnych ustaw w celu wykonywania zadań publicznych, z wyłączeniem przedsiębiorstw, instytutów badawczych, banków i spółek prawa handlowego.

RODO

- 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 inspektora ochrony danych określonych w r.o.d.o.
- Inspektor ochrony danych może być członkiem personelu administratora lub podmiotu przetwarzającego lub wykonywać zadania na podstawie umowy o świadczenie usług.
- Grupa przedsiębiorstw może wyznaczyć jednego inspektora ochrony danych.
- Jeżeli administrator lub podmiot przetwarzający są organem lub podmiotem publicznym, dla kilku takich organów lub podmiotów można wyznaczyć - z uwzględnieniem ich struktury organizacyjnej i wielkości - jednego inspektora ochrony danych.
- Kwestię fakultatywnego powołania inspektora ochrony danych oraz obowiązku powołania inspektora wynikającego z przepisów odrębnych reguluje art. 37 ust. 4 RODO.
- Status inspektora ochrony danych określa art. 38 RODO.

**Zadania inspektora ochrony danych (art. 39 RODO)**

a) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy r.o.d.o. oraz innych przepisów o ochronie danych i doradzanie im w tej sprawie;

b) **monitorowanie przestrzegania** r.o.d.o. oraz innych przepisów 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.

Ponadto 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 (art. 38 ust. 4)

- Administrator lub podmiot przetwarzający publikują dane kontaktowe inspektora ochrony danych i zawiadamiają o nich organ nadzorczy (RODO).

*Z projektu u.o.d.o.:*

**Art. 10.** 1. Podmiot, który wyznaczył inspektora, zawiadamia Prezesa Urzędu o jego wyznaczeniu w terminie 14 dni od dnia wyznaczenia, wskazując imię, nazwisko, adres poczty elektronicznej lub numer telefonu inspektora.

2. Zawiadomienie może zostać dokonane przez pełnomocnika podmiotu, o którym mowa w ust. 1. Do zawiadomienia dołącza się pełnomocnictwo udzielone w formie elektronicznej.

3. W zawiadomieniu obok danych, o których mowa w ust. 1, wskazuje się: […]

4. Podmiot, który wyznaczył inspektora, zawiadamia Prezesa Urzędu o każdej zmianie danych, o których mowa w ust. 1 i 3, oraz o odwołaniu inspektora, w terminie 14 dni od dnia zaistnienia zmiany lub odwołania.

5. W przypadku wyznaczenia jednego inspektora przez organy lub podmioty publiczne albo przez grupę przedsiębiorstw, każdy z tych podmiotów dokonuje zawiadomienia, o którym mowa w ust. 1 i 4.

6. Zawiadomienia, o których mowa w ust. 1 i 4, sporządza się w postaci elektronicznej i opatruje kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP.

**Art. 11.** Podmiot, który wyznaczył inspektora, udostępnia dane inspektora, o których mowa w art. 10 ust. 1, niezwłocznie po jego wyznaczeniu, na swojej stronie internetowej, a jeżeli nie prowadzi własnej strony internetowej, w sposób ogólnie dostępny w miejscu prowadzenia działalności.

# Przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych

***[ogólna informacja]***

- Przekazywanie danych osobowych do państwa trzeciego lub organizacji międzynarodowych regulują art. 44- 50 RODO.

- Przekazanie danych osobowych, które są przetwarzane lub mają być przetwarzane po przekazaniu do państwa trzeciego lub organizacji międzynarodowej, następuje tylko, gdy - administrator i podmiot przetwarzający spełnią warunki określone w rozdziale V RODO, w tym warunki dalszego przekazania danych z państwa trzeciego lub przez organizację międzynarodową do innego państwa trzeciego lub innej organizacji międzynarodowej (art. 44).

- Przekazywanie danych osobowych do państwa trzeciego lub organizacji międzynarodowych może być dokonywane:
  - na podstawie decyzji stwierdzającej odpowiedni stopień ochrony (art. 45),
  - z zastrzeżeniem odpowiednich zabezpieczeń (art. 46),
  - na podstawie wiążących reguł korporacyjnych (art. 47),
  - w szczególnych przypadkach określonych w art. 48-49.

# System organów ochrony danych osobowych

***[ogólna informacja]***

**Organy posiadające kompetencje z zakresu ochrony danych osobowych**

- **Organy nadzorcze**
- Polskim organem nadzorczym jest **Prezes Urzędu Ochrony Danych Osobowych.**
- Prezes Urzędu wykonuje swoje zadania przy pomocy Urzędu Ochrony Danych Osobowych.
- Przy Prezesie Urzędu działa Rada do Spraw Ochrony Danych Osobowych.

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

- **Komisja Europejska**

(wydawanie aktów delegowanych i aktów wykonawczych, sprawozdania i wnioski ustawodawcze)

- **Europejska Rada Ochrony Danych**

# Sankcjonowanie naruszeń przepisów o ochronie danych osobowych

*[ogólna informacja]*

## Rodzaje odpowiedzialności:

- **odpowiedzialność administracyjna**
- **odpowiedzialność karna**
- **odpowiedzialność cywilnoprawna**
- **odpowiedzialność pracownicza i dyscyplinarna**

**Regulacja w RODO**:

rozdział VIII Środki ochrony prawnej, odpowiedzialność i sankcje (art. 77 – 84).

- *Artykuł 77 - Prawo do wniesienia skargi do organu nadzorczego;*
- *Artykuł 78 - Prawo do skutecznego środka ochrony prawnej przed sądem przeciwko organowi nadzorczemu;*

- Artykuł 79 - Prawo do skutecznego środka ochrony prawnej przed sądem przeciwko administratorowi lub podmiotowi przetwarzającemu;
- Artykuł 80 - Reprezentowanie osób, których dane dotyczą;
- Artykuł 81 - Zawieszenie postępowania;
- Artykuł 82 - Prawo do odszkodowania i odpowiedzialność;
- Artykuł 83 - Ogólne warunki nakładania administracyjnych kar pieniężnych.

Artykuł 84 „Sankcje" Państwa członkowskie przyjmują przepisy określające **inne sankcje** za naruszenia niniejszego rozporządzenia, w szczególności za naruszenia niepodlegające administracyjnym karom pieniężnym na mocy art. 83, oraz podejmują wszelkie środki niezbędne do ich wykonania. Sankcje te muszą być skuteczne, proporcjonalne i odstraszające.

## Odpowiedzialność administracyjna

- Odpowiedzialność administracyjna przyjmuje postać **egzekucji administracyjnej** oraz **administracyjnych kar pieniężnych**.
- Egzekucję administracyjną regulują przepisy ustawy o postepowaniu egzekucyjnym w administracji
- Administracyjnych kar pieniężnych, w tym zasady i procedury ich wymierzania reguluje: art. 83 RODO, przepisy ustawy o ochronie danych osobowych oraz przepisy kodeksu postępowania administracyjnego

  W zależności od charakteru naruszenia (rodzaju naruszonego obowiązku) kary pieniężna w wysokości do 10 000 000 EUR lub do 20 000 000 EUR, a w przypadku przedsiębiorstwa - w wysokości do 2 % lub do 4% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego (zastosowanie ma kwota wyższa).

  Państwa członkowskie mogą określić, czy i w jakim zakresie administracyjne kary pieniężne można nakładać na organy i podmioty publiczne ustanowione w tym państwie członkowskim. W Polsce kwestię tę reguluje ustawa o ochronie danych osobowych. Zgodnie z postanowieniami tej ustawy PUODO może nałożyć na określone podmioty zaliczane do kategorii organów i podmiotów publicznych administracyjne kary pieniężne w wysokości, co do zasady, do 100 000 złotych.

## Odpowiedzialność karna

- Wykonywanie niektórych obowiązków z zakresu ochrony danych osobowych zabezpieczone jest za pomocą norm prawa karnego.
- Ustawa o ochronie danych osobowych określa dwa przestępstwa związane z naruszeniem przepisów o ochronie danych osobowych (por. art. 107-108 projektu nowej ustawy o.d.o.)
- Pewne przejawy sprzecznego z prawem przetwarzania danych osobowych mogą wypełniać ustawowe znamiona przestępstw określonych w k.k.:

– przestępstw przeciwko ochronie informacji określonych w rozdziale XXXIII Kodeksu Karnego (zob. art. 265 - 269b k.k.);
– przestępstwa przekroczenia uprawnień lub nie dopełnienia obowiązków przez funkcjonariusza publicznego działającego na szkodę interesu publicznego lub prywatnego (art. 231 § 1 k.k.);
– przestępstwa zniesławienia (art. 212 k.k.), którego przedmiotem jest naruszenie czci i godności człowieka;
– przestępstwa znieważenia (art. 216 k.k.).

## Odpowiedzialność cywilnoprawna

- **RODO**
  - artykuł 79 RODO (Prawo do skutecznego środka ochrony prawnej przed sądem przeciwko administratorowi lub podmiotowi przetwarzającemu);
  - artykuł 82 RODO (Prawo do odszkodowania i odpowiedzialność);
  - por. też artykuł 80 RODO (dot. reprezentowanie osób, których dane dotyczą) oraz artykuł 81 RODO (dot. możliwości zawieszenie postępowania sądowego) – dotyczą kwestii procesowych.
- **Ustawa o ochronie danych osobowych**
  - regulacja określona w art. 92-100 projektu nowej ustawy o ochronie danych osobowych.
- **Kodeks cywilny**
  - odpowiedzialnością deliktowa (art. 415 i n. k.c. regulujące czyny niedozwolone)
  - odpowiedzialność za naruszenie dóbr osobistych (art. 23-24 i 448 k.c.)
  - odpowiedzialność kontraktowa (art. 472 i n. k.c. regulujące skutki niewykonania zobowiązań)

## Odpowiedzialność pracownicza i dyscyplinarna

- W kontekście naruszeń ochrony danych osobowych pracownicy mogą ponosić (poza innymi typami odpowiedzialności) odpowiedzialność pracowniczą i dyscyplinarną.

- **Odpowiedzialność pracownicza** jest uregulowana w Kodeksie pracy i ponoszona przez pracowników niezależnie od podstawy prawnej nawiązania stosunku pracy.
- Odpowiedzialność pracownicza nie ma jednolitego charakteru, w jej ramach należy wyróżnić: odpowiedzialność porządkową (zob. art. 108–113 k.p.) oraz odpowiedzialność materialną ponoszoną, gdy pracownik ze swej winy wyrządził pracodawcy szkodę wskutek niewykonania lub nienależytego wykonania obowiązków pracowniczych (art. 114–127 k.p.).

- **Odpowiedzialności dyscyplinarnej** podlegają tylko niektórzy pracownicy objęci pragmatykami służbowymi, tj. regulacjami odnoszącymi się tylko do ich praw i obowiązków służbowych oraz osoby wykonujące określone zawody zaufania publicznego.