OCHRONA
DANYCH OSOBOWYCH

Ewa Rybus-Tołłoczko

Trener NGO – działania szkoleniowo-doradcze na rzecz rozwoju potencjału organizacji pozarządowych w województwie kujawsko-pomorskim

TORUŃSKIE STOWARZYSZENIE AKTYWNOŚCI SPOŁECZNEJ

WOJEWÓDZTWO KUJAWSKO-POMORSKIE

”

Toruń 24.10.2018r

Bydgoszcz, 25.09.2018r

Projekt dofinansowany ze środków Samorządu Województwa Kujawsko-Pomorskiego

TORUŃSKIE STOWARZYSZENIE AKTYWNOŚCI SPOŁECZNEJ

WOJEWÓDZTWO KUJAWSKO-POMORSKIE

Ochrona Danych Osobowych w praktyce w perspektywie nowego stanu prawnego (RODO)– szkolenie i warsztaty dla organizacji pozarządowych z województwa kujawsko-pomorskiego

Szkolenie prowadzi:

EWA RYBUS-TOŁŁOCZKO

Projekt dofinansowany ze środków Samorządu Województwa Kujawsko-Pomorskiego

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

Definicje

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

Definicje

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

Definicje

zbiór danych osobowych - oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;

Nie rejestruje się zbiorów danych osobowych.

Definicje

administrator - oznacza właściwy organ, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby przetwarzania są określone prawem Unii lub prawem państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania;

Administrator

Administratorem Danych Osobowych jest jednostka/instytucja/organizacja.

Współadministratorzy

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

Współadministratorzy

Uzgodnienia należycie odzwierciedlają odpowiednie zakresy obowiązków współadministratorów oraz relacje pomiędzy nimi a podmiotami, których dane dotyczą. Zasadnicza treść uzgodnień jest udostępniana podmiotom, których dane dotyczą. Niezależnie od uzgodnień osoba, której dane dotyczą, może wykonywać przysługujące jej prawa wynikające z niniejszego rozporządzenia wobec każdego z administratorów.

Definicje

podmiot przetwarzający - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę organizacyjną lub inny podmiot, który przez określony czas przetwarza dane osobowe w imieniu administratora.

Powierzenie przetwarzania:

Administrator może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych.

Podmiot, może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie.

Podmiot jest obowiązany przed rozpoczęciem przetwarzania danych podjąć środki zabezpieczające zbiór danych.

W zakresie przestrzegania tych przepisów podmiot ponosi odpowiedzialność jak administrator danych.

Odpowiedzialność za przestrzeganie przepisów niniejszej ustawy spoczywa na administratorze danych, co nie wyłącza odpowiedzialności podmiotu, który zawarł umowę, za przetwarzanie danych niezgodnie z tą umową.

Udostępnianie danych

Udostępnienie danych polega na tym, że w skutek udostępnienia danych osobowych dochodzi do faktycznego przekazania danych osobowych, w wyniku którego nowy dysponent tych danych staje się ich administratorem, a co za tym idzie będzie decydował o celach i środkach przetwarzania danych, oraz ponosił odpowiedzialność w zakresie przewidzianym dla administratora.

Udostępnianie danych

Odmowa udzielenia danych:

- ujawnienie wiadomości zawierających informacje niejawne;
- zagrożenie dla obronności lub bezpieczeństwa państwa, życia i zdrowia ludzi lub bezpieczeństwa i porządku publicznego;
- zagrożenie dla podstawowego interesu gospodarczego lub finansowego państwa;
- istotne naruszenie dóbr osobistych osób, których dane dotyczą, lub innych osób.

Definicje

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;

72 godziny na zgłoszenie zdarzenia

Naruszenie

Zgłoszenie musi zawierać co najmniej:

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

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

c)opis możliwych konsekwencji naruszenia ochrony danych osobowych;

d)opis środków zastosowanych lub proponowanych przez administratora w celu naprawy naruszenia ochrony danych osobowych, w tym w stosowanym przypadku zminimalizowania jego ewentualnych negatywnych skutków.

Naruszenie

W przypadku gdy naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o naruszeniu ochrony danych osobowych.

Skierowane do osoby, której dane dotyczą, zawiadomienie opisuje jasnym i prostym językiem charakter naruszenia ochrony danych osobowych i zawiera co najmniej informacje i środki.

Naruszenie

Skierowane do osoby, której dane dotyczą, zawiadomienie, nie jest wymagane, jeżeli spełniony został którykolwiek z następujących warunków:

a)administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, zwłaszcza środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;

b)administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osób, których dane dotyczą, wskazanych w ust. 1; lub

Naruszenie

Skierowane do osoby, której dane dotyczą, zawiadomienie, nie jest wymagane, jeżeli spełniony został którykolwiek z następujących warunków:

c) wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

Dane wrażliwe –
przetwarzanie szczególnych kategorii danych osobowych:

ujawniające:

pochodzenie rasowe lub etniczne,

poglądy polityczne,

przekonania religijne lub światopoglądowe

przynależność do związków zawodowych

Dane wrażliwe –
przetwarzanie szczególnych kategorii danych osobowych:

przetwarzanie danych:

genetycznych,

biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej,

dotyczących zdrowia

dotyczących seksualności

dotyczących orientacji seksualnej osoby fizycznej

Dane wrażliwe –
przetwarzanie szczególnych kategorii danych osobowych:

przetwarzanie danych:
dotyczących wyroków skazujących
naruszeń prawa

Kiedy przetwarzamy dane osobowe:

- osoba, której dane dotyczą, wyrazi na to zgodę;
- na podstawie przepisów prawa;
- dla dobra publicznego;
- gdy zostały udostępnione administratorowi.

Zasada minimalizacji danych

Zasada minimalizacji danych osobowych - zgodnie z nią, można przetwarzać wyłącznie takie dane osobowe, które są niezbędne do osiągnięcia celu przetwarzania danych. Przetwarzanie danych powinno więc zostać ograniczone do takich danych, bez których nie można osiągnąć celu przetwarzania danych

Prawo do sprostowania danych

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

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

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

a)dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;

b)osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie i nie ma innej podstawy prawnej przetwarzania;

c)osoba, której dane dotyczą, wnosi sprzeciw wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania

d)dane osobowe były przetwarzane niezgodnie z prawem;

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

e) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator;

f) dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego.

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

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

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

Prawo do usunięcia danych nie ma zastosowania, w zakresie w jakim przetwarzanie jest niezbędne:

a)do korzystania z prawa do wolności wypowiedzi i informacji;

b)do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;

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

c) z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego;

d) do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, o ile prawdopodobne jest, że prawo uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania; lub

e) do ustalenia, dochodzenia lub obrony roszczeń.

Prawo do ograniczenia przetwarzania

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

a)osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych – na okres pozwalający administratorowi sprawdzić prawidłowość tych danych;

b)przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;

Prawo do ograniczenia przetwarzania

c) administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;

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

Prawo do ograniczenia przetwarzania

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

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

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

Administrator informuje o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania, każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku.

Administrator informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.

Dokumentacja wewnętrzna:

1. Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane.

2. Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki, o których powyżej obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych.

Analiza ryzyka

Na ryzyko w zakresie ochrony danych wpływają różne czynniki, zarówno zewnętrzne, jak i wewnętrzne, ważne jest sporządzenie ich listy.

Do informacji zewnętrznych można przykładowo zaliczyć:

-informacje dotyczące środowiska prawnego,

-informacje dotyczące środowiska społecznego,

-informacje dotyczące środowiska politycznego,

-informacje dotyczące korzystania z usług lub zasobów podmiotów zewnętrznych,

-informacje o zasięgu terytorialnym działalności organizacji.

Analiza ryzyka

Do informacji wewnętrznych można przykładowo zaliczyć:

-strukturę i rozmiary organizacji,

-strategie i polityki stosowane w organizacji,

-systemy obiegu informacji, procesy podejmowania decyzji, rola przywództwa,

-informacje dotyczące środowiska technologicznego i możliwości jego zmian (finansowych, technicznych, organizacyjnych),

-normy i standardy przyjęte przez organizację, tzw. kultura organizacyjna.

Należy zidentyfikować i sklasyfikować wszystkie aktywa organizacji, które wiążą się z przetwarzaniem danych osobowych.

Analiza ryzyka

Poprzez „aktywa” rozumieć należy zarówno informacje, w tym dane osobowe, jak i inne zasoby organizacji, takie jak:

-posiadana wiedza,

-personel,

-sprzęt,

-oprogramowanie,

-inne środki techniczne i organizacyjne związane z przetwarzaniem danych osobowych.

Analiza ryzyka

Zagrożenia:

-organizacyjne,

-personalne

-techniczne,

-fizyczne.

Analiza ryzyka

Kryteria akceptacji ryzyka definiuje się zwykle przez wartość progową, np. przy przedziałach ryzyka w zakresie 0-2, 3-5 oraz 6-8. Jako akceptowalną wartość ryzyka można przyjąć wartość mniejszą od 2.

Kryteria akceptacji ryzyka są niezwykle istotne w postępowaniu z ryzykiem, ponieważ na ich podstawie podejmowane są decyzje dotyczące zidentyfikowanych ryzyk w zakresie ich dopuszczalności.

Przy ustalaniu kryteriów należy uwzględniać nie tylko potencjalny, bezpośredni wpływ urzeczywistnienia się danego ryzyka na działalność biznesową organizacji (jak np. utrata klientów czy kary finansowe za naruszenie ich praw).

Nie można zapominać przy tym o uwarunkowaniach prawnych, w tym karach za naruszenie przepisów RODO, jak również o zawartych umowach i przyjętych regulaminach.

Analiza ryzyka

Zabezpieczeń organizacyjnych, tj. środki organizacyjne oraz wymagania dotyczące polityki zarządzania procesem przetwarzania, w tym zastosowanych procedur:

-zarządzania projektem,

-zarządzania incydentami,

-zarządzania personelem,

-zarządzania udziałem stron trzecich, w tym podmiotów przetwarzających,

-zarządzania eksploatacją używanych systemów i innych narzędzi przetwarzania danych,

-sposobu nadzoru, w tym audytów i raportowania alertów.

Analiza ryzyka

Środków kontroli logicznej procesu przetwarzania, w tym wymagań dotyczących zastosowania takich środków ochrony, jak:

-anonimizacja i pseudonimizacja,

-środki ochrony kryptograficznej,

-środki kontroli integralności danych,

-środki kontroli dostępu do danych,

-środki kontroli dotyczące rozliczalności wykonywanych operacji,

-środki wspierające weryfikację danych na etapie ich wprowadzania, typu: zgodność z wzorcem, podanymi wartościami granicznymi itp.,

-środki bieżącego monitoringu,

-zastosowane środki ochrony przed działaniem oprogramowania szkodliwego typu wirusy, środki szpiegujące, środki służące ochronie przed wykradaniem danych itp.

-środki ochrony sieci przed działaniem osób z zewnątrz.

Analiza ryzyka

Środków ochrony fizycznej wszystkich aktywów informacyjnych i technicznych, w tym:

-dotyczących miejsca przetwarzania danych, takich jak: ukształtowanie terenu (np. podatność na powódź, wyładowania atmosferyczne itp.), sąsiedztwo obiektów lub podmiotów, mogących wpływać na bezpieczeństwo, jak np. lotnisko, stacja paliw, zakłady przetwórstwa chemicznego itp.,

-środków bezpieczeństwa infrastruktury technicznej wykorzystywanej do przetwarzania danych,

-środków bezpieczeństwa dokumentacji papierowej, w tym papierowych rejestrów zawierających dane osobowe,

-środków bezpieczeństwa związanych z przepływem informacji w postaci dokumentów papierowych lub nośników elektronicznych,

-środków ochrony przed żywiołami niezależnymi od człowieka, typu ogień, woda.

Analiza ryzyka

Określenie listy zidentyfikowanych ryzyk:

-rodzaj operacji przetwarzania danych,

-zidentyfikowane zagrożenia,

-poziom ryzyka,

-decyzja,

-uzasadnienie akceptacji wyliczonego poziomu ryzyka.

Analiza ryzyka

W przypadku, gdy podjęta zostanie decyzja o modyfikacji lub całkowitej eliminacji ryzyka, cały proces dotyczący szacowania ryzyka powinien być powtórzony, a w skrajnym przypadku (jeśli ograniczono lub zmieniono cel przetwarzania danych) nawet od samego początku.

Dodatkowo, kiedy na etapie szacowania i oceny ryzyka ustalona zostanie wysoka wartość ryzyka, zgodnie z art. 35 RODO wymagane jest przeprowadzenie dla danego procesu przetwarzania oceny jego skutków w zakresie ochrony praw i wolności dla osób, których dane są przetwarzane.

Polityka ochrony danych osobowych

1) analiza ryzyka

2) definicję bezpieczeństwa informacji, jego ogólne cele i zakres oraz znaczenie bezpieczeństwa jako mechanizmu umożliwiającego współużytkowanie informacji;

3) krótkie wyjaśnienie polityki bezpieczeństwa, zasad, standardów i wymagań zgodności mających szczególne znaczenie dla instytucji, np.:

a) zgodność z prawem i wymaganiami wynikającymi z umów;

b) wymagania dotyczące kształcenia w dziedzinie bezpieczeństwa;

c) zapobieganie i wykrywanie wirusów oraz innego złośliwego oprogramowania;

d) zarządzanie ciągłością działania biznesowego;

e) konsekwencje naruszenia polityki bezpieczeństwa;

Polityka ochrony danych osobowych

4) procedura zgłaszania przypadków naruszenia bezpieczeństwa;

5) sposób przepływu danych pomiędzy poszczególnymi systemami;

6) określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przy przetwarzaniu danych;

7) zarządzanie w systemami informatycznymi;

8) kwestie spełnienia obowiązków informacyjnych oraz praw osób, których dane dotyczą, w tym „prawa do bycia zapomnianym”;

9) prawa do przenoszalności danych.

Polityka ochrony danych osobowych

Polityka powinna zostać przyjęta przez kierownika jednostki.

Upoważnienie pisemne fakultatywne:

Tak było:

- imię i nazwisko osoby upoważnionej,
- nazwę zbioru danych osobowych,
- zakres upoważnienia,
- zobowiązanie do zachowania tajemnicy,
- termin ważności,
- możliwość wygaśnięcia upoważnienia,
- nakaz zwrotu oryginału.

Ewidencja pisemna - fakultatywna:

Tak było:

- imię i nazwisko osoby upoważnionej,
- datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych,
- identyfikator, jeżeli dane są przetwarzane w systemie informatycznym.

Przechowywanie danych osobowych

W systemach informatycznych muszą być w szczególny sposób zabezpieczone.

Pomieszczenie wyodrębnione, w sposób swobodny do przeglądania danych osobowych.

Dane osobowe powinny być przechowywane w sposób uniemożliwiający dostęp osób trzecich.

Dane osobowe w wersji papierowej powinny być przechowywane w „teczkach”, by przeglądając kartotekę nie można było widzieć wszystkich informacji.

Obowiązek informacyjny zawiera:

1. Dane kontaktowe administratora oraz Inspektora Ochrony Danych (jeżeli został powołany), np. e-mail i telefon.
2. Gdy przetwarzanie odbywa się na mocy przepisu prawa, należy wskazać ten przepis.
3. Gdy przetwarzanie odbywa się na podstawie prawnie uzasadnionego interesu administratora lub strony trzeciej, należy go wskazać.
4. Gdy przetwarzanie odbywa się na podstawie zgody podmiotu danych, o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem.

Obowiązek informacyjny zawiera:

5. Gdy dane zostały pozyskane nie bezpośrednio od podmiotu danych, źródło pochodzenia danych osobowych lub czy pochodzą one ze źródeł publicznie dostępnych.
6. Informacje o zamiarze przekazywania danych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję Europejską odpowiedniego stopnia ochrony. W przypadku przekazania do państwa nie gwarantującego odpowiedniego poziomu ochrony należy podać informację o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych.

Obowiązek informacyjny zawiera:

7. Okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu.
8. Informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania oraz o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych.
9. Prawie wniesienia skargi do organu nadzorczego.
10. Zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

Wyrażenie zgody:

Możliwość pozyskania ustnej zgody.

Zgoda elektroniczna – np. poprzez zaznaczenie odpowiednich okienek.

Należy pamiętać, że w przypadku pozyskiwania zgody w innej formie niż pisemna, to na administratorze danych osobowych będzie ciążył obowiązek udowodnienia, że została ona pozyskana, a nie dorozumiana.

RODO określa wprost: ***Milczenie, okienka domyślnie zaznaczone lub niepodjęcie działania nie powinny oznaczać zgody*****.**

Zgoda powinna dotyczyć wszystkich czynności przetwarzania dokonywanych w tym samym celu lub w tych samych celach. Jeżeli przetwarzanie służy różnym celom, potrzebna jest zgoda na wszystkie te cele.

Wyrażenie zgody:

Administrator nie musi prosić o zgodę na przetwarzanie danych, gdy:

1.Dane będą przetwarzane w związku z zawarciem umowy z osobą, której dane dotyczą.

2.Są one przetwarzane na podstawie przepisu prawa.

3.Są one przetwarzane w interesie publicznym.

4.W prawnie usprawiedliwionym celu administratora danych, np. marketing bezpośredni produktów własnych (podkreślam bezpośredni, nie dotyczy to marketingu telefonicznego i mailowego, o czym napiszę w kolejnym wpisie), dochodzenie roszczeń z tytułu prowadzonej działalności gospodarczej.

5.Żywotny interes osoby, której dane dotyczą, gdy pozyskanie zgody jest konieczne, ale niemożliwe.

Wyrażenie zgody:

RODO przewiduje, że *Administratorzy, którzy są częścią grupy przedsiębiorstw lub instytucji powiązanych z podmiotem centralnym, mogą mieć prawnie uzasadniony interes w przesyłaniu danych osobowych w ramach grupy przedsiębiorstw do wewnętrznych celów administracyjnych, co dotyczy też przetwarzania danych osobowych klientów lub pracowników.*

Należy pamiętać, że przesyłanie danych w ramach grupy przedsiębiorstw/instytucji - wymaga określenia zakresu odpowiedzialności i obowiązków tych podmiotów oraz spełnienia przez nie wymagań bezpieczeństwa określonych przez przepisy. Takie uzgodnienia powinny mieć formę pisemną (będzie to miało bardzo duże znaczenie, w przypadku wycieku danych, gdy będzie ustalany poziom i zakres odpowiedzialności oraz wysokość kary finansowej).

Wyrażenie zgody:

- imię i nazwisko osoby, od której dane są zbierane,
- wyrażenie zgody,
- nazwę, adres administratora danych osobowych,
- cel przetwarzania,
- informacja o możliwości zmiany i cofnięcia zgody na przetwarzanie.

Wyrażenie zgody:

Obowiązek powiadomienia o sprostowaniu lub usunięciu danych:

*Administrator informuje o sprostowaniu lub usunięciu **danych osobowych** lub ograniczeniu przetwarzania, (…) każdego odbiorcę, którego ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Administrator informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.*

Wyrażenie zgody:

Obowiązek powiadomienia o sprostowaniu lub usunięciu danych:

Administrator danych będzie musiał gromadzić dane podmiotów, którym udostępnił dane wraz z kontaktem, na który można będzie dokonać powiadomienia (warto rozważyć już we wniosku o udostępnienie wskazanie formy powiadomienia o zmianie danych podmiotu danych, aby potem nie mieć problemu ze skutecznym wywiązaniem się z tego obowiązku, w szczególności nie narażać się na koszty wysyłania tradycyjnych listów). Pozostaje w mocy zapis, że podmiot danych będzie o tym informowany tylko na żądanie.

Wyrażenie zgody:

Przykładowo, klauzula zgodna z RODO może otrzymać następujące brzmienie:

Zgadzam się na przetwarzanie moich danych osobowych przez spółkę XYZ sp. z o. o. z siedzibą w ……., ul. ……., w celu ……. [np. Udziału w konkursie].

Podanie danych jest dobrowolne. Podstawą przetwarzania danych jest moja zgoda. Odbiorcami danych mogą być ……. [np. podmioty zajmujące się obsługą informatyczną administratora danych]. Mam prawo wycofania zgody w dowolnym momencie. Dane osobowe będą przetwarzane ……. [np. do ew. odwołania zgody, a po takim odwołaniu, przez okres przedawnienia roszczeń przysługujących administratorowi danych i w stosunku do niego].

Mam prawo żądania od administratora dostępu do moich danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania [o prawie do przenoszenia danych, jeżeli przysługuje], a także prawo wniesienia skargi do organu nadzorczego.

[jeżeli dochodzi do profilowania, wówczas informacje dotyczące profilowania].

W przypadku pytań dotyczących przetwarzania danych osobowych prosimy o kontakt z Inspektorem Ochrony Danych pod adresem ……. [jeżeli został wyznaczony].

Rejestr czynności przetwarzania

- imię i nazwisko lub nazwa oraz dane kontaktowe administratora i, w razie potrzeby, współadministratora oraz inspektora ochrony danych;
- cele przetwarzania;
- kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub organizacjach międzynarodowych;
- opis kategorii osób, których dane osobowe dotyczą, oraz kategorii danych osobowych;
- w stosownym przypadku informacje o stosowaniu profilowania;
- w stosownym przypadku kategorie przekazań danych osobowych do państwa trzeciego lub organizacji międzynarodowej;
- wskazanie podstawy prawnej operacji przetwarzania, w tym przekazań, do których dane osobowe są przeznaczone;

Rejestr czynności przetwarzania

- jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;
- jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.

Inspektor Ochrony Danych

Kto może, a kto musi wyznaczyć inspektora ochrony danych?

Ogólne rozporządzenie o ochronie danych w art. 37 ust 1 przewiduje obowiązek wyznaczenia inspektora dla administratorów i podmiotów przetwarzających wówczas, gdy:

a) przetwarzania dokonują **organ lub podmiot** publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości;

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

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

Inspektor Ochrony Danych

Duża skala – ponad 250 osób zatrudnionych.

Inspektor Ochrony Danych

Grupa Robocza art. 29 w swoich wytycznych dotyczących inspektora ochrony danych zaleca administratorom i podmiotom przetwarzającym **udokumentowanie wewnętrznej procedury przeprowadzonej w celu ustalenia i uwzględnienia poszczególnych normatywnych przesłanek istnienia lub braku tego obowiązku**.

Ponadto Grupa Robocza art. 29 rekomenduje wyznaczenie IODO nawet w odniesieniu do podmiotów do tego niezobowiązanych. Inspektorzy ochrony danych mogą bowiem znacznie ułatwić przestrzeganie nowych przepisów oraz odegrać istotną rolę w pośredniczeniu pomiędzy zainteresowanymi stronami (np. organem ochrony danych osobowych, podmiotami danych oraz poszczególnymi jednostkami w ramach jednej organizacji).

Grupa Robocza art. 29 w Wytycznych dotyczących inspektora ochrony danych uznaje za dobrą praktykę powoływanie DPO przez prywatne jednostki realizujące zadania w interesie publicznym lub sprawujące władzę publiczną.

Inspektor Ochrony Danych

Zasady nie uniemożliwiają podmiotom niezobowiązanym do wyznaczenia DPO skorzystania z innego rozwiązania niż wyznaczenie inspektora ochrony danych, np. wyznaczenia pracownika albo zatrudnienie zewnętrznego konsultanta do wypełniania zadań związanych z ochroną danych osobowych. W takim przypadku wedle zaleceń Grupy Roboczej art. 29 ważne jest, aby nazwa stanowiska, status pracownika, pozycja i zadania nie wprowadzały w błąd. W związku z tym należy poinformować pracowników organizacji, organ nadzorczy, osoby, których dane dotyczą, i ogół społeczeństwa, iż osoba zatrudniona nie jest DPO w świetle przepisów RODO.

Zgodnie z art. 37 ust. 6 RODO inspektorem ochrony danych **może zostać zarówno pracownik administratora lub podmiotu przetwarzającego, jak i osoba spoza grona pracowników ww. podmiotów**. Możliwe będzie więc nadal pełnienie funkcji inspektora ochrony danych w modelu outsourcingu, na podstawie umowy o świadczenie usług.

Inspektor Ochrony Danych

W przypadku podmiotów prywatnych, jednego inspektora może powołać **grupa przedsiębiorstw** (np. grupa kapitałowa), o ile można będzie łatwo nawiązać z nim kontakt z każdej jednostki organizacyjnej (art. 37 ust. 2 RODO). Jeżeli administrator lub podmiot przetwarzający są **organem lub podmiotem publicznym,** dla kilku takich organów lub podmiotów można wyznaczyć – z uwzględnieniem ich struktury organizacyjnej i wielkości – jednego inspektora ochrony danych (art. 37 ust. 3 RODO).

Jak wynika z Wytycznych Grupy Roboczej , wyznaczając jednego inspektora ochrony danych dla kilku podmiotów (zarówno publicznych, jak i prywatnych), należy uwzględnić, że musi on być „łatwo dostępny” dla osób wewnątrz organizacji.

Inspektor pełni ponadto funkcję **punktu kontaktowego** dla organu nadzorczego oraz osób, których dane są przetwarzane.

Inspektor Ochrony Danych

Kwalifikacje do pełnienia funkcji:

Zgodnie z art. 37 ust. 5 RODO inspektor ochrony danych jest **wyznaczany na podstawie kwalifikacji zawodowych**, a w szczególności **wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych** oraz **umiejętności wypełnienia swoich zadań.** Poziom wiedzy inspektora powinien być ustalany w kontekście konkretnych potrzeb administratora danych i procesora.

Inspektor ochrony danych powinien wykazywać się **wiedzą zarówno teoretyczną, jak i praktyczną dotyczącą ogólnego rozporządzenia o ochronie danych oraz przepisów krajowych regulujących przetwarzanie danych.**

Jak wskazuje Grupa Robocza art. 29 wymagany **poziom wiedzy fachowej** nie jest nigdzie jednoznacznie określony, ale musi być współmierny do charakteru, skomplikowania i ilości danych przetwarzanych w ramach jednostki.

Inspektor Ochrony Danych

Istnieje kilka zabezpieczeń, które zapewniają IODO możliwość działania w sposób niezależny:

1.brak instrukcji od administratorów lub podmiotów przetwarzających dotyczących wykonywania zadań DPO;

2.zakaz zwolnienia albo nałożenia kary przez administratora danych za wykonywanie zadań DPO;

3.brak konfliktu interesów z innymi możliwymi zadaniami i obowiązkami.

Inspektor Ochrony Danych

Pozostałe zadania i obowiązki IODO nie mogą prowadzić do konfliktu interesów. Oznacza to po pierwsze, że IODO nie może zajmować stanowiska w organizacji, które prowadziłoby go do określania celów i sposobów przetwarzania danych osobowych.

Co do zasady, za powodujące konflikt interesów uważane będą stanowiska kierownicze (dyrektor generalny, dyrektor ds. operacyjnych, dyrektor finansowy, dyrektor ds. medycznych, kierownik działu marketingu, kierownik działu HR, kierownik działu IT), ale również niższe stanowiska, jeśli biorą udział w określaniu celów i sposobów przetwarzania danych. Ponadto, konflikt interesów może powstać, gdy zewnętrzny IODO zostanie poproszony o reprezentowanie administratora lub podmiotu przetwarzającego przed sądem w sprawie dotyczącej ochrony danych osobowych.

Inspektor Ochrony Danych

Zadania:

a)informowanie administratora oraz pracowników zajmujących się przetwarzaniem o obowiązkach spoczywających na nich na mocy niniejszej dyrektywy oraz na mocy innych przepisów prawa Unii lub państwa członkowskiego dotyczących ochrony danych;

b)monitorowanie przestrzegania niniejszej dyrektywy, innych przepisów prawa Unii lub państwa członkowskiego dotyczących ochrony danych oraz realizowanie polityk administratora w dziedzinie ochrony danych osobowych, w tym przydział obowiązków, działania podnoszące świadomość i szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;

c)przedstawianie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie ich wykonania;

d)współpraca z organem nadzorczym;

Inspektor Ochrony Danych

Zadania:

e)pełnienie funkcji punktu kontaktowego wobec organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami oraz w stosownym przypadku prowadzenie konsultacji we wszelkich innych sprawach;

f)pełnienie roli punktu kontaktowego dla osób, których te dane dotyczą;

g)Prowadzenie rejestru kategorii czynności.

Inspektor Ochrony Danych

- Osoba pełniąca w dniu 24 maja 2018 r. funkcję ABI, staje się, z mocy ustawy, IOD i pełni swoją funkcje do dnia 1 września 2018 r., chyba, że do tego dnia administrator zawiadomi Prezesa Urzędu o wyznaczeniu innej osoby na inspektora ochrony danych
- Administrator, który do dnia wejścia w życie niniejszej ustawy nie powołał administratora bezpieczeństwa informacji, a który ma obowiązek wyznaczenia inspektora ochrony danych, wyznacza inspektora ochrony danych oraz zawiadamia Prezesa Urzędu, w terminie do dnia 31 lipca 2018 r.

Gdzie szukać informacji?

www.uodo.gov.pl

DZIĘKUJĘ 💻

Ewa Rybus-Tołłoczko
ewa.rybus-tolloczko@rt-net.pl
601 375 416