KIPR

ePoradnik

RODO dla NGO

ePoradnik

RODO dla NGO

Warszawa 2019
Konfederacja Inicjatyw Pozarządowych Rzeczypospolitej

Wydanie I, polskie.
Warszawa 2019

rodo.konfederacjaipr.pl

Autor:
Łukasz Dudek

Nadzór merytoryczny i formalny:
Dr Tymoteusz Zych
Dr Klaudia Gawlik-Bugańska
Krystian Owczarek
Karol Handzel

Korekta:
Elżbieta Stryjek

Opracowanie graficzne:
Działania Wizualne – Agencja Kreatywna. Błażej Zych
dzialaniawizualne.pl

ISBN: 978-83-950021-1-3

Wydawnictwo: Konfederacja Inicjatyw Pozarządowych Rzeczypospolitej
ul. S. Jaracza 10/1, Warszawa
konfederacjaipr.pl

Sfinansowano przez Narodowy Instytut Wolności - Centrum Rozwoju Społeczeństwa Obywatelskiego ze środków Programu Fundusz Inicjatyw Obywatelskich na lata 2014 – 2020

SPIS TREŚCI

WSTĘP

Niniejszy poradnik ma na celu przybliżenie problematyki ochrony danych osobowych. W jego treści zamieszczone zostały podstawowe informacje odnoszące się do bezpieczeństwa przetwarzania danych osobowych, poparte licznymi przykładami mającymi na celu wyjaśnienie działań poszczególnych mechanizmów prawnych wynikających z rozporządzenia unijnego, potocznie zwanego RODO. Ponadto w skład poradnika wchodzić będą wzory dokumentów, które to będzie można wykorzystać. Sam poradnik jest adresowany głównie do III sektora i ma na celu zwiększenie świadomości prawnej organizacji wchodzących w jego skład w zakresie ochrony danych osobowych.

CZEMU OCHRONA DANYCH OSOBOWYCH JEST WAŻNA DLA ORGANIZACJI III SEKTORA?

Każda organizacja ma dostęp do danych osobowych, najczęściej są to dane członków oraz ich sympatyków *(np. imiona, nazwiska, numery telefonów czy adresy mailowe)*. W związku z tym faktem, każda organizacja zobowiązana jest do odpowiedniego stosowania zasad bezpieczeństwa oraz przetwarzania danych osobowych określonych w przepisach unijnego rozporządzenia oraz ustawie o ochronie danych osobowych.

Ochrona danych osobowych przetwarzanych przez przeróżne organizacje III sektora jest istotna ze względu na fakt, że te w większości opierają swoje działania na kontakcie między nią samą a odbiorcami jej działań. Bezpośrednim skutkiem takiego działania jest to, że każda z nich posiada pokaźne bazy danych zawierające zazwyczaj m.in. imiona i nazwiska, adresy mailowe, numery telefonów członków tych organizacji oraz ich sympatyków. W związku z posiadaniem przez nie baz danych, muszą one w pełni zapewnić ich bezpieczeństwo oraz bezpieczeństwo przetwarzania tych danych. Proces ten jest skomplikowany i bardzo często kosztowny, w związku z czym dużo małych organizacji nie stać na profesjonalne wdrożenie przepisów unijnego rozporządzenia w zakresie ochrony danych osobowych.

Dlatego też powstał niniejszy poradnik, który ma na celu przybliżenie tematyki ochrony danych osobowych oraz pomoc przy wdrażaniu RODO przez mniejsze organizacje pozarządowe.

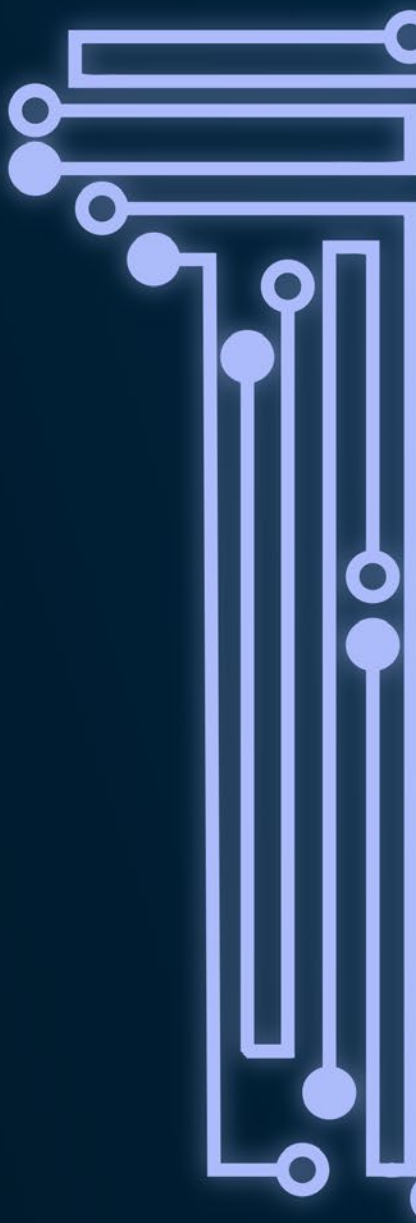
CO TO JEST RODO?

RODO to inaczej Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (inaczej ogólne rozporządzenie o ochronie danych osobowych - RODO). Od 25 maja 2018 r. w Państwach Członkowskich UE zmieniły się wymogi dotyczące przetwarzania danych osobowych. Wdrożenie RODO wynikało po pierwsze z konieczności dostosowania przepisów do rozwoju technologii a po drugie z potrzeby wprowadzenia jednolitych zasad ochrony danych osobowych we wszystkich państwach Unii Europejskiej.

RODO ma na celu wzmocnienie podstawowych praw obywateli w epoce cyfrowej i ułatwienie przedsiębiorstwom i organizacjom działania na wspólnym rynku. RODO ma zastosowanie od 25 maja 2018 r.

Rozdział

Co to są dane osobowe?



KIPR

CO TO SĄ DANE OSOBOWE?

W dzisiejszych czasach kontakt pomiędzy poszczególnymi osobami nie stanowi żadnego wyzwania. Wystarczy wyciągnąć telefon komórkowy i zadzwonić, wysłać SMS, mail albo skorzystać z jednego z kilku portali społecznościowych, aby skontaktować się z drugą osobą.

Organizacje III sektora, które w znaczącej mierze opierają swoje funkcjonowania na działalności społecznej, kładą duży nacisk na prowadzenie jak najefektywniejszego kontaktu pomiędzy swoimi członkami a odbiorcami ich działań oraz sympatykami.

CZYM SĄ DANE OSOBOWE?

Dane osobowe – oznaczają informację o **zidentyfikowanej** lub **możliwej do zidentyfikowania** osobie fizycznej.

- **Zidentyfikowana osoba fizyczna** – jest to osoba, którą możemy bezpośrednio zidentyfikować na podstawie dostępnych informacji;

- **Możliwa do zidentyfikowania osoba fizyczna** – jest to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak:

  a) imię i nazwisko;
  b) numer identyfikacyjny;
  c) dane o lokalizacji;
  d) identyfikator internetowy
  e) jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

Oznacza to, że dane osobowe oznaczają każdą informację, która umożliwia zidentyfikowanie danej osoby!

Przykłady danych osobowych:

a) imię i nazwisko
b) numer telefonu
c) adres domowy
d) data urodzenia
e) numer PESEL
f) wizerunek
g) adres mailowy

Przykłady danych osobowych w NGO:

a) imiona i nazwiska członków organizacji, wolontariuszy, mecenasów, pracowników;
b) adresy zamieszkania/korespondencji członków organizacji, wolontariuszy, mecenasów, pracowników;
c) numery telefonów członków organizacji, wolontariuszy, mecenasów, pracowników;
d) dokumentacja finansowa organizacji (zawierająca imiona i nazwiska, numery PESEL, numery rachunków bankowych oraz adresy zamieszkania)
e) zdjęcia z wizerunkami członków organizacji opublikowane na stronie internetowej.

Dane osobowe dzielą się również na **dwa rodzaje**, co do których odnoszą się inne zasady przetwarzania.

Wyróżniamy:

1) **Dane zwykłe** – są to wszystkie dane osobowe, które nie należą do szczególnych kategorii danych (danych wrażliwych). Ich przetwarzanie oparte jest na zwykłych zasadach. *(np. imię i nazwisko, numer telefonu, numer PESEL, adres mailowy)*

2) **Dane szczególnych kategorii** (zwane dalej **danymi wrażliwymi**) – RODO przewiduje **zamknięty katalog szczególnych kategorii danych**, których przetwarzanie jest zabronione poza sytuacjami wymienionymi w unijnym rozporządzeniu. Należą do nich:

   a) pochodzenie rasowe lub etniczne;
   b) poglądy polityczne;
   c) przekonania religijne lub światopoglądowe;
   d) przynależność do związków zawodowych;
   e) przetwarzanie danych genetycznych;
   f) przetwarzanie danych biometrycznych w celu jednoznacznej identyfikacji osoby fizycznej;
   g) przetwarzanie danych dotyczących zdrowia
   h) przetwarzanie danych dotyczących seksualności lub orientacji seksualnej osoby fizycznej.

Co do zasady nie można ich przetwarzać, chyba że zachodzi któryś z wyjątków określonych w art. 9 RODO *(m.in. zgoda osoby, której dane dotyczą; 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; przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą).*

W odniesieniu do organizacji NGO należy wskazać również, że unijny ustawodawca przewidział, że zakaz przetwarzania danych wrażliwych nie ma zastosowania jeżeli *„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."*

Zakres podmiotowy omawianego wyjątku jest na tyle szeroki, że bez problemu mieszczą się w nim wszelkie organizacje NGO. Przy czym wyraźnie należy zaznaczyć, aby miał on zastosowanie, muszą być spełnione łącznie dwie przesłanki:

1) Obowiązek stosowania wszelkich przepisów dotyczących zabezpieczenia danych osobowych *(art. 32 i nast. unijnego rozporządzenia)* oraz wdrożenie w organizacji określonych metod zarządzania ryzykiem i bezpieczeństwem danych osobowych.

2) Istnienie wyłącznie wewnętrznego charakteru wykorzystania danych wrażliwych *(oznacza to, że dane wrażliwe nie powinny być ujawniane poza podmiotem, który je przetwarza, chyba że osoba, której dane podlegają przetwarzaniu, wyrazi na to zgodę.)*

Zakres przedmiotowy ogranicza możliwość przetwarzania danych do członków, byłych członków oraz osób utrzymujących stały kontakt z organizacją w związku z realizacją jej celów.

> ***Przykład****: Stowarzyszenia mogą przetwarzać dane osobowe członków, sympatyków oraz osób, które finansowo wspierają stowarzyszenie (np. darczyńców czy osób przekazujących 1% podatku na realizacje celów statutowych).*

Podsumowując, należy zapamiętać, że o ile przetwarzanie danych zwykłych nie pociąga za sobą dodatkowych warunków przewidzianych przez przepisy unijne, tak przetwarzanie danych wrażliwych pociąga za sobą szereg skomplikowanych warunków wraz z koniecznością zastosowania dodatkowych zabezpieczeń, przy czym jednak występują pewne wyjątki, w zakresie których znajdą się organizacje NGO.

Rozdział 2

Przetwarzanie danych osobowych

KIPR

PRZETWARZANIE DANYCH OSOBOWYCH

Jak już wcześniej było wspomniane, każda organizacja przetwarza dane osobowe. Udało się również określić, czym są dane osobowe oraz wskazać ich rodzaje. Następnym krokiem do prawidłowego zrozumienia problematyki ochrony danych osobowych będzie wyjaśnienie pojęcia **„przetwarzania danych osobowych"**.

CZYM JEST PRZETWARZANIE DANYCH OSOBOWYCH?

Przetwarzanie danych osobowych – *oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany.*

Przetwarzanie to:

a) zbieranie,
b) utrwalanie,
c) organizowanie,
d) porządkowanie,
e) przechowywanie,
f) adaptowanie lub modyfikowanie,
g) pobieranie,
h) przeglądanie,
i) wykorzystywanie,
j) ujawnianie poprzez przesyłanie,
k) rozpowszechnianie lub innego rodzaju udostępnianie,
l) dopasowywanie lub łączenie,
m) ograniczanie
n) usuwanie lub niszczenie.

Można więc przyjąć, że jakakolwiek operacja dokonywana na danych osobowych przez organizację NGO będzie stanowiła proces przetwarzania danych osobowych!

Aby łatwiej zrozumieć, czym jest przetwarzanie danych osobowych poniżej, zostanie zaprezentowane kilka przykładów zarówno w odniesieniu do działalności zwykłej, jak i tej w III sektorze.

Przykłady przetwarzania danych osobowych:

a) proces rekrutacji (dane osobowe są przetwarzane poprzez zbieranie CV oraz późniejszy kontakt z wybranymi osobami w celu zatrudnienia);
b) monitoring miejski (dane osobowe w postaci naszego wizerunku są przetwarzane poprzez nagrywanie nas w określonym miejscu);
c) marketing bezpośredni (dane osobowe są przetwarzane w celu kontaktu z klientami i oferowaniu im nowych usług);
d) usuwanie dokumentów w przeznaczonej do tego niszczarce
e) wysłanie maila do kontrahenta.

Przykłady przetwarzania danych osobowych w NGO:

a) ewidencjonowanie członków organizacji (przetwarzaniem danych będzie stworzenie arkusza kalkulacyjnego zawierającego dane kontaktowe do poszczególnych członków organizacji);
b) kontakt z członkami organizacji (przetwarzaniem danych będzie wykorzystywanie numerów telefonu oraz adresów email do kontaktu z poszczególnymi członkami organizacji);
c) przesyłanie newslettera (przetwarzaniem będzie zbieranie i przechowywanie adresów mailowych sympatyków organizacji, aby później przesłać im newsletter);
d) rejestrowanie obrazu podczas szkoleń (przetwarzaniem danych będzie robienie zdjęć podczas szkoleń, eventów czy happeningów a następnie publikowanie ich na stronie internetowej organizacji bądź w jej mediach społecznościowych);
e) zbieranie danych wolontariuszy zaangażowanych w działalność organizacji;
f) wprowadzanie danych darczyńcy, beneficjenta do bazy kontaktów, systemu informatycznego obsługiwanego przez daną fundację, stowarzyszenia
g) wysłanie do darczyńcy listu z podziękowaniem za dokonaną darowiznę;

UWAGA: Członkowie organizacji – Definiując to pojęcie, należy rozróżnić znaczenie *sensu stricto* oraz *sensu largo*.

a) Członek organizacji *sensu stricto* – w wąskim znaczeniu tego pojęcia znajdą się przede wszystkim osoby bezpośrednio powiązane z daną organizacją poprzez łączący je stosunek prawny: *m.in. członkowie stowarzyszenia, członkowie organów stowarzyszenia, fundatorzy fundacji, członkowie organów fundacji, etc.*

b) Członek organizacji *sensu largo* – w szerokim znaczeniu tego pojęcia należy umieścić *m.in. sympatyków, darczyńców, osoby przekazujące 1 % podatku na realizację działalności statutowej, członków honorowych, osoby zapisane na newsletter, etc.*

> ***Przykład:*** *Jeżeli podczas prowadzonego przez organizację wydarzenia (np. wykładu), zostanie puszczona w obieg lista w celu zapisania adresu mailowego do jej newslettera, dochodzi do procesu przetwarzania danych osobowych wszystkich osób, które wpisały się na tę listę.*

W związku z powyższym należy zapamiętać, że przetwarzaniem danych osobowych jest jakiekolwiek działanie przeprowadzane na poszczególnych danych. Oznacza to, że organizacje przetwarzają dane osobowe praktycznie cały czas. W związku z tym wszystkie one objęte są regulacjami unijnego rozporządzenia oraz podlegają karom, jeżeli dojdzie do naruszenia bezpieczeństwa danych osobowych.

Ciekawostka:

- Niszczenie danych jest również traktowane jako przetwarzanie danych osobowych. Oznacza to, że jeżeli członkowie organizacji postanowią zniszczyć listę mailową sympatyków poprzez zniszczenie jej w niszczarce, cały ten proces będzie stanowił przetwarzanie danych!

- Jako przetwarzanie danych osobowych nie będzie traktowane zrobienie zdjęcia uczestnikom prowadzonego przez organizację wydarzenia, w sytuacji gdy wizerunek osób na nim uwiecznionych będzie stanowił jedynie fragment większej całości *(krajobrazu, zgromadzenia, imprezy masowej)*.

ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

Unijne rozporządzenie wprowadza szereg zasad, którym podlega przetwarzanie danych osobowych. Zasady te obejmują każdą organizację, która przetwarza dane osobowe. Co więcej, każda z nich musi być w stanie wykazać, że zapewniła wszelkie gwarancje, aby zapewnić jak najpełniejszą realizację tych zasad podczas przetwarzania danych.

Wyróżnia się siedem głównych zasad przetwarzania danych osobowych, które muszę być w pełni realizowane przez każdą organizację.

1. **Zasada zgodności z prawem**
2. **Zasada celowości**
3. **Zasada minimalizacji danych**
4. **Zasada prawidłowości**
5. **Zasada ograniczenia czasowego**
6. **Zasada bezpieczeństwa**
7. **Zasada rozliczalności**

ZASADA ZGODNOŚCI Z PRAWEM

W istocie są to trzy zasady skompensowane w *jednej (zasada legalności, rzetelności oraz przejrzystości)*.

Zasada legalności wprowadza obowiązek, z którego wynika, że dane osobowe muszą być przetwarzane zgodnie z prawem (w szczególności z RODO oraz krajowymi przepisami).

Oznacza to, że dane osobowe mogą być przetwarzane wyłącznie w sytuacji, w której podmiot przetwarzający posiada określoną podstawę prawną do przetwarzania danych.

Przykłady:

a. Przetwarzanie następuje na podstawie zgody, osoby której dane są przetwarzane;
b. Przetwarzanie następuje na podstawie prawnie uzasadnionego interesu
c. Przetwarzanie wynika z obowiązku prawnego ciążącego na administratorze.
d. Np. Zasada legalności zostanie zrealizowana, gdy uzyska się od konkretnej osoby pisemną zgodę na przetwarzanie jej danych osobowych albo gdy organizacja przetwarza dane osoby, z którą ma zawrzeć umowę.

Zasada rzetelności nakazuje wykorzystywać dane osobowe uczciwie i rzetelnie. Oznacza to, że przetwarzane dane powinny być przetwarzane zgodnie z tym do czego się zobowiązał się podmiot przetwarzający dane osobowe.

Przykład: *Jeżeli organizacja pozyskała adresy mailowe i numery telefonów w celu prowadzenia rekrutacji na stanowisko fundraisera, to nie może wydzwaniać do tych osób z ofertami marketingowymi czy przesyłać newslettera.*

Zasada przejrzystości wskazuje, że przetwarzanie danych osobowych musi być czytelne i zrozumiałe dla podmiotu, którego dane są przetwarzane. Oznacza to, że każdy, kogo dane osobowe ulegają przetwarzaniu, ma możliwość żądania wskazania celu i podstawy prawnej przetwarzania jego danych.

Przykład: *Każdy sympatyk fundacji otrzymujący newsletter, ma prawo wystąpić do administratora (fundacji) o wskazanie, na jakiej podstawie i w jakim celu przetwarza on jego dane osobowe.*

Zrozumiałość przetwarzania danych osobowych odnosi się zaś do komunikacji pomiędzy administratorem a podmiotem, którego dane osobowe są przetwarzane. Przyjmuje się, że komunikacja ta powinna być **prowa-**

dzona za pośrednictwem jasnego i czytelnego języka, czyli w sposób zrozumiały dla osoby, której dane są przetwarzane.

> ***Przykład:*** *Wszelkie klauzule informacyjne oraz klauzule zgody powinny być sformułowane w taki sposób, aby każdy mógł się z nimi wystarczająco zapoznać. Oznacza to, że nie powinny być one zawiłe, skomplikowane oraz charakteryzujące się wyłącznie językiem prawniczym.* ***Powinien zrozumieć je typowy odbiorca, do którego te klauzule są kierowane.***

Podsumowując – aby organizacja realizowała w pełni zasadę zgodności z prawem, musi ustalić, czy przy przetwarzaniu danych osobowych występują 3 przesłanki:

a) Dane osobowe są przetwarzane zgodnie z prawem;
b) Dane są przetwarzane rzetelnie i uczciwie
c) Przetwarzanie danych osobowych jest czytelne i zrozumiałe dla osoby, której dane podlegają przetwarzaniu.

ZASADA CELOWOŚCI

Dane mogą być zbierane tylko w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami.

Oznacza to, że administrator musi precyzyjnie wskazywać cele, w jakich przetwarza dane osobowe. W związku z czym nie może on pominąć ani zataić żadnego celu, do którego chciałby wykorzystać dane.

Zasada ta jest ściśle powiązana z obowiązkiem informacyjnym ciążącym na administratorze. Wynika to z faktu, że administrator musi każdorazowo poinformować osobę o celach, dla których przetwarza jej dane.

> ***Przykład:*** Organizacja prowadzi rekrutację a następnie, na podstawie danych pozyskanych w procesie rekrutacji, przesyła newsletter.

WAŻNE – Należy za każdym razem precyzyjnie wskazywać cel przetwarzania danych osobowych.

ZASADA MINIMALIZACJI DANYCH

Dane powinny być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane. Administrator powinien przetwarzać tylko takiego rodzaju dane i tylko o takiej treści, które są niezbędne ze względu na cel zbierania danych. Każdy rodzaj zbieranych danych administrator powinien uzasadnić potrzebą (celem) ich zbierania.

***Przykład**: Organizacja zbiera dane osobowe od swoich sympatyków w celu przesyłania newslettera. W takiej sytuacji może ona wystąpić o takie dane jak: imię, nazwisko czy adres mailowy. Prośba o podanie numeru PESEL, numeru telefonu czy adresu zamieszkania naruszałoby zasadę minimalizacji danych.*

ZASADA PRAWIDŁOWOŚCI

Dane muszą być prawidłowe i w razie potrzeby uaktualniane. Należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów i ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane.

Zasada ta wprowadza obowiązek monitorowana, czy przetwarzane dane osobowe są aktualne. Oznacza to, że administrator powinien co jakiś czas sprawdzać, czy dane, które posiada w swoich bazach, są aktualne i czy nie wygasł czas na jaki zostały one udostępnione. W razie wykrycia nieprawidłowości, powinien on je uaktualnić, poprawić lub usunąć.

***Przykład:** Organizacja, która wysyła newslettery lub kontaktuje się za pośrednictwem maili z członkami lub sympatykami, co jakiś czas powinna sprawdzać, czy przesyłane treści dochodzą do adresatów.*

Naruszeniem tej zasady jest wykorzystywanie starej bazy mailowej i wysyłanie za jej pośrednictwem maili na adresy, z których wracają zwrotki, że adres jest nieaktualny. W takiej sytuacji powinien być on niezwłocznie usunięty z bazy danych.

Zasada powyższa nakłada na organizację obowiązek, aby cały czas badała, czy przetwarzane przez nią dane osobowe są zgodne z prawdą oraz aktualne, w razie gdyby nie były, musi powziąć odpowiednie środki, aby ten stan przywrócić!

ZASADA OGRANICZENIA CZASOWEGO

Dane osobowe muszą być przechowywane w formie umożliwiającej identyfikację osoby, której dotyczą, przez okres nie dłuższy niż jest to niezbędne do celów, w których dane te są przetwarzane.

Z zasady tej wynika obowiązek administratora do klarownego określenia czasu, przez który będzie przetwarzał dane osobowe. Dodatkowo, ciąży na nim obowiązek wskazania w klauzuli informacyjnej przez jaki czas będzie przetwarzał dane osobowe.

WAŻNE – zasada ta nakłada na organizację jeden z ważniejszych obowiązków informacyjnych względem osoby, której dane będą przetwarzane. Musi ona wskazać przez jaki okres te dane będą przetwarzane.

Przyjmuje się również, że dalsze przetwarzanie danych osobowych w celach:

a) *archiwalnych w interesie publicznym,*
b) *prowadzenia badań naukowych lub historycznych*
c) *prowadzenia statystki*

nie jest uznawane za niezgodne z pierwotnymi celami!

ZASADA BEZPIECZEŃSTWA

Dane muszą być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym m.in. ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.

RODO wymaga od podmiotów, aby zagwarantowały odpowiedni poziom bezpieczeństwa poprzez zapewnienie poufności i integralności wszelkich danych osobowych.

Przyjmuje się, że bezpieczeństwo informacji składa się z trzech cech: **poufności, integralności** oraz **dostępności.**

Poufność polega na tym, że do informacji nie ma dostępu osoba nieupoważniona. Chodzi więc o to, żeby osoby niepowołane nie miały dostępu do informacji a w szczególności, aby dane osobowe nie wyciekły na zewnątrz oraz żeby osoba niepowołana nie dostała się do danych w miejscu ich przechowywania.

Przykłady:

a. Zgubienie telefonu komórkowego z dostępem do numerów telefonów i adresów mailowych do sympatyków organizacji.
b. Zgubienie dysku zewnętrznego z dokumentami oraz bazami danych kontaktowych organizacji.

WAŻNE – Zabezpieczenie poufności będzie zapewnione poprzez szereg działań mających na celu zmniejszenie ryzyka wycieku danych. Za najlepsze rozwiązania dla organizacji można przyjąć: *stosowanie polityki czystego biurka, prowadzenie rejestru czynności przetwarzania oraz baz danych, wdrożenie polityki ochrony danych, wylogowywanie się z systemu po zakończeniu określnej czynności.*

Integralność oznacza, że informacja nie zostanie zmieniona w sposób nieupoważniony czy też zniszczona.

> ***Przykład:*** *Nieuprawniony pracownik organizacji uzyska przez przypadek dostęp do baz danych kontaktowych i skopiuje dla siebie numery telefonów i adresy mailowe jej sympatyków.*

WAŻNE - Zabezpieczenie integralności będzie zapewnione poprzez szereg działań; *m.in. stosowanie polityki czystego biurka, częste zmiany haseł, zamykanie na klucz pomieszczeń z dokumentami, prowadzenie rejestru czynności przetwarzania danych, wdrożenie polityki ochrony danych.*

Dostępność polega na tym, że informacja jest dostępna tylko osobom upoważnionym.

> ***Przykłady:*** *Prowadzenie rejestru osób upoważnionych do przetwarzania określonych kategorii danych osobowych oraz przyznanie dostępu np. przy użyciu klucza, indywidualnego identyfikatora, loginu do miejsc, w których przechowywane są dane osobowe tylko upoważnionym osobom.*

Podsumowując: Pełna realizacja zasady bezpieczeństwa w danej organizacji będzie opierała się na wdrożeniu kilku podstawowych procedur, mających na celu zwiększenie bezpieczeństwa przetwarzania danych osobowych. Każda z nich powinna *m.in. przyjąć swoją politykę ochrony danych, prowadzić rejestry czynności przetwarzania danych osobowych czy podmiotów przetwarzających, odpowiednio zabezpieczać bazy danych.*

ZASADA ROZLICZNOŚCI

Administrator jest odpowiedzialny za przestrzeganie przepisów i musi być w stanie wykazać ich przestrzeganie.

Konsekwencją przyjęcia tej zasady jest przeniesienie na administratora ciężaru udowodnienia, że zapewnił odpowiedni poziom ochrony danych osobowych w danej organizacji, zgodny z przepisami RODO i ustawą krajową. Oznacza to, że administrator jest odpowiedzialny za wdrożenie odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie danych osobowych odbywało się z zgodzie z przepisami prawa. Co więcej, musi mieć on możliwość wykazanie tego.

Podsumowując: Każda organizacja będzie indywidualnie rozliczana ze środków bezpieczeństwa, jakie wprowadziła. Unijne rozporządzenie na narzuca sposobu zabezpieczenia procesu przetwarzania danych osobowych, a w razie jego naruszenia, to ona będzie musiała wykazać, że dopełniła wszelkich starań, aby do niego nie doszło. W związku z tym zaleca się, aby każda organizacja co najmniej:

a) ustanowiła politykę ochrony danych osobowych,
b) ustanowiła instrukcję zarządzania systemem informatycznym
c) przeprowadziła ocenę skutków dla ochrony danych.

Należy mieć jednak na uwadze, że każdy z administratorów danych powinien obowiązkowo:

a) Prowadzić i aktualizować rejestr czynności przetwarzania danych;
b) Prowadzić i aktualizować rejestr podmiotów przetwarzających (prowadzić tzw. rejestr procesora);
c) Na bieżąco analizować ryzyka naruszenia danych osobowych w ramach własnej organizacji
d) Upoważnić pracowników lub osoby współpracujące do przetwarzania danych *(zał. 2 – wzór upoważnienia do przetwarzania danych osobowych).*

> ***Przykład:*** *Organizacja postanowiła rozszerzyć swoją działalność o nowy projekt edukacyjny. Tym razem opierać miałby się on na edukacji historycznej. W celu realizacji projektu, jeden z jej członków zgłosił się do podjęcia funkcji jego koordynatora. Następnie został on zaakceptowany i aby mógł przetwarzać dane osobowe uczestników nowego projektu organizacji, został upoważniony do przetwarzania danych osobowych w tym zakresie. Oznacza to, że został on podmiotem przetwarzającym dane osobowe.*

Rozdział 3

Podstawa przetwarzania danych osobowych

KIPR

PODSTAWA PRZETWARZANIA DANYCH OSOBOWYCH

Zgodnie z przepisami unijnego rozporządzenia przetwarzanie danych osobowych musi opierać się na co najmniej jeden przesłance wskazanej w jego treści.

Oznacza to, że jeżeli organizacja wykaże co najmniej jedną z 6 podstawowych przesłanek przetwarzania danych, będzie ono legalne.

W odniesieniu do katalogu przesłanek umożliwiających przetwarzanie danych osobowych „zwykłych" możemy zaliczyć:

1. Zgoda osoby, której dane dotyczą;
   1a) Przetwarzanie danych nieletnich;
2. Czynności niezbędne do zawarcia lub wykonania umowy;
3. Niezbędność do wypełnienia obowiązku prawnego ciążącego na administratorze;
4. Ochrona żywotnych interesów osoby;
5. Czynności niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi
6. Prawnie uzasadniony interes administratora lub osoby trzeciej.

ZGODA NA PRZETWARZANIE DANYCH OSOBOWYCH

Przyjmuje się, że zgodą jest dobrowolne, świadome, konkretne i jednoznaczne okazanie woli osoby, której dane dotyczą. Zgoda powinna przyjąć formę oświadczenia lub działania wyraźnie potwierdzającego przetwarzanie jej danych osobowych.

Aby zgoda była wiążąca, powinna spełniać następujące przesłanki:

a) **Dobrowolność** - *osoba zainteresowana wyrażeniem zgody musi mieć możliwość dokonania wyboru, zgoda nie może być w żaden sposób wymuszona. Przyjmuje się również, że odmowa wyrażenia zgody nie może powodować negatywnych konsekwencji dla osoby zainteresowanej;*
b) **Konkretność** - *zgoda musi precyzyjnie określać cel przetwarzania danych. Niedopuszczalne są zgody o charakterze ogólnym czy nieprecyzyjnym;*
c) **Świadomość** - *polega na dostarczeniu osobie zainteresowanej wyrażeniem zgody wszelkich informacji umożliwiających jej podjęcie świadomej decyzji a w szczególności zrozumienia treści zgody. Oznacza to, że wszelkie obowiązki informacyjne należy dopełnić przy użyciu jasnego, precyzyjnego i prostego języka;*

d) **Jednoznaczność** - *zgoda powinna być wyrażona w jednoznaczny sposób poprzez złożenie stosownego oświadczenia lub wyraźne działanie potwierdzające. Nie można powoływać się na dorozumianą zgodę!*

Przyjmuje się, że zgoda może być wyrażona w dowolnej formie. Przy czym należy wyraźnie zaznaczyć, że administrator ma obowiązek w razie kontroli wykazać, że taka zgoda została udzielona. Dlatego też zgoda co do zasady powinna przybrać formę możliwą do udokumentowania.

Przykłady udzielenia zgody:

a) *Zaznaczenie checkboxa;*
b) *Wybór ustawień technicznych;*
c) *Przesłanie maila/skanu ze zgodą;*
d) *Pisemne oświadczenie;*
e) *Nagranie oświadczenia o wyrażeniu zgody udzielonej w rozmowie telefonicznej;*
f) *Kliknięcie linku weryfikacyjnego w wiadomości e-mail w ramach weryfikacji dwuetapowej;*
g) *Wrzucenie wizytówki do wyznaczonego pojemnika w celu wzięcia udziału w losowani.*
h) *Wysłanie CV zawierającego zdjęcie kandydata do pracy.*

UWAGA: "Milcząca" odpowiedź na maila nie może być traktowana jako zgoda! Zgoda nie może być również częścią innego oświadczenia np. regulaminu!

Osoba udzielająca zgody na przetwarzanie danych osobowych, powinna mieć możliwość wycofania zgody w dowolnym momencie. Co więcej, przyjmuje się, że cofnięcie zgody powinno być tak samo łatwe jak jej udzielenie!

Zgoda, mając szczególny charakter i cechy omówione wyżej, powinna być stosowana ze szczególną ostrożnością w przypadku, gdy administrator nie może zastosować innej podstawie przetwarzania danych.

Dlatego też warto zapoznać się z wzorem przykładowej zgody na przetwarzanie danych osobowych. *(zał. 1 – wzór zgody na przetwarzanie danych osobowych)*.

PRZETWARZANIE DANYCH NIELETNICH

W przypadku przetwarzania danych osobowych dzieci, które nie ukończyły 16 roku życia, w ramach usług społeczeństwa informacyjnego oferowanych bezpośrednio takiemu dziecku, należy pozyskać zgodę osoby sprawującej władzę rodzicielską lub opiekę nad dzieckiem.

Bardzo dużo organizacji społecznych (fundacji i stowarzyszeń) coraz częściej kieruje swoją ofertę do młodzieży. W związku tym ich władze muszą być świadome faktu, że jeżeli chcą przetwarzać dane osobowe dzieci, które nie ukończyły 16 roku życia, **muszą pozyskać zgodę ich rodzica bądź opiekuna prawnego!**

Przykład: *Fundacja prowadzi projekt edukacyjny skierowany do młodzieży. Projekt obejmuje dzieci w wieku 15 – 18 lat. Podczas realizowanego projektu uczniowie poszerzają swoją wiedzę z zakresu ekonomii. Osoby zainteresowane mogą wpisać się na listę, dzięki której będą otrzymywały na maila newsletter fundacji, zawierający atrakcyjne treści dydaktyczne. Należy zaznaczyć, że uczniowie będący uczestnikami projektu, którzy nie ukończyli 16 roku życia, będą musieli posiadać zgodę rodziców na przesyłanie im newslettera!*

CZYNNOŚCI NIEZBĘDNE DO ZAWARCIA LUB WYKONANIA UMOWY

Przesłanka ta obejmuje dwie sytuacje:

a) Przetwarzanie danych jest niezbędne do podjęcia działań jeszcze przed zawarciem umowy, przy czym, istotne jest to, aby przetwarzanie odbywało się na żądanie osoby której dane dotyczą.
b) Przetwarzanie danych osobowych jest niezbędne do wykonania umowy.

Przesłanka ta jest zarezerwowana głównie dla sytuacji związanych z koniecznością zawarcia umowy.

Jeżeli organizacja zamierza zawrzeć z innym podmiotem umowę, ma ona prawo przetwarzać dane osobowe tego podmiotu, nie trzeba uzyskiwać odrębnej zgody. Ponadto, może ona również przetwarzać dane osobowe, które są niezbędne do tego, aby umowa została prawidłowo wykonana, np. przekazanie faktury do księgowości obsługującej administratora celem jej zapłaty i zaksięgowania

UWAGA: Powyższa przesłanka upoważnia tylko do przetwarzania danych wyłącznie osoby, która jest stroną umowy.

Należy więc przyjąć, że przetwarzanie danych w celu zawarcia lub wykonania umowy **ogranicza się wyłącznie do przetwarzania danych, które są niezbędne dla wywiązania się przez strony zobowiązań przewidzianych w umowie.**

Przykład: *Fundacja, na podstawie umowy zlecenia, zamierza podjąć współpracę z Adamem na wykonywanie czynności fundraisingu,. Jej władze wystąpiły do niego, aby ten podał im swoje dane osobowe niezbędne do zawarcia umowy (m.in. imię, nazwisko, adres zamieszkania). Adam powinien im przesłać te dane, co więcej fundacja nie musi uzyskiwać pisemnej zgody na przetwarzanie jego danych. Przetwarzanie ich zawiera się w omawianej przesłance.*

OBOWIĄZEK WYNIKAJĄCY Z PRZEPISÓW PRAWA

Dopuszczalne jest przetwarzanie danych osobowych, jeżeli jest to niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze.

Elementem niezbędnym dla ważności tej przesłanki jest jej połączenie z właściwym przepisem prawa krajowego lub unijnego, który kreuje konkretny obowiązek prawny ciążący na administratorze.

Konstytucja RP jasno wskazuje, że nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby. Oznacza to, że powyższa przesłanka może być zastosowana wyłącznie jeżeli obowiązek prawny ma swoje źródło w przepisie prawa.

Przesłanka ta obejmuje m.in. przetwarzanie danych osobowych przez organy administracji publicznej *(np. ubezpieczenia społeczne, rejestry policji).*

OCHRONA ŻYWOTNYCH INTERESÓW OSOBY

Unijne przepisy zezwalają na przetwarzanie danych, gdy jest to niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą lub innej osoby fizycznej.

Przyjmuje się, że żywotnymi interesami podmiotów danych są takie interesy, **które mają istotne znaczenie dla życia konkretnej osoby** (są to sytuacje, w których występuje konieczność ratowania życia, zdrowia oraz ochrony majątku, czy też katastrofy naturalne).

UWAGA: Żywotny interes innej osoby fizycznej zasadniczo powinien być podstawą przetwarzania danych osobowych wyłącznie w przypadkach, gdy ewidentnie przetwarzania tego nie da się oprzeć na innej podstawie prawnej. Oznacza to, że powyższa przesłanka ma charakter awaryjnej podstawy przetwarzania danych osobowych!

CZYNNOŚCI NIEZBĘDNE DO WYKONANIA ZADANIA REALIZOWANEGO W INTERESIE PUBLICZNYM LUB W RAMACH SPRAWOWANIA WŁADZY PUBLICZNEJ POWIERZONEJ ADMINISTRATOROWI

Kolejna przesłanka przetwarzania danych osobowych obejmuje sytuacje, w których przetwarzanie danych osobowych jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.

Przyjmuje się, że zarówno w sytuacjach zadania, jak i sprawowania władzy publicznej muszą zostać one sprecyzowane w przepisach krajowych bądź unijnych. Dopiero wystąpienie takiej podstawy prawnej zadania publicznego będzie legalizowało zastosowanie tej przesłanki.

PRAWNIE UZASADNIONY INTERES ADMINISTRATORA LUB OSOBY TRZECIEJ

Ze względu na prawidłowe funkcjonowanie każdej organizacji jest to istotna przesłanka, umożliwiająca przetwarzanie danych osobowych.

Aby można było bezpiecznie wykorzystywać powyższą przesłankę, **muszą zostać spełnione łącznie** dwa następujące warunki:

a) Przetwarzanie musi być niezbędne do realizacji konkretnego celu wynikającego z prawnie uzasadnionych interesów administratora lub osoby trzeciej;
b) Interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych nie są w danym przypadku nadrzędne wobec interesu danego podmiotu wymagającego przetwarzania danych osobowych.

Przyjmuje się, że chodzi tutaj o interes prawnie uzasadniony. Co więcej, w tym przypadku **pojęcia „prawnie" nie należy utożsamiać** z koniecznością legitymowania się podstawą prawną wynikającą z przepisów prawa krajowego czy unijnego.

Za uzasadniony cel przetwarzania danych osobnych przyjmuje się ten, który wynika np. z realizacji celów statutowych fundacji bądź stowarzyszenia.

Przykłady:

a) *Prowadzenie ewidencji korespondencji przychodzącej i wychodzącej;*
b) *Rozpatrywanie skarg członków organizacji przez organy kontrolne organizacji*
c) *Kontakt z członkami organizacji, wraz z przesyłaniem zaproszeń do udziału w obradach jej organów.*

Przykład: *Stowarzyszanie prowadzi ewidencję swoich członków. W ewidencji przetwarzane są m.in. następujące dane: imiona i nazwiska, numery telefonów, adresy mail, adresy korespondencyjne, status członka czy kwestia opłacenia składek. Stowarzyszenie co roku wysyła do wszystkich aktywnych członków stowarzyszenia zaproszenie na walne zgromadzenie członków m.in. celem wyboru nowych władz. Przetwarzanie tych danych w postaci przesyłania zaproszeń jest oparte właśnie o przesłankę prawnie uzasadnionego interesu administratora.*

PROFILOWANIE

Automatyczne przetwarzanie danych osobowych w celu podjęcia decyzji nazywane jest potocznie profilowaniem. Automatyczne przetwarzanie danych osobowych staje się coraz popularniejszym zjawiskiem, pozwalającym dokonać analizy zebranych danych osobowych i wyciągnięciu z nich odpowiednich wniosków (np. żeby spersonalizować reklamy)

Profilowanie zostało zdefiniowane, *jako dowolna forma zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystywaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodność, zachowania, lokalizacji lub przemieszczania się.*

Profilowanie więc opiera się na tworzeniu profili osobowościowych, które pozwalają na dokonywanie oceny wybranych aspektów odnoszących się do konkretnej osoby.

Odwołując się do pojęcia profilowania, należy również wskazać, że występują dwa jego rodzaje.

1) Profilowanie zwykłe – samo w sobie jest jedną z czynności przetwarzania danych osobowych podczas której występuje efekt w postaci oceny niektórych czynników osobowych. Polega to w szczególności na analizie i prognozie (*wyciąganiu wniosków na przyszłość*) aspektów dotyczących tej osoby. Istotny jest również fakt, że profilowanie zwykłe odbywa się z udziałem czynnika ludzkiego. **W skrócie: na podstawie danych osobowych określona osoba dokonuje oceny lub prognozy postępowania osoby, której dane są przetwarzane.**

2) Profilowanie kwalifikowane – tak samo jak profilowanie zwykłe jest jedną z czynności przetwarzania danych osobowych podczas której występuje efekt w postaci oceny niektórych czynników osobowych. Polega to w szczególności na analizie i prognozie (*wyciąganiu wniosków na przyszłość*) aspektów dotyczących tej osoby. Różnica polega jednak na tym, że całego procesu oceny oraz podjęcia decyzji dokonują programy komputerowe.

Aby zakwalifikować przetwarzanie danych osobowych jako profilowanie, muszą być spełnione trzy warunki:

1) Przetwarzanie jest w pełni zautomatyzowane (opiera się na algorytmach);
2) Przetwarzanie jest dokonywane na danych osobowych
3) Efektem przetwarzania jest ocena osobistych cech osoby fizycznej służących danym celom przetwarzającego.

Administrator przetwarzający dane osobowe w oparciu o profilowanie ma obowiązek dopełnić kilku szczególnych obowiązków:

1) Informowania o decydowaniu automatycznym i w oparciu o profilowanie
2) Informowania o prawie do sprzeciwu;
3) Prawa sprzeciwu;
4) Prawa do ludzkiej interwencji;
5) Konieczności przeprowadzenia oceny skutków.

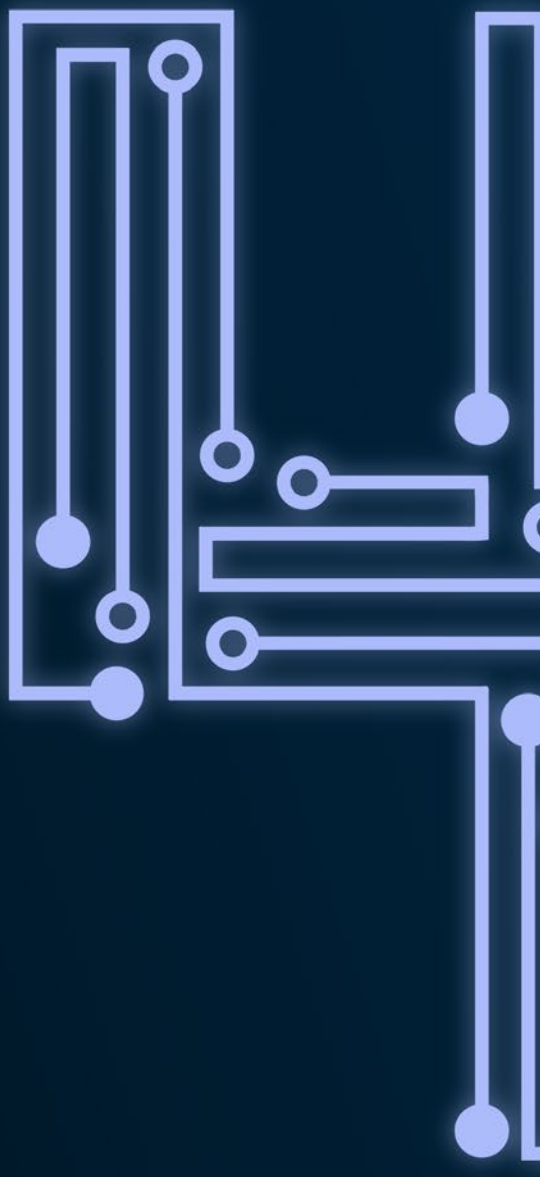
Profilowanie jest dozwolone wyłącznie w dwóch przypadkach:

1) Przepis prawa na to zezwala
2) Osoba, której dane dotyczą, udzieliła wyraźnej zgody.

Na administratorze ciąży szczególny obowiązek zapewnienia odpowiednich środków bezpieczeństwa przetwarzania danych osobowych z wykorzystaniem profilowania. Osoba, której dane są przetwarzane przy użyciu profilowania, powinna zostać niezwłocznie powiadomiona o tym fakcie oraz wiążących się z nim prawach jej przysługujących oraz konsekwencjach.

Rozdział

Obowiązki administratora danych osobowych



KIPR

OBOWIĄZKI ADMINISTRATORA DANYCH OSOBOWYCH

Za administratora uważa się osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innym ustala cele i sposoby przetwarzania danych osobowych.

Oznacza to, że tak naprawdę każdy, kto korzysta z danych osobowych do własnych celów, jest administratorem danych osobowych.

O tym, czy dany podmiot jest administratorem danych osobowych przesądzają łącznie następujące warunki:

1) Przetwarza on dane osobowe samodzielnie lub z wspólnie innymi podmiotami;
2) Ustala cele i sposoby przetwarzania danych osobowych
3) Przetwarza dane osobowe w związku z działalnością zawodową lub handlową, tj. w ramach działalności czysto osobistej lub domowej, chyba że udostępnia środki przetwarzania danych osobowych na potrzeby takiej działalności osobistej lub domowej.

Przykłady: przyjmuje się, że administratorem danych osobowych mogą być:

a) *Osoby fizyczne prowadzące jednoosobową działalność gospodarczą,*
b) *Spółki kapitałowe,*
c) *Fundacje,*
d) *Stowarzyszenia,*
e) *Partie polityczne,*
f) *Związki zawodowe,*
g) *Organy publiczne,*
h) *Jednostki organizacyjne nie posiadające osobowości prawnej.*

> ***Przykład:*** *Stowarzyszenie prowadzące pośród młodzieży licealnej działalność edukacyjną z zakresu ekonomii, podczas realizowania swoich celów statutowych przetwarza dane osobowe, m.in. swoich pracowników oraz uczestników projektu. W przypadku stowarzyszenia administratorem danych osobowych będzie stowarzyszenie. Administrator będzie reprezentowany przez organ zarządzający stowarzyszeniem, czyli w tym przypadku przez zarząd.*

Na administratorze ciąży pełna odpowiedzialność za prawidłowość przetwarzania danych zarówno w swoim imieniu, jak również w części powierzonej podmiotowi przetwarzającemu. Ponadto unijne rozporządze-

nie nakłada na niego szereg obowiązków zawartych bezpośrednio w przepisach RODO. Odpowiada on również za dobór i wdrożenie środków organizacyjnych oraz bezpieczeństwa w odniesieniu do przetwarzania danych osobowych.

> ***Przykład:*** *Fundacja jako administrator będzie odpowiedzialna za prawidłowe przestrzeganie przepisów ochrony danych osobowych oraz zapewnienie bezpieczeństwa danych osobowych. To na administratorze będzie ciążył obowiązek wprowadzenie m.in. polityki ochrony danych, zawarcia umów powierzenia z podmiotami przetwarzającymi dane w imieniu administratora, prowadzenie i aktualizowanie rejestru czynności przetwarzania danych, wywiązywanie się z obowiązku informacyjnego oraz, o ile jest wymagane, powołanie inspektora ochrony danych. Wszystkich tych czynności będzie dokonywał zarząd fundacji reprezentujący administratora.*

OBOWIĄZKI CIĄŻĄCE NA ADMINISTRATORZE DANYCH OSOBOWYCH

Przepisy unijne nakładają na administratora danych szereg obowiązków, z których realizacji jest on rozliczany. Oznacza to, że w przypadku, gdy dojdzie do naruszenia bezpieczeństwa danych osobowych w danej organizacji a administrator nie przedsięwziął odpowiednich środków bezpieczeństwa albo naruszył któryś z przewidzianych obowiązków, może to skutkować wszczęciem postępowania przed organem kontrolnym i nałożeniem kary.

Do najważniejszych obowiązków administratora należą:

1) Zapewnienie prawidłowego przetwarzania danych osobowych zgodnie z obowiązującymi zasadami;
2) Zapewnienie prawidłowej podstawy prawnej przetwarzania danych osobowych;
3) Zapewnienie prawa do informacji podmiotom, których dane są przetwarzane;
4) Zapewnienie prawa dostępu do danych, w tym dostarczenia kopii danych;
5) Zapewnienie prawa do sprostowania danych;
6) Zapewnienie prawa do usunięcia danych i bycia zapomnianym;
7) Zapewnienie prawa do ograniczenia przetwarzania danych osobowych;
8) Zapewnienie prawa do sprzeciwu;
9) Zapewnienie prawa do cofnięcia zgody na przetwarzanie danych;
10) Wdrożenie odpowiednich procedur bezpieczeństwa;
11) Zawieranie umów w zakresie powierzenia przetwarzania danych osobowych z podmiotami przetwarzającymi;
12) Prowadzenie rejestru czynności przetwarzania danych osobowych;
13) Współpraca z organem nadzorczym;
14) Zgłaszanie wszelkich naruszeń ochrony danych osobowych do organu nadzorczego lub inspektora ochrony danych, o ile jest powołany w organizacji;

15) Przeprowadzenie sformalizowanej oceny skutków dla ochrony danych, gdy zachodzi duże prawdopodobieństwo wysokiego ryzyka naruszenia praw i wolności osób, których dane są przetwarzane;
16) Przeprowadzenie analizy ryzyka
17) Powołanie Inspektora Danych Osobowych, jeżeli przepisy przewidują taką konieczność.

Zakres powyższych obowiązków powinien być proporcjonalny do wielkości danego podmiotu, zakresu, kontekstu i celu przetwarzania oraz ryzyka naruszenia praw lub wolności osób fizycznych. Oznacza to, że dwie organizacje, przetwarzająca dane osobowe 10 osób i przetwarzająca dane osobowe 10 000 osób, pomimo, że ciążą na nich takie same obowiązki będą one je realizowały przy zastosowaniu innych środków bezpieczeństwa dostosowanych do stopnia ryzyka.

PODMIOT PRZETWARZAJĄCY

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

Zadaniem podmiotu przetwarzającego jest przetwarzanie danych osobowych zgodnie z przepisami, na rzecz i w imieniu administratora.

> ***Przykład:*** *Podmiotem przetwarzającym dane osobowe w organizacji będzie księgowa, ponieważ będzie miała ona dostęp do wszystkich danych osobowych pracowników. Podmiotem przetwarzającym dane osobowe będą również podmioty świadczące na jej rzecz usługi drukarskie, dostawcy usług hostingu, firmy marketingowe, reklamowe.*

Przyjmuje się, że administrator powinien korzystać z usług wyłącznie takich podmiotów przetwarzających, którzy zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych oraz zweryfikować, czy przetwarzanie danych przez procesora będzie spełniało wymogi stawiane przez przepisy prawa, jak również chroniło prawa osób, których dane podlegają przetwarzaniu.

Zakres obowiązków ciążący na podmiocie przetwarzającym będzie wynikał z umowy powierzenia przetwarzania danych łączącej go z administratorem lub wprost z przepisów.

Obligatoryjne elementy umowy powierzenia przetwarzania danych podmiotowi przetwarzającemu wynikające z RODO obejmują m.in:

1) przedmiot i czas trwania przetwarzania,
2) charakter i cel przetwarzania,
3) rodzaj przetwarzanych danych osobowych,
4) kategorie osób, których dane dotyczą,

5) przetwarzania danych osobowych wyłącznie na udokumentowane polecenia administratora,
6) zapewnianie, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy,
7) zapewnianie odpowiedniego stopnia bezpieczeństwa przetwarzania danych osobowych poprzez wdrożenie odpowiednich środków technicznych i organizacyjnych,
8) przestrzeganie warunków korzystania z usług innego podmiotu przetwarzającego,
9) pomoc administratorowi w wywiązywaniu się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw jednostek oraz w zakresie bezpieczeństwa danych,
10) zobowiązanie do usunięcia danych osobowych po zakończeniu umowy,
11) udostępnianie administratorowi wszelkie informacji niezbędnych do wykazania spełnienia obowiązków określonych powyżej,
12) umożliwienie administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzania audytów, w tym inspekcji, i przyczynianie się do nich
13) zgłaszanie wszelkich naruszeń ochrony powierzonych danych osobowych do administratora.

Dodatkowo umowa powierzenia przetwarzania danych z podmiotem przetwarzającym może zawierać następujące elementy:

a) Szczegółowy opis gwarancji zapewnienia bezpieczeństwa przetwarzania danych przez podmiot przetwarzający;
b) Zobowiązanie do zachowania poufności;
c) Zobowiązanie do ograniczenia podpowierzania danych osobowych;
d) Zapewnianie przez procesora pełnej realizacji praw jednostki osób, których dane są przetwarzane, w imieniu administratora;
e) Uregulowanie szczegółowych procedur w razie ryzyka naruszenie praw lub wolności osób fizycznych
f) Udział w ocenie skutków dla ochrony danych.

PRAWA JEDNOSTKI, KTÓREJ DANE OSOBOWE SĄ PRZETWARZANE

PRAWO DO INFORMACJI I OBOWIĄZEK INFORMACYJNY

Jednym z podstawowych praw wynikających z rozporządzenia unijnego przyznanym osobie, której dane są przetwarzane jest prawo do informacji. Prawu temu odpowiadają konkretne obowiązki informacyjne leżące postronnie administratora danych.

Przyjmuje się, że administrator ma obowiązek informować osobę o przetwarzaniu jej danych w czterech podstawowych sytuacjach:

1) Zbierając dane bezpośrednio od tej osoby;
2) Zbierając dane o osobie z innych źródeł niż ta osoba;
3) Zmieniając cel przetwarzania danych osobowych lub dodając nowy
4) W wykonaniu żądania dostępu do danych.

Administrator planując przetwarzać dane osobowe, powinien wręczyć lub wysłać klauzulę informacyjną do osoby, której dane mają być przetwarzane, informującą o **celu przetwarzania danych osobowych** oraz **przekazać jej następujące informacje:**

a) Dane organizacji wraz z danymi kontaktowymi i danymi o przedstawicielu organizacji;
b) Dane kontaktowe inspektora ochrony danych *(jeżeli został powołany)*;
c) Podstawę prawną przetwarzania dla każdego celu;
d) Informacje o odbiorcach danych osobowych oraz kategorii odbiorców;
e) Informacje o zamiarze przekazania danych osobowych do państwa trzeciego;
f) Okresie przechowywania danych osobowych;
g) Informacje o podstawowych prawach przysługujących osobie, której dane dotyczą *(m.in. prawo do żądania informacji, prawo do usunięcia danych, prawo do sprzeciwu, prawo do skargi do organu nadzorczego, etc.)*;
h) Informacje o tym, czy podanie danych 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 tych danych.
i) Informacje o tym, czy występuje zautomatyzowane podejmowanie decyzji, w tym profilowanie.

Istotne jest to, że forma przekazania danych osobowych powinna być: **zwięzła, przejrzysta, zrozumiała, łatwo dostępna oraz opisana jasnym i prostym językiem**.

WAŻNE: obowiązek informacyjny stanowi jeden z najważniejszych obowiązków ciążących na organizacji, która przetwarza dane osobowe. Obowiązek ten najczęściej jest realizowany poprzez zamieszczenie klauzuli informacyjnej na odwrocie strony ze zgodą, lub w miejscu łatwo dostępnym dla osoby, której dane będą przetwarzane *(np. na stronie internetowej)*.

Dlatego też kluczowym dla prawidłowego funkcjonowania każdej organizacji jest przygotowanie klauzuli informacyjnej, która to zostanie zamieszczona m.in.: pod formularzem kontaktu umieszczonym na stronie internetowej, w miejscu zapisu do newslettera, na papierowym formularzu zapisu do uczestnictwa w organizowanym przez fundację wydarzeniu *(zał. 2* – wzór klauzuli informacyjnej.)

PRAWO DOSTĘPU DO DANYCH

Administrator danych ma obowiązek potwierdzić osobie, czy przetwarza dane osobowe jej dotyczące, a jeśli ma to miejsce, przekazuje tej osobie informacje zawarte w klauzuli informacyjnej, o której mowa wyżej. Dodatkowo, na żądanie osoby, administrator jest zobowiązany wydać kopię danych. Powinien spełnić powyższe żądania niezwłocznie, nie później jednak niż w ciągu miesiąca od dnia złożenia wniosku przez osobę zainteresowaną.

WAŻNE: Można więc przyjąć, że niniejszy obowiązek jest powiązany z prawem do informacji, dlatego też znacznym ułatwieniem będzie przygotowanie przez organizację klauzuli informacyjnej, która to będzie realizowała obowiązek zarówno prawa do informacji, jaki i obowiązek prawa dostępu do danych. Ponadto istotne jest, aby prowadziła ona aktualizowane bazy danych osób, których dane przetwarza.

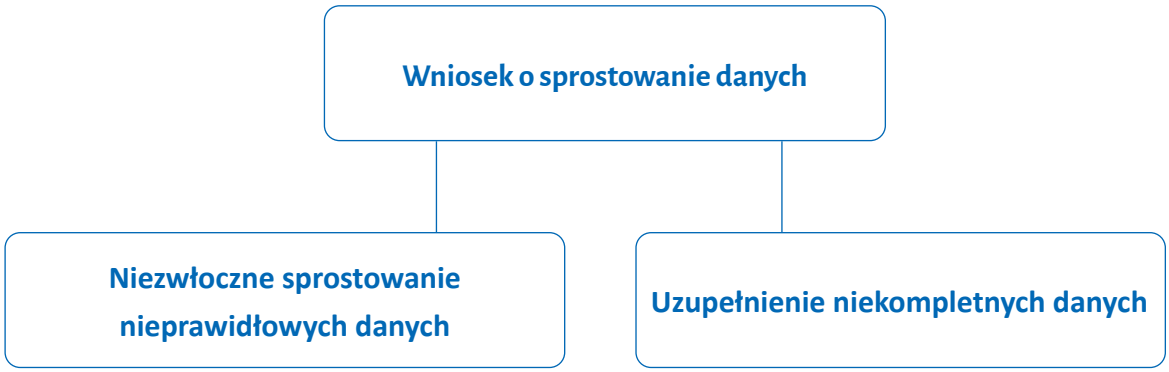
> ***Przykład:*** *Pan Paweł otrzymuje co kwartał informacje marketingowe od organizacji. Fakt ten zaniepokoił go, ponieważ nie przypomina sobie, czy udzielił zgody na przetwarzanie swoich danych osobowych. W związku z tym skorzystał z przysługującego mu prawa dostępu do danych i zażądał informacji, na jakiej podstawie organizacja posiada jego dane oraz co to są za dane. W związku z faktem, że ta prowadzi i aktualizuje na bieżąco swoje bazy danych jest w stanie udzielić niezwłocznie odpowiedzi na żądanie pana Pawła.*

Administrator dostarcza osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu. Za wszelkie kolejne kopie, o które zwróci się osoba, której dane dotyczą, administrator może pobrać opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych.

> ***Przykład:*** *Pan Paweł co tydzień występuje z żądaniem obejmującym prawo dostępu do danych osobowych. W związku z faktem, że nadużywa tego prawa, organizacja ma prawo pobrać rozsądną opłatę albo odmówić podjęcia działań w związku z żądaniem.*

PRAWO DO SPROSTOWANIA DANYCH

Osoba fizyczna ma prawo żądania od administratora niezwłocznego sprostowania jej danych osobowych, które są nieprawidłowe. Ponadto, z uwzględnieniem celów przetwarzania, osoba fizyczna ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym również poprzez przedstawienie dodatkowego oświadczenia.



Przykład: *Organizacja w ramach swojej działalności przeprowadziła konkurs wiedzy ekonomicznej, zamieszczając na stornie internetowej zdjęcie z gali wręczenia nagród wraz ze zdjęciami laureatów. Konkurs wygrał Maciek. Natomiast pod swoim zdjęciem był podpisany jako Karol, w związku z powyższym skorzystał ze swojego prawa do sprostowania danych i wystąpił do organizacji o sprostowanie nieprawidłowych danych na stronie.*

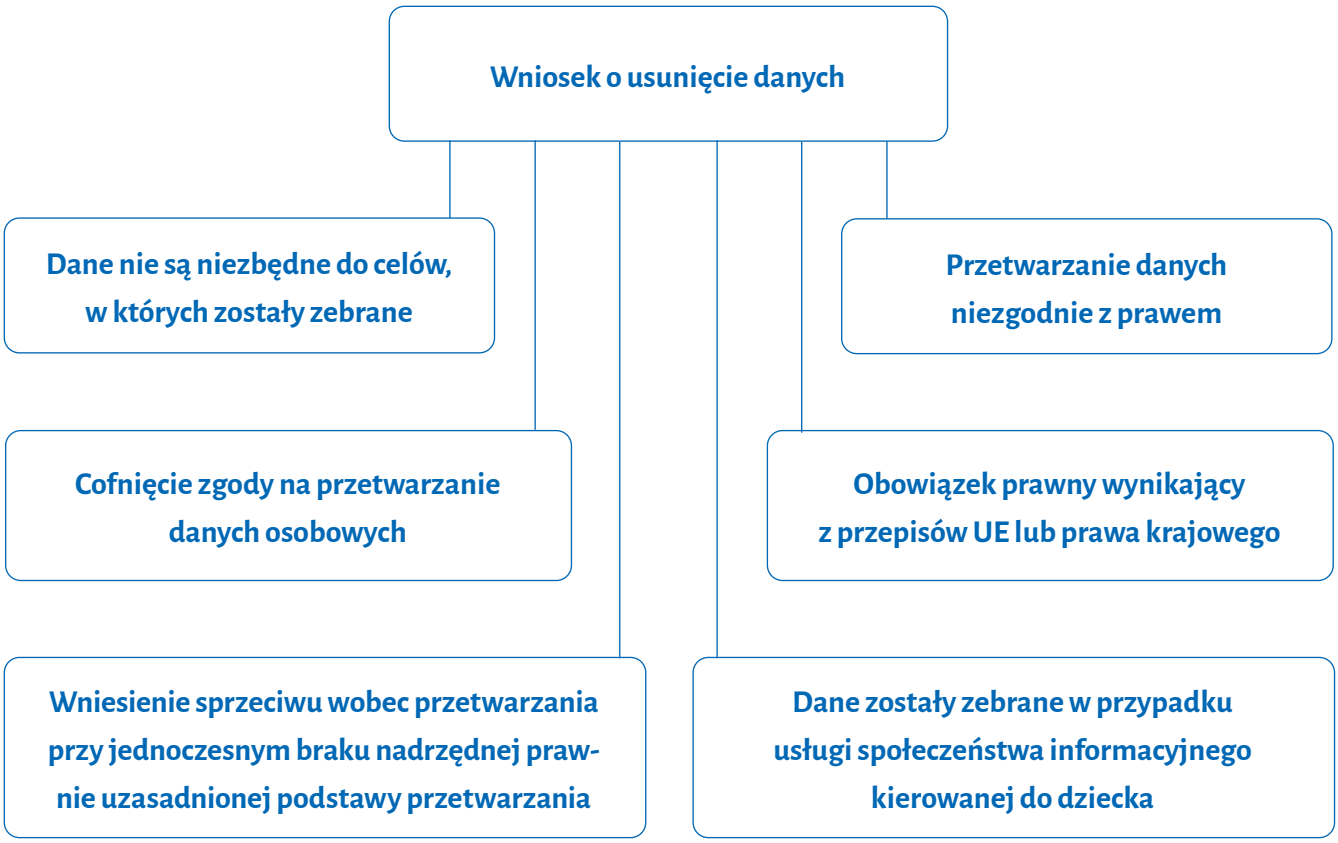
PRAWO DO BYCIA ZAPOMNIANYM

Osoba fizyczna ma prawo żądania usunięcia swoich danych osobowych, jeżeli zostały zebrane z naruszeniem ustawy albo są zbędne do realizacji celu, dla którego zostały zebrane.

Jeżeli osoba fizyczna domaga się usunięcia swoich danych osobowych, administrator ma obowiązek:

a) Usunąć dane;
b) Jeżeli przekazał dane odbiorcom, ma obowiązek poinformować o ich usunięciu
c) Jeżeli upublicznił dane podlegające usunięciu, ma obowiązek domagać się od innych administratorów, którzy przetwarzają te dane, żeby zostały one usunięte.

Osoba, której dotyczą dane, może skorzystać z prawa do bycia zapomnianym (usunięcia danych) w następujących przypadkach:



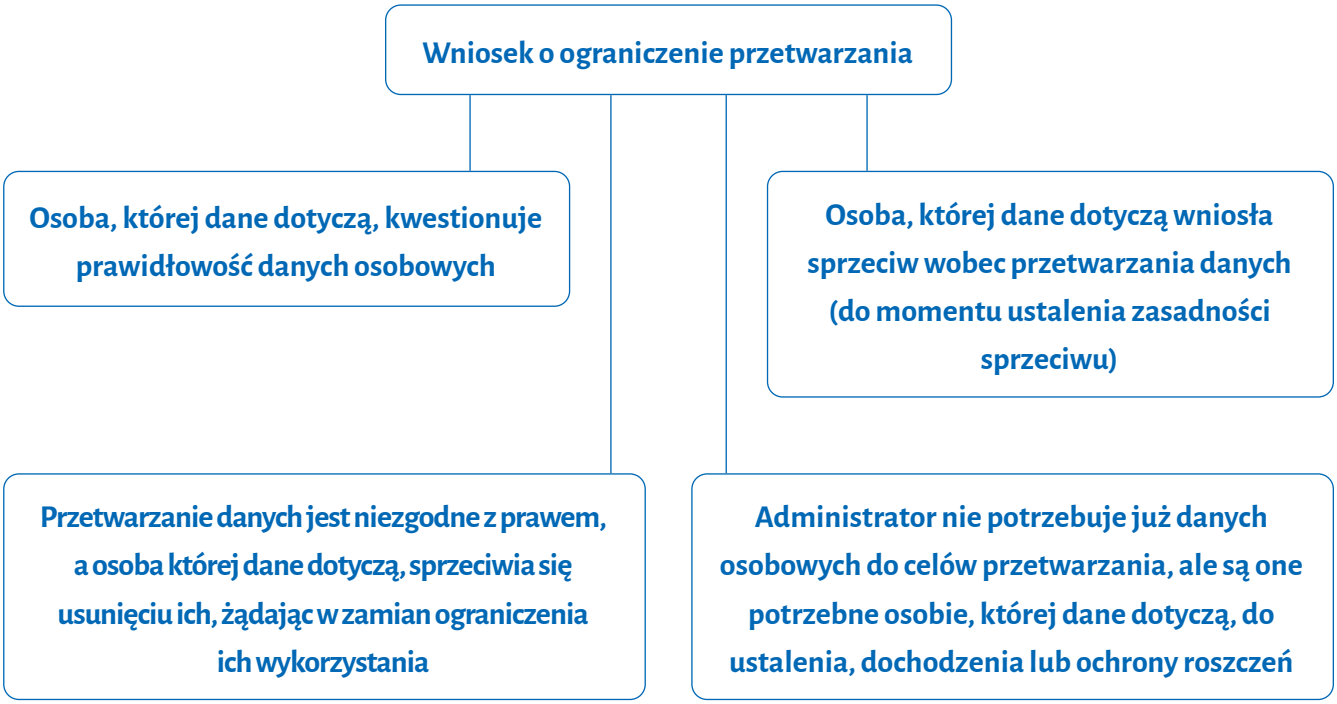
Od ogólnej zasady prawa do bycia zapomnianym przysługują pewne wyjątki. Pomimo spełnienia wyżej wskazanych przesłanek, dana osoba nie może domagać się usunięcia swoich danych osobowych w następujących przepadkach, jeżeli przetwarzanie jest niezbędne:

1) Do korzystania z prawa do wolności wypowiedzi i informacji;
2) 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;
3) Z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego;
4) Do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych
5) Do ustalenie dochodzenia i obrony roszczeń.

Wystąpienie jakiejkolwiek z wyżej wskazanych przesłanek sprawia, że administrator nie ma obowiązku usunięcia przetwarzania danych, nawet jeżeli żąda tego osoba, której dane dotyczą.

PRAWO DO OGRANICZENIA PRZETWARZANIA DANYCH OSOBOWYCH

Osoba, której dotyczą dane, może skorzystać z prawa do ograniczenia przetwarzania danych osobowych w następujących wypadkach:



Przyjmuje się, że wskutek ograniczenia przetwarzania danych osobowych administrator może przechowywać dane oraz wykonywać tylko te operacje:

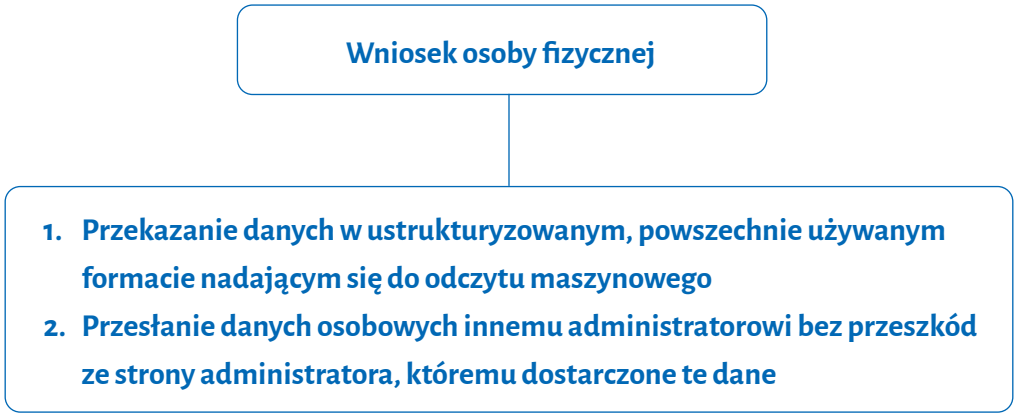
a) Na które zgadza się podmiot danych;
b) W celu ustalenia, dochodzenia lub obrony roszczeń;
c) W celu ochrony praw innej osoby fizycznej lub prawnej
d) Gdy zachodzi ważny interes publiczny Unii lub państwa członkowskiego.

Należy również pamiętać, że w razie skorzystania z prawa do ograniczenia przetwarzania danych, administrator ma obowiązek poinformować o spełnieniu żądania nie później niż w terminie miesiąca od otrzymania żądania.

Przed uchyleniem ograniczenia przetwarzania administrator jest zobowiązany poinformować osobę, której dane dotyczą, która żądała takiego ograniczenia.

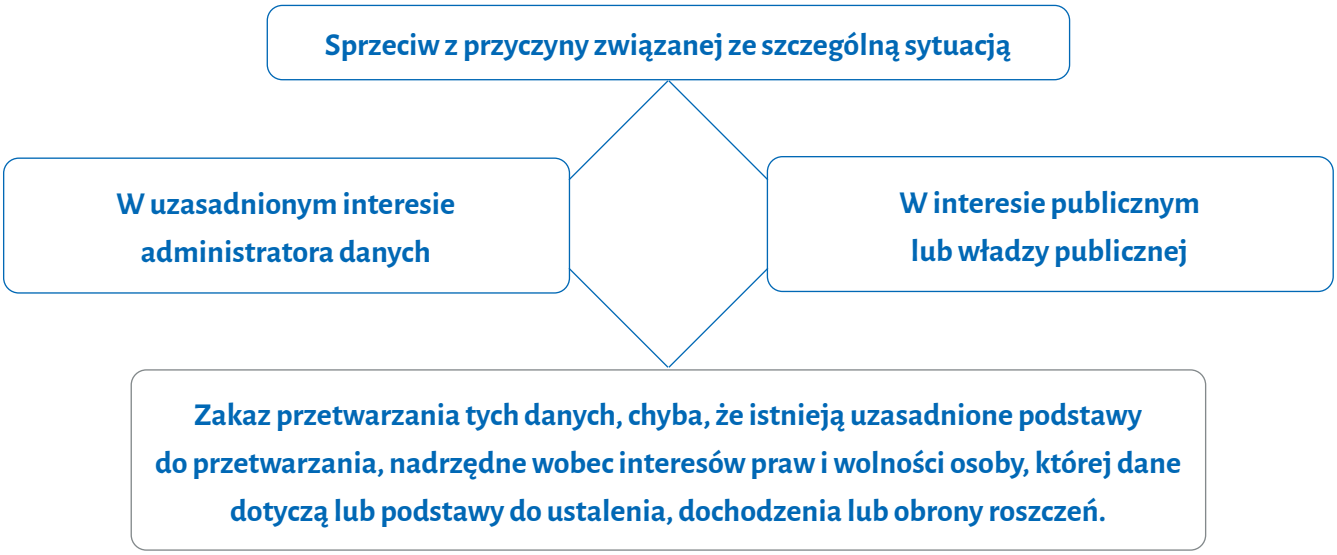
PRAWO DO PRZENOSZENIA DANYCH

Prawo to polega na przeniesieniu danych od jednego administratora do drugiego (*pomiędzy administratorami*), na wniosek złożony przez osobę fizyczną do administratora.



PRAWO DO SPRZECIWU

Każda osoba, której dane osobowe podlegają przetwarzaniu może wnieść do administratora sprzeciw. Skutecznie wniesiony sprzeciw względem przetwarzania danych osobowych powinien powodować zaprzestanie przetwarzania danych osobowych objętych zgłoszonym sprzeciwem.



FORMA SPRZECIWU

Przyjmuje się, że osoba, która chce złożyć sprzeciw, może dokonać tego w dowolnej formie. Wskazane jest jednak udokumentowanie wniesienia sprzeciwu w formie pisemnej lub za pomocą e-maila, SMS-a czy też odpowiedniego formularza zgłoszeniowego albo nagranej rozmowy telefonicznej.

UWAGA:

W klauzuli informacyjnej organizacja powinna poinformować osobę, której dotyczą dane, o prawie wniesienia sprzeciwu.

Rozdział 5

Ocena skutków dla ochrony danych

KIPR

OCENA SKUTKÓW DLA OCHRONY DANYCH

OCENA SKUTKÓW DLA OCHRONY DANYCH

Unijne rozporządzenie nakłada na administratora szereg obowiązków wdrożenia odpowiednich środków ochrony danych osobowych. To na administratorze podczas trwania kontroli lub zgłoszenia naruszenia danych będzie ciążył obowiązek wykazania wdrożenia odpowiednich środków bezpieczeństwa chroniących organizację przed naruszeniem bezpieczeństwa przetwarzanych danych osobowych.

W związku z powyższym unijny ustawodawca nałożył na administratora obowiązek przeprowadzenia oceny skutków dla danych osobowych 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.

Ocena skutków dla ochrony danych osobowych składa się z następujących elementów:

a) Opisu procesów przetwarzania danych osobowych;
b) Oceny niezbędności i proporcjonalności przetwarzania danych osobowych;
c) Dokonania oceny ryzyka wynikającego z przetwarzania danych
d) Wypracowania środków zaradczych.

Przyjmuje się, że w danej organizacji **proces oceny skutków dla ochrony danych osobowych powinien być przeprowadzony raz na 3 lata lub** częściej, jeżeli wymaga tego natura przetwarzania *(istnieje duże ryzyko wystąpienia naruszenia)* lub wpływają na to zmieniające się okoliczności.

KIEDY ADMINISTRATOR MA OBOWIĄZEK PRZEPROWADZENIA OCENY SKUTKÓW DLA OCHRONY DANYCH?

a) Ocenę skutków dla ochrony danych należy przeprowadzić w sytuacji, gdy przetwarzanie danych może prowadzić do naruszenia praw lub wolności osób fizycznych *(wysokie ryzyko występuje gdy m.in.: administrator przetwarza dane osobowe przy pomocy profilowania albo przetwarzana na dużą skalę danych szczególnych kategorii)*;

b) Przykłady operacji, w których może wystąpić wysokie ryzyko naruszenia lub wolności osób fizycznych zawiera Komunikat Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 czerwca 2019 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony. Wśród nich Komunikat wymienia m.in. *przetwarzanie szczególnych kategorii*

danych osobowych i dotyczących wyroków skazujących i czynów zabronionych przez partie polityczne, komitety wyborcze, komitety referendalne i inicjatywy ustawodawcze, organizacje społeczne, kampanie wyborcze; przetwarzanie danych przez podmioty zajmujące się zgłaszaniem nieprawidłowości związanych np. z korupcją, mobbingiem) – w szczególności gdy przetwarzane są w nim dane pracowników,

KIEDY ADMINISTRATOR NIE MUSI PRZEPROWADZIĆ OCENY SKUTKÓW DLA OCHRONY DANYCH

Ocena skutków dla ochrony danych nie jest wymagana w następujących okolicznościach:

a) gdy ryzyko naruszenia praw lub wolności osób fizycznych jest niskie;
b) gdy operacje przetwarzania zostały sprawdzone przez organ nadzorczy;
c) jeżeli zwolnienie operacji przetwarzania ma podstawę prawną w przepisach UE lub prawa krajowego;
d) jeżeli operacja przetwarzania została umieszczona w utworzonym przez organ nadzorczy wykazie operacji, które nie podlegają wymogowi przeprowadzenia oceny skutków dla ochrony danych.

RADA: Należy przyjąć za dobrą praktykę systematyczne przeprowadzanie oceny skutków dla ochrony danych bez względu na fakt czy jest ona obowiązkowa czy nie. Działanie takie zwiększy bezpieczeństwo ochrony danych osobowych w każdej organizacji i skutkować będzie minimalizacją wystąpienia takiego ryzyka.

PROCES PRZEPROWADZENIA OCENY SKUTKÓW DLA OCHRONY DANYCH

Proces przeprowadzenia oceny skutków dla ochrony danych osobowych powinien składać się z następujących etapów:

1. Dokonanie opisu procesów przetwarzania danych osobowych;
2. Dokonanie oceny niezbędności i proporcjonalności przetwarzania danych osobowych;
3. Wskazanie środków służących wykazaniu zgodności przetwarzania danych zgodnie z prawem;
4. Dokonanie oceny ryzyka wynikającego z przetwarzania danych;
5. Wskazanie środków mających na celu minimalizację wystąpienia ryzyka;
6. Monitorowanie procesów przetwarzania danych i systematyczne ponawianie oceny skutków dla ochrony danych.

UWAGA: Wszelkie działania powinny zostać udokumentowane, ponieważ na administratorze ciąży obowiązek rozliczenia się z prawidłowości zapewnienia bezpieczeństwa ochrony danych osobowych!

OPIS PROCESÓW PRZETWARZANIA DANYCH OSOBOWYCH

W pierwszym etapie należy zidentyfikować wszystkie operacje w danej organizacji, które angażują dane osobowe oraz określić ich zakres i cel.

Oznacza to, że administrator powinien przygotować zestawienie wszystkich operacji dokonywanych w danej organizacji na danych osobowych oraz określić następujące fakty:

a) Określić rodzaje operacji przetwarzania danych osobowych *(w tym określenie: na czym polegają, czemu służą czy jaką rolę odgrywają w nich dane osobowe)*;
b) Określić zakres i cel przetwarzania konkretnych danych osobowych;
c) Określić rodzaje przetwarzanych danych osobowych *(w tym, czy są przetwarzane dane wrażliwe)*;
d) Określić kategorie osób, których dane podlegają procesowi przetwarzania *(czy dane należą do: członków organizacji, wolontariuszy, sympatyków, pracowników, etc.)*;
e) Określić odbiorców, do których przesyłane są dane osobowe *(czy organizacja przesyła dane osobowe do np. biura rachunkowego, firmy zarządzającej chmurą, firmy informatycznej)*
f) Określić okres przetwarzania danych osobowych.

OCENA NIEZBĘDNOŚCI I PROPORCJONALNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH

W drugim etapie należy zweryfikować, czy wszystkie dane i związane z nimi procesy są niezbędne i proporcjonalne oraz czy organizacja posiada odpowiednie podstawy prawne do przetwarzania danych.

Oznacza to, że administrator powinien sprawdzić czy:

a) Potrafi wykazać cel i podstawę przetwarzania danych osobowych *(np. dane są przetwarzane w celu kontaktu z sympatykami organizacji na podstawie udzielonej przez nich zgody)*;
b) Przetwarzanie danych jest niezbędne do osiągnięcia danego celu *(np. nie przetwarza za dużo danych, które są zbędne z punktu widzenia realizacji celu)*;
c) Przetwarzane dane powinny zostać poddane anonimizacji lub pseudonimizacji;
d) Przetwarzając dane osobowe, wykonuje ciążące na nim obowiązki informacyjne
e) Przetwarzając dane osobowe, realizuje prawa jednostki *(np. prawo do bycia zapomnianym, prawo do skargi, praw od skorygowania danych)*.

OPIS ŚRODKÓW SŁUŻĄCYCH WYKAZANIU ZGODNOŚCI PRZETWARZANIA DANYCH ZGODNIE Z PRAWEM

W trzecim etapie, po zidentyfikowaniu wszystkich operacji przetwarzania danych osobowych oraz zweryfikowaniu ich legalności, należy określić, czy dana organizacja posiada określone procedury związane z realizacją ciążących na administratorze obowiązków wynikających z przepisów prawa.

Na tym etapie administrator powinien przeanalizować, czy w jego organizacji zostały wdrożone procedury związane z:

a) Realizacją obowiązku informacyjnego *(obejmuje to zarówno stworzenie klauzuli informacyjnej jak również określenie procedur związanych z prawem do informacji oraz obowiązkiem informacyjnym);*
b) Realizacją prawa dostępu do danych osobowych;
c) Realizacją prawa do sprostowania danych, ich usunięcia oraz ograniczenia przetwarzania;
d) Realizacją praw do przenoszenia danych;
e) Realizacją prawa do sprzeciwu i wycofania zgody na przetwarzanie;
f) Realizacją obowiązków związanych z powierzaniem danych osobowych podmiotom przetwarzającym *(m.in. określenie zasad powierzania przetwarzania danych osobowych, podpisaniu umów powierzenia przetwarzania danych);*
g) Realizacją obowiązku powołania Inspektora ochrony danych *(jeżeli jest wymagany)*
h) Realizacją obowiązku przeprowadzenia uprzednich konsultacji z organem nadzorczym *(jeżeli jest to konieczne).*

OCENA RYZYKA WYNIKAJĄCEGO Z PRZETWARZANIA DANYCH

W czwartym etapie należy zidentyfikować wszystkie możliwe ryzyka związane z przetwarzaniem danych osobowych oraz określić jakie mogą wywołać skutki.

Administrator powinien określić:

a) Jakie zagrożenia mogą wystąpić w związku z przetwarzaniem danych;
b) Jakie i kogo dane osobowe są zagrożone;
c) Z czego te zagrożenia mogą wynikać;
d) Czy istnieje szansa ich wystąpienia, a jeżeli tak, to jak duża ona jest
e) Jakie konsekwencje może wywołać ewentualna realizacja zagrożenia.

Głównym celem przeprowadzenia oceny ryzyka jest pomoc administratorowi w określeniu możliwych zagrożeń dla praw i wolności osób, których dane są przetwarzane oraz odpowiedzi na pytanie, jakie należy wdrożyć środki zaradcze, aby zminimalizować możliwość wystąpienia określonego ryzyka. Oznacza to, konieczność zidentyfikowania rodzajów, źródeł oraz poziomu ryzyka możliwych do wystąpienia zagrożeń.

PROCES PRZEPROWADZENIA OCENY RYZYKA

Pierwszym etapem przeprowadzenia oceny ryzyka jest zidentyfikowanie zagrożeń, jakie mogą wystąpić w związku z przetwarzaniem danych. Na administratorze ciąży obowiązek określenia zagrożeń.

Mogą być to m.in.:

a) osoby trzecie wchodzą w posiadanie danych osobowych;
b) dochodzi do ataku hackerskiego i upublicznienia danych osobowych;
c) dochodzi do utraty danych osobowych
d) dochodzi do niezamierzonej ingerencji do baz danych osobowych i ulegają one pomieszaniu.

> ***Przykład:*** *Fundacja posiada bazę danych kontaktowych do swoich sympatyków w pliku arkusza kalkulacyjnego, który jest umieszczony na dysku wirtualnym. Administratorowi udało się zidentyfikować następujące zagrożenia względem przetwarzanych w tym pliku danych osobowych. Przed wszystkim organizacja może bezpowrotnie utracić dostęp do tych danych, ponieważ nie posiada kopii zapasowych, ponadto w związku z faktem, iż są one przechowywane na dysku wirtualnym, istnieje zagrożenie, że może dojść do ataku hackerskiego, czego bezpośrednim skutkiem może być wyciek zawartych w nim danych.*

W drugim etapie należy ustalić jakie i kogo dane osobowe mogą być zagrożone w wyniku ich naruszenia. W tym momencie administrator musi ustalić, czy zagrożone są dane zwykłe czy dane szczególnej kategorii oraz przede wszystkim jakie i kogo dane są zagrożone.

> ***Przykład:*** *Fundacja posiada bazę danych kontaktowych do swoich sympatyków w pliku arkusza kalkulacyjnego, który jest umieszczony na dysku wirtualnym. Oznacza to, że zagrożone są dane osobowe sympatyków fundacji a w szczególności dane dotyczące ich: imion, nazwisk oraz adresów.*

W trzecim etapie dzięki ustaleniu potencjalnych zagrożeń, administrator będzie miał za zadanie ustalić w jaki sposób może dojść do zagrożenia bezpieczeństwa danych osobowych.

W tym celu administrator musi określić co oraz kto może doprowadzić do zagrożenia bezpieczeństwa danych.

> ***Przykład:*** *Administrator zidentyfikował możliwe w wystąpieniu zagrożenie w przedmiocie pliku arkusza kalkulacyjnego zawierającego dane osobowe sympatyków fundacji umieszczonego na dysku wirtualnym. Udało się określić krąg osób, jakie posiadają dostęp do tego pliku (członkowie fundacji upoważnieni imiennie przez Prezesa Fundacji). W związku z powyższym można przypuszczać, że do ewentualnego zagrożenia może dojść poprzez:*
>
> 1. *błąd pracownika – może on umyślnie bądź nieumyślnie udzielić dostępu do pliku osobie trzeciej albo usunąć lub zmodyfikować dane zawarte w pliku;*
> 2. *awarii systemu – wskutek awarii systemu dysku wirtualnego, organizacja może utracić dane zawarte w pliku*

3. *zagrożenia zewnętrznego – w wyniku ataku hackerskiego mogą zostać wykradzione dane zawarte w pliku.*

W czwartym etapie administrator powinien określić, jakie jest prawdopodobieństwo, że zagrożenie się zrealizuje. Na tym etapie administrator musi określić, czy wśród możliwych zagrożeń istnieją bardziej prawdopodobne lub takie, które w razie zrealizowania się pociągną za sobą szczególnie dotkliwe konsekwencje.

Na tym etapie administrator musi odpowiedzieć sobie na następujące pytania:

a) Jak bardzo w razie wystąpienia zagrożenia dane osobowe są narażone na niebezpieczeństwo?
b) Jak dotkliwe w skutkach może być urzeczywistnienie się zagrożenia?
c) W jakim stopniu są zagrożone dane procesy przetwarzania danych osobowych?

Przykład: *Administrator zidentyfikował możliwe w wystąpieniu zagrożenie w przedmiocie pliku arkusza kalkulacyjnego zawierającego dane osobowe sympatyków fundacji umieszczonego na dysku wirtualnym. Jako potencjalne zagrożenia wskazane zostały:*

1. *błąd pracownika skutkujący udostępnieniem danych osobie trzeciej – zagrożenie to jest minimalne ze względu na fakt, że pracownicy nie mają możliwości udostępniania danych osobowych.*
2. *ataku hackerskiego – zagrożenie to jest minimalne ze względu na fakt stosowania przez fundację nowoczesnego oprogramowania antywirusowego.*

WAŻNE: Podczas badania stopnia prawdopodobieństwa wystąpienia zagrożenia, w razie ustalenia, że występuje wysokie ryzyko, na administratorze ciąży obowiązek przeprowadzenia konsultacji na ten temat z organem nadzorczym!

Analogiczna sytuacja ma miejsce, gdy ocena skutków dla ochrony danych wykaże, że przetwarzanie spowoduje wysokie ryzyko, jeśli administrator nie zastosuje środków w celu zminimalizowania tego ryzyka, to przed rozpoczęciem przetwarzania powinien skonsultować się z organem nadzorczym.

Podczas uprzednich konsultacji z Urzędem Ochrony Danych Osobowych należy wskazać:

a) Cele i sposoby zamierzonego przetwarzania;
b) Środki i zabezpieczenia mające chronić prawa i wolności osób, których dane dotyczą;
c) Ocenę skutków dla ochrony danych
d) Dane kontaktowe do Inspektora ochrony danych (jeżeli został wyznaczony).

W piątym etapie należy wskazać, jakie mogą wystąpić skutki zaistniałego zagrożenia oraz jakie osoby będą nim dotknięte. W tym celu administrator powinien ustalić, jakie skutki wystąpią w razie wystąpienia danego zagrożenia oraz kto i w jaki sposób na tym ucierpi.

> ***Przykład:*** *W fundacji doszło do ataku hackerskiego na systemy informatyczne. W związku z nim osoby trzecie weszły w posiadanie danych osobowych jej sympatyków (imiona i nazwiska oraz adresy mailowe). Oznacza to, że skutkiem realizacji zagrożenia w postaci ataku hackerskiego było wejście w posiadanie danych osobowych sympatyków przez osoby nieuprawnione, które teraz mogą np. nękać spamem sympatyków fundacji.*

PRZYKŁADOWY ŁAŃCUCH PROCESU ANALIZY RYZYKA

(na przykładzie pliku kalkulacyjnego zawierającego dane kontaktowe sympatyków fundacji zamieszczonego na dysku wirtualnym – zagrożenie atak hackerski)

IDENTYFIKACJA ZAGROŻENIA
Możliwość ataku hackerskiego, czego bezpośrednim skutkiem będzie kradzież danych

↓

JAKIE I KOGO DANE SĄ ZAGROŻONE
Dane osobowe sympatyków fundacji a w szczególności dane dotyczące ich: imion, nazwisk oraz adresów

↓

SPOSÓB DOPROWADZENIA DO POWSTANIA ZAGROŻENIA
Zagrożenie zewnętrzne – atak hackerski, w wyniku którego zostaną wykradzione dane osobowe

↓

PRAWDOPODOBIEŃSTWO ZAISTNIENIA NEGATYWNYCH SKUTKÓW RYZYKOWNEJ SYTUACJI
Zagrożenie to jest minimalne ze względu na fakt stosowania przez fundację nowoczesnego oprogramowania antywirusowego

↓

KONSEKWENCJE W RAZIE URZECZYWISTNIENIA ZAGROŻENIA
Skutkiem realizacji zagrożenia w postaci ataku hackerskiego było wejście w posiadanie danych osobowych sympatyków przez osoby nieuprawnione, które teraz mogą np. nękać spamem sympatyków Fundacji

OKREŚLENIE ŚRODKÓW MAJĄCYCH NA CELU MINIMALIZACJĘ WYSTĄPIENIA RYZYKA

Po zidentyfikowaniu możliwych zagrożeń oraz stopnia ich wystąpienia, należy określić i wdrożyć odpowiednie środki zabezpieczające mające na celu ograniczyć a nawet wyeliminować całkowicie ryzyko naruszenia bezpieczeństwa danych osobowych.

Jako środki techniczne mające na celu minimalizację lub eliminację zagrożeń naruszenia można przyjąć:

a) Zakup nowoczesnego oprogramowania antywirusowego;
b) Zakup nowoczesnych systemów zarządzania danymi;
c) Zakup nowoczesnego sprzętu odpowiednio przystosowanego poprzez wyposażenie go w oprogramowanie szyfrujące dyski, procedury archiwizacji plików, bieżące wsparcie producenta w postaci aktualizacji oprogramowania oraz wprowadzenie procedur bezpieczeństwa. *(np. dwustopniowe logowanie – wpisanie hasła oraz potwierdzenie zalogowania tokenem)*;
d) Zakup niszczarki według odpowiedniej kategorii;
e) Zainstalowanie systemu monitorowania przetwarzania danych
f) Zakup środków zwiększających poufność, integralność i odporność systemów.

Jako środki organizacyjne mające na celu minimalizację lub eliminację zagrożeń naruszenia można przyjąć:

a) Organizację szkoleń z zakresu ochrony danych osobowych;
b) Wprowadzenie określonych procedur związanych z przetwarzaniem danych
c) Wprowadzenie i egzekwowanie polityki czystego biurka, polityki czystego ekranu.

> ***Przykład:*** *Administrator przeprowadził analizę ryzyka i ustalił, że zagrożeniem występującym w jego organizacji jest możliwość wycieku danych osobowych sympatyków fundacji zamieszczonych na dysku wirtualnym. W celu zmniejszenia ryzyka wystąpienia powyższego zagrożenia zakupił profesjonalne oprogramowanie mające na celu chronić dane przed wirusami oraz atakami osób trzecich. Ponadto, wprowadził rejestr zatrudnionych u administratora osób mających dostęp do pliku zawierającego dane sympatyków oraz uzależnił wszelkie udostępnienie danych osobowych od uprzedniej, pisemnej, zgody zarządu fundacji.*

MONITOROWANIE PROCESÓW PRZETWARZANIA DANYCH I SYSTEMATYCZNE PONAWIANIE OCENY SKUTKÓW DLA OCHRONY DANYCH

Polega on na stałym monitorowaniu procesów przetwarzania danych osobowych i wyszukiwaniu nowych zagrożeń oraz uchybień w dotychczas wprowadzonym procesie. Proces ten powinien być stały ze względu na dynamikę rozwoju organizacji, przetwarzanie nowych kategorii danych osobowych oraz pojawiania się nowych zagrożeń.

Ponadto, na tym etapie powinno się stale zwiększać bezpieczeństwo przetwarzania danych osobowych poprzez wdrażanie nowych procedur, szkolenie członków oraz pracowników organizacji oraz modernizowanie systemów bezpieczeństwa.

Dobrą praktyką jest, aby osobą odpowiedzialną za tego typu działania był powołany w organizacji Inspektor ochrony danych lub też osoba, której takie zadania zostaną przekazane w ramach łączącego ją stosunku prawnego z administratorem.

REJESTR CZYNNOŚCI PRZETWARZANIA

Przed wejściem w życie unijnego rozporządzenia podmioty miały obowiązek posiadania szeregu dokumentów odnoszących się do zabezpieczenia danych osobowych w danej organizacji. Należały do nich m.in.: polityka bezpieczeństwa, instrukcje zarządzania systemem informatycznym. RODO wprowadziło zasadę rozliczności, która to obciąża administratora obowiązkiem wykazania, że sposób przetwarzania danych osobowych i wprowadzone przez niego zabezpieczenia są wystarczające.

UWAGA: Niemniej jednak dobrą praktyką pozwalającą na świadome funkcjonowanie organizacji, wraz z dostatecznym zapewnieniem bezpieczeństwa przetwarzania danych osobowych, będzie przygotowanie dla niej powyższych dokumentów !

RODO zniosło obowiązek zgłaszania zbiorów danych do rejestracji do organu nadzorczego. Natomiast zastąpiło go obowiązkiem prowadzenia przez administratora rejestru czynności przetwarzania!

W rejestrze powinny znaleźć się m.in. następujące informacje:

a) imię i nazwisko lub nazwa oraz dane kontaktowe administratora,
b) dane kontaktowe do Inspektora ochrony danych,
c) cel przetwarzania danych oraz jego podstawa,
d) opis kategorii osób, których dane są przetwarzane,
e) kategorie odbiorców, którym dane osobowe zostały ujawnione lub zostaną ujawnione;,
f) czy dane są przekazywane do państwa trzeciego,
g) okres przez jaki dane będą przetwarzane,
h) opis technicznych i organizacyjnych środków bezpieczeństwa.

Zał. 3 – wzór rejestru czynności przetwarzania

Rozdział

Inspektor Ochrony Danych Osobowych

KIPR

INSPEKTOR OCHRONY DANYCH OSOBOWYCH

Inspektor ochrony danych osobowych jest osobą, która pośredniczy pomiędzy administratorem a osobami, których dane są przetwarzane. Jest to osoba, która będzie odpowiadała za bezpieczeństwo ochrony danych osobowych w danej organizacji oraz będzie odpowiedzialna za kontakt z osobami, których dane są przetwarzane, m.in. poprzez udzielanie informacji.

Funkcję inspektora powinna piastować osoba posiadająca odpowiednią wiedzę z zakresu prawa ochrony danych osobowych, jak również doświadczenie w tym względzie. Funkcję tą może sprawować osoba zatrudniona przez administratora lub zewnętrzny podmiot.

UWAGA: Warto zaznaczyć, że IOD nie ponosi odpowiedzialności za prawidłowe wdrożenie przepisów RODO oraz zgodność działań organizacji z nimi. Jego funkcja ma bardziej charakter doradczo – kontrolny.

OBOWIĄZEK POWOŁANIA IOD

Na wstępie warto zaznaczyć, że nie każda organizacja posiada obowiązek posiadania Inspektora ochrony danych. Konieczność powołania takiej osoby powinna być poprzedzona dogłębną analizą w celu ustalenia, czy faktycznie trzeba powołać taką osobę

Każda organizacja ma obowiązek powołania IOD – w następujących sytuacjach:

a) 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;

b) Główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych albo danych osobowych dotyczących wyroków skazujących i naruszeń prawa.

WAŻNE: Chociaż przepisy nie zobowiązują każdej organizacji do powołania IOD, to przyjmuje się, że powołanie takiego podmiotu **stanowi dobrą praktykę**, pozwalającą na zwiększenie profesjonalizmu podmiotu oraz jego stopnia bezpieczeństwa ochrony danych!

ZADANIA INSPEKTORA OCHRONY DANYCH

Inspektor Ochrony Danych ma następujące zadania:

1. Realizacja obowiązku informacyjnego;
2. Monitorowanie przestrzegania przepisów prawa przez administratora oraz podmioty przetwarzające poprzez:
   a) Zbieranie informacji w celu identyfikacji procesów przetwarzania;
   b) Analizowanie i sprawdzanie zgodności tego przetwarzania
   c) Informowanie, doradzanie i rekomendowanie określonych działań administratorowi albo podmiotowi przetwarzającemu.
3. Organizacja i prowadzenie szkoleń i audytów;
4. Udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania
5. Współpraca z organem nadzorczym i pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem.

Inspektorowi Ochrony Danych można powierzyć również inne zadania! (np. prowadzenie rejestru czynności przetwarzania danych).


3 4
6 7
3 4 5
3 4
delete

Rozdział 7

Postępowanie w razie naruszenia danych osobowych

KIPR

POSTĘPOWANIE W RAZIE NARUSZENIA OCHRONY DANYCH OSOBOWYCH

W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

Naruszenie ochrony danych osobowych oznacza **naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.**

PRZYKŁADY NARUSZENIA DANYCH OSOBOWYCH:

1) Zniszczenie danych osobowych – sytuacja, w której dane przestają istnieć *(np. nieodwracalne wykasowanie plików zawierających dane osobowe z komputera, zalanie lub spalenie dokumentacji)*;
2) Zmiana danych osobowych – uszkodzenie danych osobowych prowadzące do sytuacji, w której to dane osobowe stały się niekompletne, nieczytelne lub nieprawidłowe *(np. pomieszanie numerów telefonów, wprowadzenie zmian do plików tekstowych)*;
3) Utrata danych osobowych – sytuacja, w której dane normalnie istnieją, natomiast administrator utracił nad nimi kontrolę, dostęp lub nie znajduje się już w ich posiadaniu *(np. kradzież telefonu, laptopa, zgubienie pendrive'a)*.

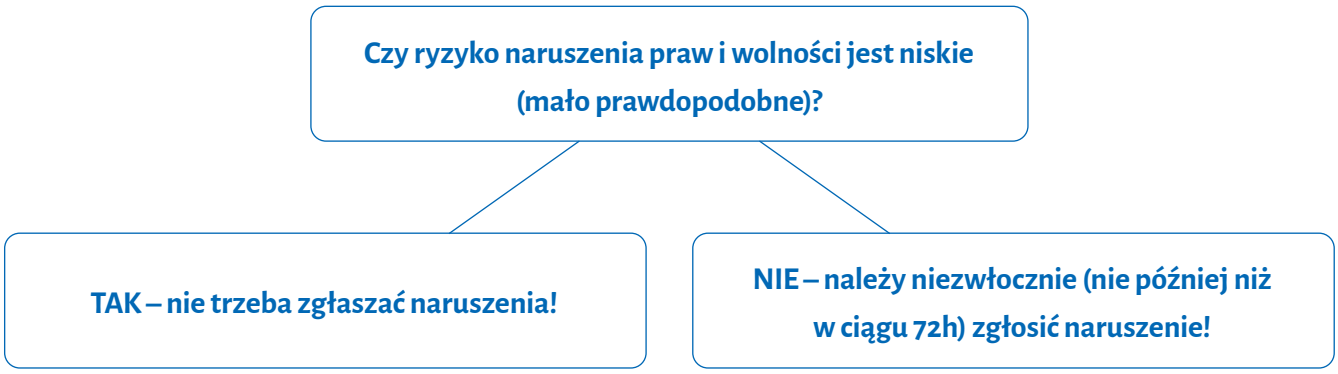
> ***Przykład:*** *Prezes fundacji na co dzień wykorzystuje tablet fundacji, który to ma dostęp do wirtualnych dysków zawierających dokumenty organizacji oraz bazy kontaktowe sympatyków. Podczas podróży pociągiem skradziono mu tablet. Ten nie był zabezpieczony, w związku z tym osoba, która go ukradła, uzyskała bezpośredni dostęp do dokumentów fundacji oraz danych osobowych jej sympatyków. Oznacza, to że doszło do sytuacji naruszenia danych osobowych i fundacja ma obowiązek zgłosić ten fakt organowi nadzorczemu.*

CZY KAŻDE NARUSZENIE TRZEBA ZGŁASZAĆ?

Istotną kwestią z punktu widzenia każdej organizacji jest odpowiedź na pytanie,czy każde naruszenie trzeba zgłaszać.

Jak już zostało wyżej wspomniane, takie sytuacje jak: zgubienie kartki zawierającej imiona, nazwiska i numery telefonów członków , czy też przypadkowe spojrzenie osoby postronnej na ekran telefonu, komputera lub ta-

bletu podczas przeglądania baz danych, stanowi naruszenie ochrony danych osobowych. W razie wystąpienia takiej sytuacji, należy odpowiedzieć sobie na bardzo ważne pytanie:



PROCEDURA ZGŁASZANIA NARUSZEŃ OCHRONY DANYCH OSOBOWYCH

Administrator ma obowiązek zgłosić naruszenie ochrony danych **bez zbędnej zwłoki, ale nie później niż w terminie 72 godzin po stwierdzeniu naruszenia.** W razie uchybienia temu terminowi, administrator musi załączyć wyjaśnienie przyczyn opóźnienia w zgłoszeniu.

Zgłoszenie przez administratora naruszenia do organu nadzorczego musi zawierać co najmniej:

a) opis charakteru naruszenia wraz z informacją o kategorii i przybliżonej liczbie osób, których dane dotyczą oraz kategorii i liczbie wpisów (*np. kradzież laptopa, na którym są imiona, nazwiska i numery telefonów 50 sympatyków organizacji, zalanie dokumentów zawierających adresy mailowe do wysyłki newslettera);*
b) dane kontaktowe do Inspektora Ochrony Danych;
c) opis możliwych konsekwencji naruszenia *(np. nieuprawnione osoby będą miały dostęp do danych osobowych sympatyków organizacji)*
d) opis zastosowanych lub proponowanych środków zaradczych *(np. wykasowanie danych z zagubionego telefonu komórkowego przy użyciu aplikacji uprzednio na nim zainstalowanej, możliwość odtworzenia bazy danych z ustawionego backupu danych).*

> ***Przykład:*** *Prezes fundacji niezwłocznie po stwierdzeniu kradzieży tabletu zgłosił naruszenie danych do organu nadzorczego. W zgłoszeniu wskazał, że kradzieży uległ tablet zawierający dane osobowe (imiona i nazwiska oraz adresy mailowe) około 100 sympatyków fundacji; podał również, jakie działania podjęła organizacja w celu minimalizacji szkód poniesionych w związku z naruszeniem oraz dane kontaktowe do Inspektora ochrony danych.*

SYSTEM ZGŁASZANIA NARUSZEŃ

Mając na względzie prawidłowe funkcjonowanie organizacji, w razie wystąpienia naruszenia ochrony danych osobowych, istotne będzie uprzednie przygotowanie systemu zgłaszania naruszeń. Dzięki wdrożeniu odpowiednich środków organizacyjnych, administrator będzie mógł zainterweniować w odpowiedni i szybki sposób.

Aby skutecznie przejść przez proces związany z naruszeniem bezpieczeństwa danych, należy posiadać:

1) procedurę postępowania w przypadku naruszenia,
2) instrukcję postępowania w razie podejrzenia naruszenia,
3) przeszkolenie personelu co do znaczenia naruszenia ochrony danych oraz sposobu postępowania w takim przypadku,
4) ustalenia z podmiotami przetwarzającymi dane jednolitych zasad postępowania w razie wystąpienia naruszenia,
5) metody dokumentowania naruszeń i podejrzeń naruszeń
6) możliwość wskazania osoby odpowiedzialnej do zgłaszania naruszenia do organu nadzorczego.

ZAWIADOMIENIE OSOBY, KTÓREJ DANE DOTYCZĄ O NARUSZENIU OCHRONY DANYCH OSOBOWYCH

Jeżeli naruszenie 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 powinno być sporządzone w jasnym i prostym języku. Przyjmuje się, że powinno ono przyjąć formę pisemną lub mailową. Zakres zawiadomienia osoby poszkodowanej powinien mieścić się w zakresie zgłoszenia do organu nadzorczego, przy czym nie musi zawierać informacji o skali wycieku i innych poszkodowanych.

W treści zawiadomienia powinny znaleźć się następujące informacje:

a) Charakter naruszenia
b) Dane kontaktowe inspektora ochrony danych
c) Możliwe konsekwencje naruszenia
d) Opis zastosowanych lub proponowanych przez administratora środków w celu zaradzenia naruszeniu, zminimalizowaniu jego ewentualnych negatywnych skutków

SANKCJE

W przypadku stwierdzenia przez organ nadzorczy naruszenia przepisów RODO, uprawniony jest on do **nałożenia administracyjnej kary pieniężnej, która to powinna być proporcjonalna do wagi naruszenia przepisów oraz odstraszająca**. Kary grożą zarówno administratorowi jak i podmiotom przetwarzającym.

Kara w wysokości 10 000 000 euro albo 2% całkowitego rocznego obrotu może być nałożona w przypadku następujących naruszeń:

1) *Niezastosowanie się do warunków wyrażenia zgody przez dziecko w przypadku usług społeczeństwa informatycznego;*
2) *Nieuwzględnienie ochrony danych w fazie projektowania oraz domyślnej ochrony danych;*
3) *Nieprzestrzeganie przepisów dotyczących rejestrowania czynności przetwarzania;*
4) *Niedopełnienie obowiązków z inspektorem ochrony danych;*
5) *Niedopełnienie obowiązków ciążących na współadministratorze;*
6) *Niedopełnienie obowiązków oraz naruszenie przepisów przez Podmiot Przetwarzający;*
7) *Nieodpowiednie zapewnienie poziomu bezpieczeństwa danych (np. niewdrożenie odpowiednich środków technicznych i organizacyjnych zapewniających odpowiedni stopień bezpieczeństwa);*
8) *Nieinformowanie podmiotu, którego dane osobowe są przetwarzane, o wysokim ryzyku naruszenia jego praw i wolności*
9) *Niepoinformowanie podmiotu, którego dane osobowe zostały naruszone, o zaistniałym incydencie.*

Kara w wysokości 20 000 000 euro albo 4% całkowitego rocznego obrotu może być nałożona w przypadku następujących naruszeń:

1) *Naruszenie podstawowych zasad przetwarzania danych osobowych;*
2) *Naruszenie warunków wyrażania zgody;*
3) *Naruszenie przepisów dotyczących przetwarzania szczególnej kategorii danych;*
4) *Niedopełnienie obowiązku informacyjnego;*
5) *Niedopełnienie obowiązków wynikających z prawa dostępu, sprostowania, przenoszenia, usunięcia i ograniczenia przetwarzania danych;*
6) *Niedopełnienie obowiązków wynikających z realizacji prawa do sprzeciwu wobec przetwarzania danych.*


Hackers
Networks

ZAŁĄCZNIKI

ZAŁ. 1 – WZÓR ZGODY NA PRZETWARZANIE DANYCH OSOBOWYCH

ZGODA NA PRZETWARZANIE DANYCH OSOBOWYCH

Wyrażam zgodę na przetwarzanie moich danych osobowych przez *[nazwa podmiotu, forma prawna, adres, KRS, NIP, REGON]*, w celu *[określenie celu przetwarzania danych osobowych]*

Podstawą przetwarzania danych jest *[wskazanie podstawy przetwarzania danych osobowych z art. 6 ust. 1 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku]*

Podstawą przetwarzania danych jest [wskazanie podstawy przetwarzania danych osobowych z art. 6 ust. 1 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku]

[data, podpis osoby wyrażającej zgodę]

ZAŁ. 2 – WZÓR UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH

[dzień, miesiąc, rok]

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie art. 29 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektyw 95/46/WE (ogólne rozporządzenie o ochronie danych), niniejszym w *[nazwa podmiotu, forma prawna, adres, KRS, NIP, REGON]*, upoważniam do przetwarzania danych osobowych:

- *[Imię i nazwisko osoby upoważnionej do przetwarzania danych osobowych]*

Upoważnienie obejmuje uprawnienie do przetwarzania danych osobowych w zakresie:

- *[zakres upoważnienie do przetwarzania danych]*

Upoważnienie jest udzielona [wskazanie na jaki okres jest udzielone upoważnienie]

[Podpis osoby uprawnionej do reprezentowania Administratora]

ZAŁ. 3 – WZÓR KLAUZULI INFORMACYJNEJ

Klauzula informacyjna *[nazwa podmiotu]*

Zgodnie z art. 13 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektyw 95/46/WE (ogólne rozporządzenie o ochronie danych) (dalej „RODO") w imieniu [nazwa podmiotu], informujemy, że

[Administrator] Administratorem Pani/Pana danych osobowych jest *[nazwa podmiotu, forma prawna, adres, KRS, NIP, REGON]*

[Administrator Bezpieczeństwa Danych Osobowych / Inspektor Ochrony Danych Osobowych] W razie konieczności może Pani/Pan skontaktować się z naszym Administratorem Bezpieczeństwa Danych Osobowych / Inspektorem Ochrony Danych Osobowych *[imię nazwisko oraz sposób kontaktu (mail lub numer telefonu)]*

[Cel i podstawy przetwarzania danych] Będziemy przetwarzać Pani/Pana dane osobowe w celach: *[wskazanie celu przetwarzania danych osobowych oraz podstawy prawnej z art. 6 ust 1 RODO]*

[Kategorie danych osobowych] Będziemy przetwarzać Pani/Pana dane osobowe takie jak: *[wskazanie jakie kategorie danych osobowych będą przetwarzane (np. imię, nazwisko, adres mailowy, itp.)]*

[Odbiorcy danych] Pani/Pana dane osobowe mogą zostać ujawnione *[wskazanie jakim podmiotom zostaną ujawnione pozyskane dane osobowe (np. księgowość, pracownicy, itp.)]*.

[Przekazywanie danych do państw trzecich] Pani/Pana dane osobowe mogą być przekazywane do państwa trzeciego tj. poza Europejski Obszar Gospodarczy. Jednak nastąpi to wyłącznie jedynie w zakresie na jaki będzie pozwalać prawo, w szczególności na podstawie decyzji Komisji Europejskiej stwierdzającej odpowiedni poziom ochrony lub standardowych klauzul umownych UE. W każdym wypadku Administrator zapewnia możliwość uzyskania dalszych informacji i otrzymania kopii odpowiednich zabezpieczeń. *[jeżeli dane nie będą udostępnianie do państw trzecich należy to zaznaczyć]*

[Okres przechowywania danych] Pani/Pana dane osobowe będą przechowywane przez nas przez okres *[wskazanie okresu przez jaki będą przechowywane dane osobowe]*

[Prawa osób, których dane dotyczą] Zgodnie z RODO przysługuje Pani/Panu:

1. Prawo dostępu do Pani/Pana danych oraz otrzymania ich kopii;
2. Prawo sprostowania (poprawienia) Pani/Pana danych;

3. Prawo usunięcia, ograniczenia lub wniesienia sprzeciwu wobec przetwarzania Pani/Pana danych;
4. Prawo do cofnięcia zgody w dowolnym momencie;
5. Prawo przenoszenia danych;
6. Prawo wniesienia skargi do organu nadzorczego, którym w Polsce jest Prezes Urzędu Ochrony Danych Osobowych.

[Wymóg podania danych] Podanie przez Panią/Pana danych jest dobrowolne, ale konieczne do tego, żeby *[wskazanie, dlaczego podanie danych osobowych jest koniczne (np. konieczne jest, aby odpowiedzieć na Pani/Pana pytania oraz przesłać newseltter, w razie braku wyrażenia zgody nie będziemy mogli skontaktować się z Panią/Panem.)]*

[Informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu] Podane przez Panią/Pana dane osobowe *[wskazanie czy przetwarzane dane osobowe będą profilowane]*.

ZAŁ. 4 – REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH

Kategorie przetwarzań/ czynności przetwarzania oraz cel przetwarzania danych	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa	Nazwa i dane kontaktowe administratora	Inspektor Ochrony Danych Osobowych/ Administrator Bezpieczeństwa Danych Osobowych	Czas trwania przetwarzania	Nazwy państw trzecich lub organizacji międzynarodowych, do których dane są przekazywane	Dokumentacja odpowiednich zabezpieczeń danych osobowych przekazywanych na podstawie art. 49 ust. 1 akapit drugi	Nazwa i dane kontaktowe podmiotu przetwarzającego
[wskazanie jakich czynności związanych z przetwarzaniem danych osobowych dokonuje administrator i w jakim celu]	[wskazanie oraz opisanie środków technicznych oraz organizacyjnych jakich stosuje administrator w celu zabezpieczenia procesów przetwarzania danych]	[nazwa podmiotu, forma prawna, adres, KRS, NIP, REGON]	[imię nazwisko, adres mailowy lub telefon]	[wskazanie przez jaki okres czasu będą przetwarzane dane osobowe przyporządkowane do określonej czynności przetwarzania]	[wskazanie czy dane osobowe będą udostępniane państwom trzecim, jeżeli tak, to jakim]	[gdy ma to zastosowanie – Wskazanie jakie dane są przekazywane do państwa trzeciego lub organizacji międzynarodowej oraz wskazanie dokumentów mających na celu wprowadzenie odpowiednich zabezpieczeń]	[nazwa podmiotu, forma prawna, adres, KRS, NIP, REGON – jeżeli występuje podmiot przetwarzający dane osobwe należy przygotować dla niego również rejestr czynności przetwarzania danych osobowych]

ŁUKASZ DUDEK

autor poradnika

prawnik i aplikant adwokacki. Absolwent Wydziału Prawa i Administracji Uniwersytetu Śląskiego. Fundator i Wiceprezes Fundacji Rozwoju Społeczno – Gospodarczego Prospekt.

Swoje doświadczenie społeczne i ekspercie zdobywał piastując zarządcze funkcje w organizacjach III sektora, oraz zarządzając licznymi projektami edukacyjnymi na szczeblu lokalnym oraz ogólnopolskim.

Naukowe oraz zawodowe zainteresowania skupia wokół ochrony danych osobowych, szeroko pojętego prawa przedsiębiorców w tym w szczególności prawa gospodarczego i handlowego oraz prawnych aspektów organizacji III sektora. W chwili obecnej realizuje się zawodowo w jednej z warszawskich kancelarii w obszarze prawa spółek, fuzji i przejęć oraz praw karnego gospodarczego.

KIPR

Patronat: Fundacja PROSPEKT

ISBN 978-83-950021-1-3

Związek Stowarzyszeń Konfederacja Inicjatyw Pozarządowych Rzeczypospolitej
ul. Jaracza 10/1 01-378 Warszawa
REGON: 366784788 KRS: 0000668126 NIP: 5272800295