DANE 2.0: RODO W NGO

poradnik dla organizacji pozarządowych

współfinansowane z budżetu
Województwa Zachodniopomorskiego

Pomorze Zachodnie

SEKTOR 3
Centrum Wspierania Organizacji Pozarządowych

DANE 2.0:
RODO W NGO
poradnik dla organizacji pozarządowych

Szczecin, 2018

w imieniu Centrum Wspierania Organizacji Pozarządowych Sektor 3 Szczecin i autorki Pani Marty Turskiej, przekazujemy poradnik, który powstał w ramach realizacji zadania publicznego 'dane 2.0: rodo w ngo' na podstawie lokalnych spotkań i pytań organizacji pozarządowych. Mamy nadzieję, że niniejsza publikacja okaże się pomocna w codziennej działalności organizacji.

Sektor 3 Szczecin

www.sektor3.szczecin.pl
al. Wojska Polskiego 63, Szczecin, 91 350 82 99
biuro@sektor3.szczecin.pl
FB/sektor3szczecin

od autora
Marta Turska
radca prawny

Szanowni Państwo,

przekazuję Państwu poradnik dotyczących stosowania ogólnego rozporządzenia o ochronie danych (RODO) w organizacjach pozarządowych. W poradniku przedstawiam podstawowe informacje merytoryczne w przedmiocie zakresu stosowania RODO w odniesieniu do działalności NGO. Prócz tego omawiam zasady przetwarzania danych osobowych oraz związane z tym określone w RODO obowiązki, z uwzględnieniem charakterystyki związanej z działalnością Organizacji Pozarządowych. Poradnik uzupełnia dodatkowo wybór wzorów podstawowych dokumentów do zastosowania w codziennej pracy. W odrębnej części poradnika zawarto odpowiedzi na pytania zebrane podczas przeprowadzonych szkoleń.

Mam nadzieję, że publikacja okaże się przydatna we wdrażaniu w ogólnego rozporządzenia o ochronie danych (RODO).

współfinansowane z budżetu
Województwa Zachodniopomorskiego

Wykaz skrótów

IOD - Inspektor Ochrony Danych

KC - Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny (t.j. Dz. U. z 2017 r. poz. 459 z późn. zm.)

KP - Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy (t.j. Dz. U. z 2018 r. poz. 108 z późn. zm.)

KPA - Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (t.j. Dz. U. z 2017 r. poz. 1257 z późn. zm.)

KPC - Ustawa z dnia 17 listopada 1964 r. Kodeks postępowania cywilnego (t.j. Dz. U. z 2018 r. poz. 155 z późn. zm.).

PPSA - Ustawa z dnia 30 sierpnia 2002 r. Prawo o postępowaniu przed sądami administracyjnymi (t.j. Dz. U. z 2017 r. poz. 1369 z późn. zm.)

UODO - ustawa o ochronie danych osobowych z dnia 16 marca 2018 r.

PUODO - Prezes Urzędu Ochrony Danych Osobowych

RODO - 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) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1)

Poruszone zagadnienia w poradniku

Źródła prawa
Definicje i ogólne pojęcia
Dane osobowe (DO) i ich kategorie
Wyłączenia stosowania RODO
Zasady związane z przetwarzaniem DO
Podstawy prawne i czynności przetwarzania
Charakterystyka podmiotów
Obowiązki Administratora
Obowiązek informacyjny
Privacy by design
Bezpieczeństwo ochrony DO
Naruszenie zasad ochrony DO
Ocena skutków dla ochrony danych
Rejestr czynności przetwarzania danych osobowych
Inspektor danych osobowych
Uprawnienia podmiotu którego dotyczą dane osobowe
Środki ochrony prawnej
Kary pieniężne
Harmonogram wdrożenia RODO

dodatkowo

10 podstawowych zasad dla NGO
Wzory podstawowych dokumentów związanych z przetwarzaniem danych osobowych
Materiały pomocnicze i zagadnienia praktyczne

ŹRÓDŁA PRAWA

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

państwa członkowskie mają przyjąć i opublikować przepisy wykonujące dyrektywę do dnia 6 maja 2018 r., czyli wcześniej niż zaczyna obowiązywać RODO

Ustawa z dnia 10 maja 2018r. o ochronie danych osobowych

1) służy stosowaniu rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych),

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

3) zmienia szereg krajowych ustaw, które wpływają również na działalność organizacji pozarządowych

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)

Rozporządzenie Parlamentu Europejskiego i Rady ma zasięg ogólny, wiąże w całości, co do wszystkich zawartych w nim postanowień, i jest bezpośrednio stosowane we wszystkich państwach członkowskich. Ze swej natury staje się ono częścią krajowych systemów prawnych i wywiera skutki bezpośrednie w stosunku do jednostek. Równocześnie RODO w pewnym zakresie przewiduje uzupełnienie własnych regulacji przepisami krajowymi. Zawarte w RODO odesłania do prawa krajowego mają na celu przede wszystkim doprecyzowanie lub ograniczenie stosowania w tymże prawie krajowym przepisów RODO. Przepisy RODO wyznaczają ustawodawcy krajowemu obligatoryjny oraz fakultatywny zakres regulacji prawnej, która uzupełnia RODO w wewnętrznym porządku krajowym.

DEFINICJE I OGÓLNE POJĘCIA

Termin „dane osobowe” jest zdefiniowany w art. 4 pkt 1 RODO w następujący sposób: „informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, której dane dotyczą; możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej”.

Zakres pojęcia danych osobowych jest bardzo szeroki. Celem takiego ujęcia tego terminu jest zapewnienie osobom fizycznym jak najpełniejszej ochrony w związku z przetwarzaniem ich danych osobowych.

Pojęcie „informacji” należy rozumieć szeroko, w odniesieniu do wszelkich stwierdzeń na temat osoby. Treść informacji dotyczyć może zarówno sfery życia prywatnego osoby fizycznej, jak i sfery zawodowej, wszelkiego rodzaju aktywności, czynności ekonomicznych i gospodarczych czy społecznych, w rozmaitych konfiguracjach. Informacje ww. mogą zatem dotyczyć tzw. „prywatnej” osoby fizycznej – to pojęcie ma charakter bardzo umowny i służyć ma odróżnieniu jej od osoby fizycznej występującej zawodowo, także w obrocie gospodarczym.

Rodzaje danych osobowych - na podstawie RODO można wyróżnić trzy rodzaje danych osobowych:

- tzw. dane zwykłe,
- szczególne kategorie danych osobowych,
- dane osobowe dotyczące wyroków skazujących i naruszeń prawa.

Do ostatniej kategorii zaliczają się – zgodnie z art. 10 RODO – dane osobowe dotyczące wyroków skazujących oraz naruszeń prawa lub powiązanych środków bezpieczeństwa.

Szczególne kategorie danych określone są w art. 9 ust. 1 RODO. Są to: dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, dane biometryczne przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej oraz dane dotyczące zdrowia, seksualności lub orientacji seksualnej.

Niektóre ze szczególnych kategorii danych są szczegółowo zdefiniowane w art. 4 pkt 13-15 RODO:

- „dane genetyczne oznaczają dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej”;
- „dane biometryczne oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne”;
- „dane dotyczące zdrowia oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia”.

Natomiast wszelkie inne dane osobowe określane są jako tzw. zwykłe dane osobowe. Innymi słowy, dane zwykłe są danymi osobowymi, które nie należą ani do szczególnych kategorii danych, ani nie dotyczą wyroków skazujących lub naruszeń prawa.

DEFINICJE I OGÓLNE POJĘCIA

Przedmiotowym zakres stosowania RODO określony jest w art. 2 RODO. Zgodnie z art. 2 ust. 1 RODO, ogólne rozporządzenie „ma zastosowanie do przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany oraz do przetwarzania w sposób inny niż zautomatyzowany danych osobowych stanowiących część zbioru danych lub mających stanowić część zbioru danych". Znaczenie dla określenia przedmiotowego stosowania RODO mają zatem definicje „przetwarzania", „danych osobowych" oraz „zbioru".

Termin „przetwarzanie" jest zdefiniowany w art. 4 pkt 2 RODO jako czynność lub zestaw czynności „wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie". Zakres pojęciowy przetwarzania jest zatem bardzo szeroki, a wyliczenie operacji w powyższej definicji ma charakter przykładowy.

Definicja „danych osobowych" została omówiona w podrozdziale 2.1. Natomiast „zbiór danych" został określony w art. 4 pkt 6 RODO w następujący sposób: „uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie".

Należy pamiętać, że pojęcie zbioru danych odnosi się tylko do ręcznego przetwarzania danych osobowych.

WYŁĄCZENIA STOSOWANIA RODO

Na mocy art. 2 ust. 2 RODO stosowanie RODO wyłączone jest w następujących przypadkach przetwarzania danych osobowych:

- przez osobę fizyczną w ramach czynności o czysto osobistym lub domowym charakterze;
- przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom.
- w ramach działalności nie objętej zakresem prawa Unii, np. działalność dotycząca bezpieczeństwa narodowego;
- przez państwa członkowskie w ramach wykonywania działań wchodzących w zakres wspólnej polityki zagranicznej i bezpieczeństwa Unii;

Omówienia szczegółowego wymagają dwie pierwsze sytuacje.

Poprzez przetwarzanie w ramach czynności o charakterze osobistym lub domowym rozumie się przetwarzanie bez związku z działalnością zawodową lub handlową. Jako przykłady takiej działalności w motywie 18 RODO wskazano prowadzenie korespondencji osobistej i przechowywanie adresów, podtrzymywanie więzi społecznych oraz działalność internetową podejmowaną w ramach takiej działalności. Natomiast drugie wyłączenie odnosi się do przetwarzania danych osobowych przez organy ścigania w ramach wykonywanych przez nie zadań dotyczących zapobiegania przestępczości, prowadzenia postępowań karnych itd.

Z kolei art. 9 RODO wskazuje na zakaz przetwarzania danych, który odnosi się do następujących sytuacji. Otóż zgodnie z jego brzmieniem zabrania się przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby.

WYŁĄCZENIA STOSOWANIA RODO

Wcześniej opisana ogólna i bezwzględnie obowiązująca norma, przewiduje wyjątki i dopuszcza w określonych przypadkach wyłączenia jej zastosowania, o ile spełniony jest eden z określonych warunków:

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

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

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

4. 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;

5. przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą;

6. przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy;

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

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

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

10. przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie, konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.

ZASADY ZWIĄZANE Z PRZETWARZANIEM

Wszystkie czynności przetwarzania danych powinny być zgodne z podstawowymi zasadami dotyczącymi przetwarzania danych osobowych, wskazanymi w art. 5 RODO

1. zasada zgodności z prawem, rzetelności i przejrzystości

„Dane osobowe muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą"

Zgodność z prawem przetwarzania oznacza, że podstawą prawną przetwarzania jest jedna z przesłanek wymienionych w art. 6 ust. 1 RODO lub art. 9 ust. 2 RODO, a także, że przetwarzanie jest zgodne z innymi przepisami o ochronie danych osobowych. Rzetelność przetwarzania interpretuje się jako jego ogólną uczciwość oraz proporcjonalność ingerencji w prywatność związaną z przetwarzaniem danych osobowych. Aby zachować zasadę przejrzystości, należy przekazywać osobom, których dane dotyczą zrozumiałe i kompletne informacje na temat przetwarzania ich danych osobowych. Dodatkowe wymogi dotyczące zasady przejrzystości sformułowane są w art. 12 RODO. Zgodnie z tym przepisem, wszelkie informacje i komunikaty przekazywane osobom, których dane dotyczą, powinny być łatwo dostępne i zrozumiałe oraz napisane jasnym i prostym językiem.
Celem tej zasady jest zapewnienie, aby osoby, których dane dotyczą miały pełną wiedzę na temat operacji przetwarzania, w tym konsekwencji przetwarzania ich danych oraz przysługujących im praw związanych z przetwarzaniem danych osobowych.

2. zasada ograniczenia celu

„Dane osobowe muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami"

Zasada ograniczenia celu wymusza po pierwsze wskazanie określonego, zgodnego z prawem celu przetwarzania w momencie zbierania danych. Po drugie, zgodnie z tą zasadą zabronione jest przetwarzanie w innym celu, chyba że dalsze przetwarzanie odbywa się na podstawie przepisów prawa unijnego lub prawa krajowego, lub administrator uzyskał zgodę osoby, której dane dotyczą na dalsze przetwarzanie, lub ten wtórny cel przetwarzania nie jest niezgodny z celem pierwotnym. Zgodność wtórnego celu przetwarzania z celem pierwotnym ocenia się między innymi na podstawie kryteriów wskazanych w art. 6 ust. 4 RODO, takich jak wszelkie związki między celami, kontekst, w którym zebrano dane osobowe, charakter danych osobowych, a także ewentualne konsekwencje zamierzonego dalszego przetwarzania dla osób, których dane dotyczą. Dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uważane za niezgodne z pierwotnym celem przetwarzania, na mocy art. 5 ust. 1 lit. b) RODO.

3. zasada minimalizacji danych

Szeroko omawiana w trakcie szkoleń zasada minimalizacji danych oznacza, że „dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane".

Zgodnie z tą zasadą administrator danych może zbierać tylko takie dane osobowe, które są mu konieczne do osiągnięcia celu ich zebrania. Zakazane jest zatem zbieranie danych w niepotrzebnych w konkretnym celu, czy też zbieranie danych „na zapas". Zasada ta powiązana jest z zasadą ograniczenia celu, ponieważ to cel przetwarzania determinuje zakres danych potrzebnych do osiągnięcia tego celu. Należy wręcz – pozyskując dane – powstrzymywać przekazujących dane przed przekazaniem nawet dobrowolnym szerszego niż niezbędny zakresu.

ZASADY ZWIĄZANE Z PRZETWARZANIEM

4. zasada prawidłowości danych

„Dane osobowe muszą być prawidłowe i w razie potrzeby uaktualniane"

Powyższa zasada odnosi się do poprawności danych i ich zgodności z prawną. Zgodnie z zasadą prawidłowości danych, jakiekolwiek nieprawidłowe, niepoprawne, nieprawdziwe dane osobowe powinny być jak najszybciej usunięte lub poprawione.

5. zasada ograniczenia przechowywania

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

Zgodnie z zasadą ograniczenia przechowywania, przetwarzanie danych osobowych jest dopuszczalne tylko tak długo, jak jest to konieczne do osiągnięcia celów przetwarzania danych. Zakazane jest bowiem przechowywanie danych osobowych w nieskończoność. W konsekwencji administratorzy muszą ustalić okresy przechowywania danych lub – gdy ustalenie z góry okresu przechowywania nie jest możliwe – kryteria ustalania takich okresów.

Należy wskazać wyraźnie, że na podstawie art. 5 ust. 1 lit. e) RODO dopuszczalne jest przechowywanie danych osobowych po osiągnięciu pierwotnych celów przetwarzania, pod warunkiem, że dane będą przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych. Przetwarzanie danych w tych celach po upływie pierwotnego okresu przetwarzania wymaga jednak wdrożenia odpowiednich środków technicznych i organizacyjnych w celu ochrony praw i wolności osób, których dane dotyczą.

6. zasada integralności i poufności

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

Powyższa zasada nakłada na podmioty przetwarzające dane osobowe obowiązek odpowiedniego zabezpieczenia danych osobowych, tak aby zachowane zostały właściwości integralności i poufności danych.

7. zasada rozliczalności

Szczegółowego omówienia wymaga także zasada rozliczalności występująca – zdaniem autorki – w ścisłym związku z zasadą minimalizacji danych. Zgodnie z tą zasadą administrator danych jest odpowiedzialny za przestrzeganie reguł przetwarzania danych oraz musi być w stanie wykazać ich przestrzeganie. Konieczne jest zatem wdrożenie odpowiednich wewnętrznych procedur w celu spełniania wymogów RODO oraz stworzenie dokumentacji, dzięki której można wykazać, udowodnić spełnianie tych wymogów.

PODSTAWY PRAWNE I CZYNNOŚCI PRZETWARZANIA

Zgodnie z zasadą zgodności z prawem, przetwarzanie danych osobowych musi być oparte o podstawę prawną wskazaną w RODO. W zależności od rodzaju danych osobowych, zastosowanie mogą mieć różne przesłanki legalizujące przetwarzanie: inne podstawy przetwarzania mają zastosowanie do szczególnych kategorii danych, a inne – do danych zwykłych.

Poniżej wymienione są wszystkie możliwe podstawy prawne przetwarzania danych osobowych.

1. Podstawy prawne przetwarzania tzw. danych zwykłych uregulowane są w art. 6 ust. 1 RODO. Zgodnie z tym przepisem przetwarzanie danych jest legalne, jeżeli spełniony jest co najmniej jeden z poniższych warunków:

1) Osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów. Zgoda taka musi być dobrowolnym, konkretnym, świadomym i jednoznacznym okazaniem woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych (zgodnie z definicją zgody zawartą w art. 4 pkt 11 RODO). Zgoda na przetwarzanie zasadniczo nie powinna być elementem innego dokumentu, np. zapisem nawet odrębnego paragrafu umowy. Zaleca się uzyskanie odrębnego oświadczenia, sformułowanego w ramach odrębnego dokumentu. Jeżeli oświadczenie o zgodzie zawarte jest mimo wszystko w innym dokumencie musi dawać możliwość złożenia odrębnego oświadczenia o wyrażeniu zgody lub jej braku.

2) Przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy. W tym kontekście należy zwrócić szczególną uwagę na kryterium niezbędności danych zawarcia lub wykonania umowy – pojęcie to powinno być interpretowane wąsko. Jeżeli zatem jakaś informacja nie jest potrzebna do zawarcia lub wykonywania umowy, podstawą jej przetwarzania nie może być powyższa przesłanka.

3) Przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze. W tym przypadku podstawa prawna przetwarzania musi być określona w prawie unijnym lub w prawie krajowym, a cel przetwarzania powinien wynikać z tych przepisów.

4) Przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej.

5) Przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi. W tym przypadku podstawa prawna przetwarzania musi być określona w prawie unijnym lub w prawie krajowym, a celem przetwarzania powinno być wykonanie zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej.

6) Przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem. Jeżeli przetwarzanie danych ma być oparte o powyższą przesłankę, konieczne jest przeprowadzenie tzw. testu równowagi, czyli analizy, czy w danej sytuacji interes administratora w przetwarzaniu danych jest nadrzędny wobec interesów, praw i wolności osoby fizycznej.

PODSTAWY PRAWNE I CZYNNOŚCI PRZETWARZANIA

2. Przetwarzanie szczególnych kategorii danych np. danych o stanie zdrowia, danych ujawniających pochodzenie etniczne lub poglądy religijne jest - jak to już wskazano - co do zasady zabronione.

Dla przypomnienia należy wskazać, że przetwarzanie szczególnych kategorii danych dozwolone jest w następujących przypadkach:

1) Osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach.

2) Przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem unijnym lub krajowym, lub porozumieniem zbiorowym na mocy prawa krajowego przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą.

3) Przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody.

4) 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.

5) Przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą.

6) Przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy.

7) Przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa unijnego lub krajowego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.

8) Przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa unijnego lub krajowego lub zgodnie z umową z pracownikiem służby zdrowia i z zastrzeżeniem dodatkowych warunków i zabezpieczeń.

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

10) Przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, na podstawie prawa unijnego lub krajowego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie, konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.

PODSTAWY PRAWNE I CZYNNOŚCI PRZETWARZANIA

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

Prawodawca UE w RODO wskazuje przykładowe rodzaje czynności przetwarzania, takie jak:

- zbieranie danych osobowych – wszelkie działania mające na celu uzyskanie danych osobowych bezpośrednio od osoby, której dane dotyczą (np. poprzez wypełnienie formularza elektronicznego), lub pośrednio (np. przez zakup bazy danych)

- pobieranie danych osobowych – wykonanie kopii danych osobowych na jednym nośniku z innego nośnika, za pośrednictwem sieci telekomunikacyjnej. Może to być np. pobranie danych osobowych z serwera na komputer osobisty.

- przeglądanie danych osobowych – zapoznawanie się z treścią danych osobowych jednej po drugiej.
- wykorzystywanie danych osobowych – użycie danych osobowych do założonego celu.

- ujawnianie danych osobowych przez przesłanie – dowolna forma przekazania danych osobowych innej osobie, np. poprzez wysłanie pocztą, kurierem, e-mailem, przez komunikator internetowy.

- **ujawnianie danych osobowych przez rozpowszechnianie** – zamieszczenie danych osobowych w miejscu publicznym, np. na ogólnie dostępnej stronie internetowej, do której ma dostęp nieograniczona liczba użytkowników; na forum internetowym; na słupie ulicznym.

- ujawnianie danych osobowych przez inne udostępnianie – wszystkie inne czynności niż przesłanie i rozpowszechnianie, np. przekazanie papierowego wykazu, przekazanie pendrive'a z danymi, wyrzucenie na śmietnik dysków zawierających dane osobowe.

- dopasowywanie danych osobowych – czynność polegająca na sprawdzeniu, czy w dwóch różnych zbiorach znajdują się dane osobowe tej samej osoby i czy są one ze sobą spójne.

- łączenie danych osobowych – scalanie danych osobowych jednej osoby, które są zamieszczone w różnych zbiorach, np. danych o aktywności w Internecie, jak również scalanie danych osobowych różnych osób pod względem określonego kryterium.

- ograniczanie przetwarzania danych osobowych – oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania.

- usuwanie danych osobowych – usunięcie treści danych z określonego nośnika bez niszczenia nośnika, czyli np. usunięcie adresu e-mail z bazy newslettera, skasowanie nagrania z kamery.

- niszczenie danych osobowych – fizyczna destrukcja nośnika, na którym znajdują się dane osobowe, np. poprzez spalenie papieru, zniszczenie płyty CD.

CHARAKTERYSTYKA PODMIOTÓW

Ogólne rozporządzenie wyróżnia trzy kategorie podmiotów obowiązanych do ochrony danych osobowych: administrator, współadministrator oraz podmiot przetwarzający.

Zgodnie z art. 4 pkt 7 RODO ”administrator” oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. Dopuszczalne jest również określenie celów i sposobów przetwarzania w prawie Unii lub w prawie państwa członkowskiego. Wtedy administrator może zostać wyznaczony lub mogą zostać określone konkretne kryteria jego wyznaczania w prawie Unii lub w prawie państwa członkowskiego.

Definicja pojęcia „administratora” składa się z trzech elementów:

1) element podmiotowy, czyli adresat przepisu: osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot;

2) sposób działania dopuszczający możliwość współdecydowania o przetwarzaniu danych osobowych: samodzielnie lub wspólnie ustala cele i sposoby przetwarzania;

3) zakres decyzyjny: ustala cele i sposoby przetwarzania.

Zakres podmiotowy pojęcia „administratora” jest szeroki.

Administratorem może być osoba fizyczna, osoba prawna (np. spółka akcyjna lub spółka z ograniczoną odpowiedzialnością, stowarzyszenie, fundacja), organ publiczny, jednostka lub inny podmiot. W zakres tych dwóch ostatnich kategorii mogą wchodzić m.in. jednostki organizacyjne nieposiadające osobowości prawnej takie jak spółka jawna, spółka partnerska, spółka komandytowa lub spółka komandytowo-akcyjna. Podmiot, aby posiadać status administratora nie musi przetwarzać danych osobowych samodzielnie, może dokonać zlecenia przetwarzania podmiotowi przetwarzającymi. O statusie administratora decyduje możliwość ustalania celów i sposobów przetwarzania.

„Współadministrator” jest podkategorią pojęcia „administrator”. „Współadministrator” to osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. Konstrukcję współadministratorów dopuszcza art. 26 ust. 1 RODO, zgodnie z którym „Jeżeli co najmniej dwóch administratorów wspólnie ustala cele i sposoby przetwarzania, są oni współadministratorami”. Ogólne rozporządzenie w ramach współadministrowania nie narzuca sztywnych ram na ustalanie celów i sposobów przez współadministratorów. Współudział może polegać zarówno na ścisłej i skoordynowanej współpracy jak i na częściowym współdziałaniu. Jeżeli strony ustalą, że w ramach prowadzonych przez nich działać dochodzi do współadministrowania, to powinni w sposób przejrzysty uzgodnić zakresy swojej odpowiedzialności dotyczącej wykonywania obowiązków z RODO. Uzgodnienia te powinny dotyczyć w szczególności wykonywania przez osobę, której dane dotyczą jej praw oraz obowiązków współadministratorów co do spełniania obowiązków informacyjnych. Współadministratorzy mogą również utworzyć wspólny punkt kontaktowy dla podmiotów danych.

„Podmiot przetwarzający” oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora.
Chodzi tutaj o sytuację, gdy administrator przekazuje innemu podmiotowi posiadane przez siebie dane osobowe, a podmiot przetwarzający wykonuje pewne operacje na tych danych – na polecenie administratora oraz w zakresie przez niego wskazanym.

CHARAKTERYSTYKA PODMIOTÓW

Przykład:

- zlecenie obsługi kadrowo-płacowej biuru rachunkowemu (biuro rachunkowe przetwarza dane osobowe kontrahentów i pracowników administratora),
- zlecenie obsługi informatycznej firmie IT (firma IT przetwarza np. dane w systemach informatycznych należące do administratora),
- zlecenie przeprowadzenia kampanii mailingowej agencji reklamowej (agencja reklamowa przetwarza np. bazę e-maili klientów administratora).

Jeżeli przetwarzanie ma być dokonywane w imieniu administratora, korzysta on wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi niniejszego rozporządzenia i chroniło prawa osób, których dane dotyczą.
Przetwarzanie przez podmiot przetwarzający odbywa się na podstawie umowy lub innego instrumentu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego i wiążą podmiot przetwarzający i administratora, określają przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora.

Zgodnie z art. 4 pkt 8 RODO ”podmiot przetwarzający” oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora. Tak jak w przypadku pojęcia administratora definicja obejmuje szeroki zakres podmiotów.

W przeciwieństwie do poprzednich regulacji prawnych, w RODO podmiot przetwarzający (zwany również procesorem) jest bezpośrednim adresatem wielu norm zarówno tych określających obowiązki jak i tych regulujących sankcje na naruszenie przepisów o ochronie danych osobowych.

Zgodnie z art. 28 ust. 1 RODO administrator odpowiada za poprawność wyboru podmiotu powierzającego, który zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych spełniających wymogi RODO oraz chroniła prawa podmiotów danych. Na podstawie art. 28 ust. 2 lit a) RODO podmiot przetwarzający może działać wyłącznie na udokumentowane polecenie administratora. Działanie podmiotu powierzającego w imieniu administratora oznacza również, że jest związany celami i sposobami przetwarzania wyznaczonymi przez administratora.

Odniesienie do NGO
Administrator danych osobowych to podmiot, który decyduje o zbieraniu danych osobowych – czyje dane zbiera, w jakim celu. W przypadku organizacji pozarządowych pojęcie administratora danych osobowych odnosi się zazwyczaj do organizacji jako całego podmiotu (stowarzyszenia, fundacji). Nie jest to konkretna osoba fizyczna, która jest odpowiedzialna za przetwarzanie danych w organizacji, tylko cała organizacja.

Podmiot przetwarzający dane osobowe (można też spotkać się z określeniem „procesor”) - to podmiot przetwarzający dane w imieniu administratora (to np. firma ewaluacyjna, która otrzymuje dane beneficjentów projektów od administratora – organizacji, która realizowała projekt). W niektórych projektach organizacje pozarządowe mogą być podmiotami przetwarzającymi dane na zlecenie instytucji zlecającej wykonanie zadania publicznego - wtedy to ta instytucja ustala zakres i cele zbierania danych osobowych (bardzo często tak się dzieje np. przy realizacji projektów dofinansowanych przez PFRON).

OBOWIĄZKI ADMINISTRATORA

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

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

Administrator zobowiązany jest do udzielania osobie, której dane osobowe zostały pozyskane:
- informacji dotyczących między innymi swoich danych kontaktowych,
- danych inspektora danych osobowych,
- celu przetwarzania oraz odbiorcach danych osobowych i kategoriach tychże odbiorców.

OBOWIĄZEK INFORMACYJNY

Jednym z podstawowych obowiązków administratora danych na podstawie RODO jest przekazanie osobom, których dane dotyczą informacji na temat przetwarzania ich danych osobowych.

Na podstawie art. 13 i 14 RODO można wyróżnić dwie sytuacje spełniania obowiązku informacyjnego:
1) kiedy dane zbierane są bezpośrednio od osoby, której dane dotyczą (tę sytuację reguluje art. 13 RODO), oraz
2) kiedy dane zbierane są od podmiotu trzeciego (tę sytuację reguluje art. 14 RODO).

W zależności od sposobu zbierania danych (bezpośrednio czy niebezpośrednio) różnią się:

1) zakres informacji, które należy przekazać osobie, której dane dotyczą;

2) moment przekazania informacji;

3) okoliczności wyłączające obowiązek informacyjny.

Katalog informacji, które należy przekazać osobie, której dane dotyczą będzie szczegółowo omówiony w dalszej części niniejszego podrozdziału. Jeśli chodzi o moment spełnienia obowiązku informacyjnego, jeżeli dane zbierane są bezpośrednio od osoby, której dane dotyczą, administrator musi jej przekazać informacje dotyczące przetwarzania danych w momencie zbierania danych. Natomiast jeżeli dane zbierane są od osoby trzeciej, wówczas zgodnie z art. 14 ust. 3 RODO obowiązek informacyjny powinien być spełniony w rozsądnym terminie po pozyskaniu danych osobowych, biorąc pod uwagę konkretne okoliczności przetwarzania danych osobowych, ale nie później niż w ciągu miesiąca od uzyskania danych. Jeżeli dane osobowe mają być wykorzystane do komunikacji z osobą, której dane dotyczą – wówczas obowiązek informacyjny należy spełnić przy pierwszej komunikacji z osobą, której dane dotyczą, nawet jeżeli nie upłynął jeszcze miesiąc od uzyskania danych. Podobnie, jeżeli administrator planuje ujawnić dane osobowe innemu odbiorcy, obowiązek informacyjny powinien być spełniony najpóźniej przy pierwszym ujawnieniu danych, nawet jeżeli nie upłynął jeszcze miesiąc od uzyskania danych. W przypadku, w którym administrator zbiera dane bezpośrednio od osoby, której dane dotyczą, obowiązek informacyjny jest wyłączony tylko w jednej sytuacji – jeżeli osoba ta już dysponuje wszystkimi informacjami, które mają być jej przekazane na mocy art. 13 ust. 1-2 RODO.

OBOWIĄZEK INFORMACYJNY

Natomiast art. 14 ust. 5 RODO – dotyczący zbierania danych od podmiotu trzeciego – przewiduje cztery sytuacje, w których spełnienie obowiązku informacyjnego nie jest wymagane:

1) osoba, której dane dotyczą, dysponuje już informacjami wymienionymi w art. 14 ust. 1-2 RODO;

2) udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku;

3) pozyskiwanie lub ujawnianie danych osobowych jest wyraźnie uregulowane prawem unijnym lub krajowym, przewidującym odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą;

4) dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianym w prawie unijnym lub krajowym, w tym ustawowym obowiązkiem zachowania tajemnicy.

Poniżej wymienione są elementy obowiązku informacyjnego wraz z krótkim omówieniem niektórych elementów. Wskazane będą też elementy, których zawarcia jest wymagane tylko w przypadku zbierania danych od podmiotów trzecich.

Zgodnie z art. 13 ust. 1-2 i art. 14 ust. 1-2 RODO klauzula informacyjna powinna zawierać:

1) Tożsamość i dane kontaktowe administratora oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe przedstawiciela. Chodzi tutaj o wskazanie imienia i nazwiska lub nazwy administratora danych. Jako dane kontaktowe można podać np. adres siedziby, inny adres korespondencyjny, numer telefonu, adres email, adres strony internetowej.

2) Gdy ma to zastosowanie - dane kontaktowe inspektora ochrony danych. Jeżeli administrator danych wyznaczył inspektora ochrony danych, w klauzuli informacyjnej powinien podać jego dane kontaktowe. Może to być np. adres pocztowy, adres email, numer telefonu. Nie występuje obowiązku podawania imienia i nazwiska IOD w klauzuli informacyjnej.

3) Cele przetwarzania danych osobowych, oraz podstawę prawną przetwarzania. Cele przetwarzania powinny być wyraźne, określone i zgodne z prawem. Należy wskazać wszystkie cele, dla których dane mogą być przetwarzane. Powinno się także wskazać podstawę prawną przetwarzania, przy czym chodzi tylko o te przesłanki legalizujące, które mają zastosowanie w danym przypadku.

4) Kategorie odnośnych danych osobowych. Chodzi tutaj o podanie kategorii danych osobowych, które są przetwarzane. Ten element jest obowiązkowy tylko w sytuacji zbierania danych od podmiotu trzeciego. W takiej sytuacji osoba, której dane dotyczą nie ma bowiem świadomości jakie informacje o niej są przekazywane administratorowi. W przypadku zbierania danych osobowych bezpośrednio od osoby, której dane dotyczą, osoba ta sama przekazuje dane administratorowi, a zatem zdaje sobie sprawę, jaki jest ich zakres.

5) Jeżeli przetwarzanie odbywa się na podstawie prawnie uzasadnionego interesu (art. 6 ust. 1 lit. f) RODO) – prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią. Konieczne jest określenie prawnie uzasadnionego interesu realizowanego przez administratora danych lub stronę trzecią, który to interes w ocenie administratora pozwala na przetwarzanie danych osobowych.

6) Informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją. Należy pamiętać, że w rozumieniu RODO odbiorcami danych są nie tylko inni administratorzy, ale także podmioty przetwarzające dane osobowe w imieniu administratora (np. dostawcy usług IT). Definicja odbiorcy znajduje się w art. 4 pkt 9 RODO.

OBOWIĄZEK INFORMACYJNY

7) Gdy ma to zastosowanie - informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania na podstawie odpowiednich zabezpieczeń (art. 46, art. 47 lub art. 49 ust. 1 akapit drugi RODO), wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii dokumentu zabezpieczeń lub o miejscu udostępnienia danych. Konieczne jest wskazanie państwa trzeciego lub organizacji międzynarodowej, do której będą przekazywane dane osobowe. Należy też podać podstawę prawną transferu, tj. decyzję Komisji Europejskiej w sprawie uznania państwa trzeciego lub organizacji międzynarodowej za zapewniającą odpowiedni stopień ochrony danych, lub tzw. odpowiednie zabezpieczenia. Odpowiednimi zabezpieczeniami mogą być np. standardowe klauzule ochrony danych, wiążące reguły korporacyjne, zatwierdzony kodeks postępowania. Ponadto w klauzuli informacyjnej należy wskazać, w jaki sposób osoba, której dane dotyczą może uzyskać kopię dokumentu zabezpieczeń. Należy zwrócić uwagę, że w tym zakresie w polskim tłumaczeniu RODO znajduje się błąd, bowiem w przepisie art. 13 ust.1 lit f.) RODO oraz art. 14 ust. 1 lit. f) RODO mowa jest o możliwości uzyskania kopii danych lub miejsce udostępnienia danych. Porównanie polskiej wersji językowej RODO do innych wersji językowej (angielskiej, francuskiej) pozwala jednak na ustalenie, że chodzi tutaj o kopię odpowiednich zabezpieczeń lub miejsce udostępnienia zabezpieczeń.

8) Okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu. Jeżeli to możliwe, należy wskazać konkretny okres, przez który dane osobowe będą przetwarzane (np. 5 lat). Jeżeli ustalenie konkretnego okresu przetwarzania nie jest możliwe, należy podać kryteria ustalania okresu przechowywania danych (np. okres przedawnienia roszczeń).

9) Informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych. Informację o prawach przysługujących osobie, której dane dotyczą należy dostosować do okoliczności przetwarzania. W celu zachowania zasady przejrzystości, osobę, której dane dotyczą należy poinformować tylko o tych prawach, które będą miały do niej zastosowanie. Przykładowo, prawo sprzeciwu stosuje się tylko wówczas, gdy podstawą przetwarzania danych jest prawnie uzasadniony interes lub wykonanie zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej. Natomiast z prawa przenoszenia danych można korzystać tylko w sytuacji, gdy dane są przetwarzane w sposób zautomatyzowany.

10) Jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) - informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem. Informację o prawie do wycofania zgody należy zawrzeć tylko w sytuacji, gdy jest ona podstawą prawną przetwarzania danych.

11) Informacje o prawie wniesienia skargi do organu nadzorczego. Aby zapewnić większą przejrzystość informacji, można wskazać nazwę organu nadzorczego, do którego można złożyć skargę związaną z przetwarzaniem danych osobowych.

12) Źródło pochodzenia danych osobowych, a gdy ma to zastosowanie - czy pochodzą one ze źródeł publicznie dostępnych. Informację tę podaje się tylko w przypadku zbierania danych od podmiotów trzecich. Osoba, której dane dotyczą musi być bowiem poinformowana, jaki podmiot przekazał administratorowi jej dane osobowe.

13) Informację, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych. Powyższą informację należy umieścić w klauzuli informacyjnej tylko w przypadku zbierania danych bezpośrednio od osoby, której dane dotyczą. Chodzi o to, aby osoba, której dane dotyczą miała świadomość istnienia obowiązku podania przez nią danych osobowych oraz konsekwencji niepodania danych.

OBOWIĄZEK INFORMACYJNY

14) Informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4, oraz - przynajmniej w tych przypadkach - istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą. Jeżeli dochodzi do zautomatyzowanego podejmowania danych osobowych, w klauzuli informacyjnej należy umieścić o tym szczegółową informację. Chodzi tutaj o m.in. przedmiot decyzji, konsekwencje decyzji, dane wykorzystywane do podjęcia decyzji, sposoby zakwestionowania decyzji.

Najczęstszym sposobem spełniania obowiązku informacyjnego jest sposób pisemny (za pośrednictwem informacji pisemnej), w tym elektronicznie. Dopuszczalne jest także spełnianie obowiązku informacyjnego ustnie.

Szczególnie w przypadku spełniania obowiązku informacyjnego w środowisku elektronicznym rekomenduje się stosowanie „warstwowej" klauzuli informacyjnej. W pierwszej warstwie przedstawione są podstawowe informacje dotyczące przetwarzania w formie skrótowej (np. sama nazwa administratora, krótko określony cel przetwarzania). Natomiast w warstwie szczegółowej podane są szczegółowe informacje dotyczące przetwarzania, zgodnie z treścią art. 13 ust. 1-2 albo art. 14 ust. 1-2 RODO. Dzięki temu osoba, której dane dotyczą może szybko zorientować się, na czym ma polegać przetwarzanie jej danych osobowych – za pomocą warstwy podstawowej. Jednocześnie osoba, której dane dotyczą może zapoznać się z pełną wersja klauzuli informacyjnej, jeżeli chce uzyskać bardziej szczegółowe informacje.

UWZGLĘDNIANIE OCHRONY DANYCH W FAZIE PROJEKTOWANIA (PRIVACY BY DESIGN)

Administrator - zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania, uwzględnia:

• stan wiedzy technicznej,
• koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz
• ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania,
• wdraża odpowiednie środki techniczne i organizacyjne, zaprojektowane w celu skutecznej realizacji zasad ochrony danych oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi RODO oraz chronić prawa osób, których dane dotyczą, takie jak pseudonimizacja czy minimalizacja danych.

Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji przedstawiła propozycję strategii w określaniu procedury privacy by design oraz privacy by default:

1) Minimalizacja danych:
ilość danych osobowych powinna być ograniczona do minimum. Dla każdego projektu administrator powinien oszacować, jakie dane mogą być przetwarzane (pomocne będzie zbudowanie rejestru czynności przetwarzania, aby odpowiedzieć na wiele pytań pomocniczych w tym zakresie).

2) Ukrycie danych:
dane osobowe i ich wzajemne relacje powinny być ukryte przed prostym dostępem nieograniczonego kręgu osób. Należy to rozumieć nie tylko jako wprowadzenie opcji widoku publiczny/prywatny, lecz szerzej, np. przez wdrożenie narzędzi antyśledzących, szyfrowania, pseudonimizacji, maskowania tożsamości, deidentyfikacji, anonimizacji w określonych przypadkach (z pomocą może przyjść ustalenie procesu przy uwzględnieniu potencjalnego naruszenia bezpieczeństwa).

3) Separacja danych:
dane osobowe powinny być przetwarzane w sposób rozproszony (należy rozważyć dostępne technologie i rozwiązania).

PRIVACY BY DESIGN

4) Agregacja danych:
dane osobowe zbiorcze powinny być przetwarzane na najwyższym poziomie agregacji i przy najmniejszych możliwych szczegółach, w których są nadal użyteczne (np. anonimizacja lub pseudonimizacja, w zależności od okoliczności).

5) Przejrzystość przetwarzania:
osoby, których dane dotyczą, powinny być odpowiednio informowane za każdym razem, gdy ich dane są przetwarzane, w jaki sposób dane są przetwarzane (np. widok publiczny/prywatny).

6) Kontrola:
osoby, których dane dotyczą, powinny mieć możliwość wpływania na to, w jaki sposób ich dane są przetwarzane i komu są udostępniane.

7) Egzekwowanie:
polityka prywatności zgodna z wymogami prawnymi powinna być dostępna i egzekwowana (należy w niej opisać mechanizmy ochrony danych, których przestrzega administrator).

8) Zgodność:
administrator musi być w stanie wykazać zgodność z obowiązującą polityką prywatności i wszelkimi obowiązującymi wymogami prawnymi

„Pseudonimizacja" - oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.

BEZPIECZEŃSTWO OCHRONY DANYCH

Oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności ryzyko wiążące się z przetwarzaniem, wynikające z przypadkowego lub niezgodnego z prawem:

- zniszczenia,
- utraty,
- modyfikacji,
- nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
- pseudonimizację i szyfrowanie danych osobowych;
- zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;
- zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;
- regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

NARUSZENIE ZASAD OCHRONY DANYCH

Rozporządzenie ogólne przewiduje obowiązki administratora w przypadku naruszenia ochrony danych osobowych.

Pod pojęciem naruszenia ochrony danych rozumie się: „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" (art. 4 pkt 12 RODO).

NARUSZENIE ZASAD OCHRONY DANYCH

Obowiązki administratora związane z naruszeniami można podzielić na trzy kategorie:

1) zgłaszanie przez administratora naruszenia ochrony danych osobowych organowi nadzorczemu (art. 33 ust.1-4 RODO);
2) dokumentowanie przez administratora naruszeń ochrony danych osobowych (art. 33 ust. 5 RODO);
3) zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych (art. 34 RODO.

Zgłaszanie przez administratora naruszenia ochrony danych osobowych organowi nadzorczemu.

Artykuł 33 ust. 1 RODO przewiduje, że w przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości nie później niż w terminie 72 godzin stwierdzeniu naruszenia – zgłasza je właściwemu organowi nadzorczemu. W przypadku dokonania zgłoszenia po upływie 72 godzin od stwierdzenia naruszenia administrator powinien załączyć wyjaśnienie przyczyn opóźnienia. Zgłoszenie nie jest wymagane, jeżeli jest mało prawdopodobne, że naruszenie skutkowałoby naruszeniem praw lub wolności osób fizycznych, co oznacza że obowiązek zgłaszania naruszeń nie ma charakteru bezwzględnego. Jednakże to na administratorze ciąży obowiązek oceny, czy doszło do naruszenia praw lub wolności osób fizycznych. Jako przykłady sytuacji, w których bez wątpienia dochodzi do takiego naruszenia należy wymienić sytuacje, w których dochodzi do:
1) utrata kontroli nad własnymi danymi,
2) negatywne konsekwencji wizerunkowych,
3) negatywnym odbiorze społecznym związanym z upublicznieniem danych osobowych.

Minimalne wymogi treści zgłoszenia naruszenia ochrony danych osobowych.

Zgodnie z art. 33 ust. 3 RODO zgłoszenie naruszenia ochrony danych osobowych musi co najmniej:

1) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
2) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
3) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
4) opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

W przypadku, gdy nie jest możliwe udzielenie wszystkich wyżej wskazanych informacji w jednym zgłoszeniu, to administrator może przekazywać te dane organowi nadzorczemu sukcesywnie bez zbędnej zwłoki (art. 33 ust. 4 RODO).

Dokumentowanie przez administratora naruszeń ochrony danych osobowych.

Zgodnie z art. 33 ust. 5 RODO przewiduje obowiązek administratora dokumentowania wszelkich naruszeń ochrony danych osobowych, w tych w szczególności okoliczności naruszenia ochrony danych osobowych, jako skutków, oraz podjętych działań zaradczych. Sporządzona dokumentacja musi pozwolić organowi nadzorczemu weryfikację przestrzegania obowiązków z art. 33 RODO. Obowiązek ten jest przejawem zasady rozliczalności z art. 5 ust. 2 RODO.

W praktyce regulacja ta oznacza, że administrator powinien przewidzieć w ramach wewnętrznej procedury dotyczącej zgłaszania naruszeń ochrony danych osobowych organowi nadzorczemu procedurę rejestrowania naruszeń w rejestrze, który spełni określone wyżej wymagania.

Zawiadamianie osoby, której dane dotyczą o naruszeniu ochrony danych osobowych

NARUSZENIE ZASAD OCHRONY DANYCH

Kolejnym obowiązkiem nałożonym na administratora w związku z naruszeniem ochrony danych osobowych jest zawiadomienie osobowy, której dane dotyczą. Zgodnie z art. 34 ust. 1 RODO jeżeli naruszeniem ochrony danych może spowodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu. Konieczność zawiadomienia osoby, której dane dotyczą aktualizuje się, jeżeli zostaną kumulatywnie spełnione dwie przesłanki: zaistnieje ryzyko naruszenia praw lub wolności oraz to ryzyko jest wysokie. Ogólne rozporządzenie nie precyzuje pojęcia „wysokiego ryzyka".

Wymogi co do treści zawiadomienia osoby, której dane dotyczą.

Zawiadomienie skierowane do osoby, której dane dotyczą powinno jasnym i prostym językiem opisywać charakter naruszenia ochrony danych osobowych (art. 33 ust. 2 RODO).

Zawiadomienie osoby, której dane dotyczą musi co najmniej:
1) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
2) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
3) opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

Wyłączenia co do zawiadamiania osoby, której dane dotyczą

Zawiadomienie osoby, której dane dotyczą, nie jest wymagane, jeżeli wystąpi co najmniej jeden z trzech wymienionych przypadków (art. 34 ust. 3 RODO):

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

2) administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą;

3) 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.

W przypadku, gdy administrator nie zawiadomił jeszcze osoby, której dane dotyczą o naruszeniu ochrony danych osobowych, organ nadzorczy może biorąc pod uwagę prawdopodobieństwo że naruszenie spowoduje wysokie ryzyko naruszenia:

1) zażądać zawiadomienia osoby, której dane dotyczą, lub
2) stwierdzić, że został spełniony jeden z warunków wyłączających obowiązek zawiadomienia.

Każdy administrator, w tym organizacja NGO, powinien wdrożyć wewnętrzną procedurę dotyczącą wykrywania, a następnie zgłaszania naruszeń oraz zawiadamiania osób, których dane dotyczą o takim naruszenia. Procedura powinna być dostosowana do wielkości podmiotu.

OCENA SKUTKÓW DLA OCHRONY DANYCH

Ogólne rozporządzenie znosi ogólny obowiązek zawiadamiania organów nadzorczych o przetwarzaniu danych osobowych, który był przewidziany w dyrektywie 95/46/WE. Na gruncie prawa polskiego oznacza to zniesienie obowiązku rejestracji zbiorów danych do organu nadzorczego. Jak wskazano w motywie 89 obowiązek zawiadamiania o przetwarzaniu danych osobowych powodował obciążenia finansowe i administracyjne, a mimo to nie przyczyniał się w oczekiwanym zakresie do poprawy ochrony danych osobowych. W konsekwencji prawodawca unijny uznał, że ogólne obowiązki zawiadamiania należy zastąpić skutecznymi procedurami i mechanizmami, które będą się koncentrować na tych operacjach przetwarzania, które ze względu na swój charakter, zakres, kontekst i cele mogą powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych. Przeprowadzanie oceny skutków dla ochrony danych jest jednym z elementów zarządzania ryzykiem związanym z przetwarzaniem danych. Ocenę skutków należy podzielić na dwa etapy. W pierwszym etapie administrator dokonuje oceny, czy dany rodzaj przetwarzania (w szczególności z użyciem nowych technologii) ze względu na swój zakres kontekst lub cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych (art. 35 ust. 1 RODO). Jeżeli odpowiedź jest twierdząca, to administrator powinien przystąpić do drugiego etapu oceny skutków. Dokonując oceny skutków, administrator jest zobowiązany do podjęcia konsultacji z inspektorem ochrony danych, jeżeli został powołany.

Zakres czynności, które powinny się znaleźć w ocenie skutków został określony w art. 35 ust. 7 RODO:

a) systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez administratora;

b) ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów;

c) ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą,

d) środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie niniejszego rozporządzenia, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy.

Artykuł 35 ust. 3 RODO zawiera przykładowe wyliczenie sytuacji, w których przeprowadzenie skutków dla ochrony danych jest obowiązkowe w przypadku:

a) systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną;

b) przetwarzania na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1, lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10;

c) systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.

Ponadto na podstawie art. 35 ust. 1, art. 35 ust. 3 lit. a-c), motywów 71, 75 oraz 91 preambuły RODO, Grupa Robocza art. 29 wskazała kryteria, które należy brać pod uwagę przy ocenie ryzyka dla naruszenia praw lub wolności osób fizycznych:

OCENA SKUTKÓW DLA OCHRONY DANYCH

1) ocena lub punktacja, w tym profilowanie i przewidywanie, w szczególności dotyczące takich aspektów podmiotu danych jak świadczenie pracy, sytuacja ekonomiczna, zdrowie, osobiste preferencje, zainteresowania, wiarygodność, zachowanie, lokalizacja czy poruszanie się,

2) zautomatyzowane podejmowanie decyzji wywołujące skutki prawne lub wpływające na podmiot danych w podobny sposób,

3) systematyczne monitorowanie mające na celu obserwowanie, monitorowanie lub kontrolowanie podmiotu danych, w tym systematyczne monitorowanie miejsc dostępnie publicznych,

4) przetwarzanie tzw. danych wrażliwych lub przetwarzanie danych o charakterze wysoce osobistym,

5) dane przetwarzane na dużą skalę,

6) przetwarzanie danych osobowych podlegające łączeniu lub dopasowywaniu,

7) dane dotyczące osób wymagających szczególnej opieki, których dane dotyczą,

8) wykorzystanie do przetwarzania danych innowacyjnych rozwiązań technicznych lub organizacyjnych,

9) jeżeli przetwarzanie danych samo w sobie utrudnia podmiotom danych wykonywanie przysługujących im praw lub korzystanie z usługi lub z umowy.

Dokument oceny powinien zawierać ma co najmniej:

1) systematyczny opis planowanych operacji przetwarzania i celów przetwarzania,

2) ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów,

3) ocenę ryzyka naruszenia praw lub wolności osób fizycznych, których dane dotyczą,

4) środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie unijnego rozporządzenia, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy,

Dokonując oceny skutków dla ochrony danych, administrator konsultuje się z inspektorem ochrony danych, jeżeli został on wyznaczony.

Ocena skutków dla ochrony danych jest wymagana w szczególności w przypadku:

1) systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną;

2) przetwarzania na dużą skalę szczególnych kategorii danych osobowych lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa lub

3) systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.

OCENA SKUTKÓW DLA OCHRONY DANYCH

Motyw 75 RODO stanowi, iż ryzyko naruszenia praw lub wolności osób, o różnym prawdopodobieństwie i wadze zagrożeń, może wynikać z przetwarzania danych osobowych mogącego prowadzić do uszczerbku fizycznego lub szkód majątkowych lub niemajątkowych, w szczególności: jeżeli przetwarzanie może skutkować:

1) dyskryminacją;

2) kradzieżą tożsamości lub oszustwem dotyczącym tożsamości;

3) stratą finansową;

4) naruszeniem dobrego imienia;

5) naruszeniem poufności danych osobowych chronionych tajemnicą zawodową;

6) nieuprawnionym odwróceniem pseudonimizacji lub inną znaczną szkodą gospodarczą lub społeczną;

7) pozbawieniem praw i wolności lub możliwości sprawowania kontroli nad danymi osobowymi;

8) ujawnieniem pochodzenia rasowego lub etnicznego, poglądów politycznych, wyznania lub przekonań światopoglądowych, lub przynależności do związków zawodowych;

9) przetwarzanie danych genetycznych, dotyczących zdrowia lub seksualności lub wyroków skazujących i naruszeń prawa lub związanych z tym środków bezpieczeństwa;

10) przetwarzanie, w związku z którym oceniane są czynniki osobowe, w szczególności analizowane lub prognozowane aspekty dotyczące efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się – w celu tworzenia lub wykorzystywania profili osobistych;

11) przetwarzanie danych osób wymagających szczególnej opieki, w szczególności dzieci; jeżeli przetwarzanie dotyczy dużej ilości danych osobowych i wpływa na dużą liczbę osób, których dane dotyczą.

W przypadku analizy ryzyka w zakresie bezpieczeństwa danych osobowych podaje się następujące przykłady podatności na ryzyko:

1) wrażliwość na zmiany temperatury,
2) wrażliwość na zmiany zasilania,
3) brak mechanizmów uwierzytelniania,
4) brak aktualnych poprawek bezpieczeństwa,
5) brak szyfrowania transmisji,
6) brak redundancji sprzętu,
7) praca kontrahentów bez nadzoru,
8) brak kontroli dostępu,
9) brak fizycznej ochrony,
10) brak planów ciągłości,
11) niewykonywanie audytów.

Podmiot będący administratorem powinien dokonywać stałej i systematycznej oceny, czy dany rodzaj przetwarzania ze względu na swój zakres kontekst lub cele podlega obowiązkowi oceny skutków dla ochrony danych osobowych. Przegląd ten winien obejmować wszystkie czynności przetwarzania danych, w szczególności w kontekście planowanych działań.

Kluczowe dla rozstrzygnięcia, czy należy przeprowadzić ocenę skutków, jest pojęcie „dużej skali". Oceniając, czy przetwarzanie odbywa się na „dużą skalę", należy brać pod uwagę takie czynniki jak ilość osób, których przetwarzanie dotyczy, wielkości oraz różnorodności przetwarzanych danych, czasu przetwarzania danych osobowych oraz zasięgu terytorialnego przetwarzania danych. Wydaje się, że z duża skala przetwarzania danych z art. 9 i 10 RODO może wystąpić przykładowo w przypadku dużych organizacji zajmujących się na przykład sprawami medycznymi.

OCENA SKUTKÓW DLA OCHRONY DANYCH

Przetwarzanie danych osobowych nie wystąpi natomiast w przypadku prowadzenia przez organizację działalności na niewielką skalę. Wskazuje na to motyw 91 RODO:

„Przetwarzanie danych osobowych nie powinno zostać uznane za przetwarzanie danych osobowych na dużą skalę, jeżeli dotyczy danych osobowych pacjentów lub klientów i jest dokonywane przez pojedynczego lekarza, innego pracownika służby zdrowia lub prawnika. W takich przypadkach ocena skutków dla ochrony danych nie powinna być obowiązkowa".

Gdy nie jest jasne, czy ocena skutków jest konieczna, zaleca się jej przeprowadzenie.

Jeżeli dochodzi do przetwarzania danych, które wymaga przeprowadzania oceny skutków dla ochrony danych, to dobrą praktyką jest stałe przeprowadzanie przeglądu oceny skutków dla ochrony danych i regularne przeprowadzanie ponownej oceny. Ocena skutków dla ochrony danych to proces ciągły wymagający określenia cykliczności jej wykonywania u administratora przez cały czas trwania danego procesu przetwarzania danych.

Norma ISO/EIC 29134

W 06.2017 r. została opublikowana norma, w której sformułowano wytyczne dla szacowania ryzyka w odniesieniu do oceny skutków. Standard zawiera wskazówki do przeprowadzenia szacowania ryzyka dla prywatności osoby. Określono strukturę i zawartość raportu z przeprowadzenia oceny skutków. Norma może być stosowana w następujących sytuacjach:
1) identyfikacja skutków, ryzyk i odpowiedzialności dotyczących prywatności,
2) dostarczanie wskazówek dla zapewnienia ochrony danych osobowych w fazie projektowania,
3) ograniczanie ryzyka związane z przetwarzaniem danych osobowych w odniesieniu do podstawowych zadań ochrony danych osobowych.

REJESTR CZYNNOŚCI PRZETWARZANIA

Podmioty i instytucje przetwarzające dane wrażliwie, zobowiązane będą do prowadzenia rejestru czynności przetwarzania danych osobowych, który zawierać będzie, w szczególności:

- imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także inspektora ochrony danych,
- cele przetwarzania,
- opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych,
- kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione,
- jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych,
- jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.

Obowiązek prowadzenia rejestru czynności określono w art. 30 RODO:
dla administratora (ust.1)
oraz dla podmiotu przetwarzającego (ust.2).

Celem prowadzenia rejestrów jest przede wszystkim:
1) w przypadku rejestru administratora – identyfikacja czynności przetwarzania, za które administrator jest odpowiedzialny oraz opis podstawowych zagadnień dotyczących tych czynności w celu zapewnienia zgodności z RODO,
2) w przypadku rejestru podmiotu przetwarzającego – identyfikacja administratorów oraz czynności przetwarzania, w związku z którymi nastąpiło powierzenie przetwarzania danych osobowych, wraz z podstawowymi informacjami dotyczącymi tych czynności w celu zapewnienia zgodności z RODO.

Zgodnie z art. 30 ust. 5 RODO obowiązek jest wyłączony w stosunku do przedsiębiorcy lub podmiotu zatrudniającego mniej niż 250 osób, chyba że występuje przynajmniej jedna z trzech wymienionych sytuacji:
1) przetwarzanie, którego dokonują, może powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą,
2) przetwarzanie nie ma charakteru sporadycznego,
3) przetwarzanie obejmuje szczególne kategorie danych osobowych, o których mowa w art. 9 ust. 1 RODO, lub dane osobowe dotyczące wyroków skazujących i naruszeń prawa, o czym mowa w art. 10 RODO.

Rejestry mają formę pisemną, w tym formę elektroniczną. Administrator lub podmiot przetwarzający udostępniają rejestr na żądanie organu nadzorczego.

INSPEKTOR DANYCH OSOBOWYCH

W RODO przewiduje się funkcję inspektora ochrony danych (IOD), która służy wspieraniu administratora (podmiotu przetwarzającego) w wykonywaniu jego obowiązków określonych w RODO. Powyższą funkcję może wykonywać pracownik lub osoba świadczącą usługę na podstawie umowy cywilnoprawnej. W RODO wskazuje się trzy sytuacje, gdy wyznaczenie IOD jest obowiązkowe. W pozostałych sytuacjach wyznaczenie IOD pozostawiono uznaniu administratora (procesora). W szczególności administrator (podmiot przetwarzający) musi to uczynić , gdy:

- główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę; lub

- gdy główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych (określonych w art. 9 lub 10 RODO).

Pojęcie dużej skali przetwarzania danych ustala się w oparciu o następującej kryteria:

- liczby osób, których dane dotyczą (jako konkretnej liczby, bądź jako proporcji odpowiedniej populacji),
- ilości danych lub zakresu różnych kategorii danych, jakie poddawane są przetwarzaniu,
- okresu czy trwałości czynności przetwarzania danych,
- geograficznego zakresu czynności przetwarzania.

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

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

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

c) główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa.

Przez organy i podmioty publiczne zobowiązane do wyznaczenia inspektora ochrony danych rozumiane będą organy oraz podmioty publiczne wskazane w art. 9 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych oraz instytuty badawcze w rozumieniu ustawy z dnia 30 kwietnia 2010 r. o instytutach badawczych.

Obowiązek wyznaczenia inspektora ochrony danych, mają, m.in:

1) organy władzy publicznej, w tym organy administracji rządowej, organy kontroli państwowej i ochrony prawa oraz sądy i trybunały,
2) jednostki samorządu terytorialnego oraz ich związki,
3) samodzielne publiczne zakłady opieki zdrowotnej,
4) uczelnie publiczne,
5) inne państwowe lub samorządowe osoby prawne utworzone na podstawie odrębnych ustaw w celu wykonywania zadań publicznych, z wyłączeniem przedsiębiorstw, instytutów badawczych, banków i spółek prawa handlowego,
6) instytuty badawcze w rozumieniu ustawy z dnia 30 kwietnia 2010 r. o instytutach badawczych.

INSPEKTOR DANYCH OSOBOWYCH

Do zadań IOD należy:

a) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie (art. 39 ust. 1 lit a RODO),

b) monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty (art. 39 ust. 1 lit b RODO),

c) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO (art. 39 ust. 1 lit c RODO),
d) współpraca z organem nadzorczym (art. 39 ust. 1 lit d RODO),

d) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach (art. 39 ust. 1 lit e RODO),

e) pełnienie funkcji punktu kontaktowego wobec osób, których dane dotyczą (art. 38 ust. 4 RODO).

Administracyjne wyznaczenie konkretnej osoby do pełnienia funkcji IOD dokonywane jest oświadczeniem administratora przyjmowanym przez wyznaczonego, przy czym należy ustalić podstawę świadczeń ze strony tej osoby pracowniczą lub cywilnoprawną oraz odpowiednio określić obowiązki IOD w treści umowy z nim. RODO stawia wobec osoby mającej pełnić IOD wymogi posiadania stosownych kwalifikacji. IOD jest wyznaczany na podstawie kwalifikacji zawodowych, w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, które nakłada na niego RODO. W RODO określa się także warunki organizacyjne wykonywania funkcji IOD. Administrator powinien jednocześnie zapewnić, aby IOD był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych, a także wspierać go w wypełnianiu zadań określonych w RODO, zapewniając mu zasoby niezbędne do ich wykonania oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej. **RODO wymaga również, aby IOD miał zapewnioną niezależność wewnątrz jednostki organizacyjnej nie może otrzymywać instrukcji dotyczących wykonywania zadań określonych w RODO, nie może być także odwoływany ani karany przez administratora za wypełnianie swoich zadań, a podlegać ma bezpośrednio kierownikowi jednostki organizacyjnej.** Równocześnie z wyznaczeniem IOD administrator może uszczegółowić jego zadania w organizacji, a to ze względu na użycie w RODO pojęć nieostrych w tym zakresie (np. monitorowanie przestrzegania) , jak również nałożyć inne, dodatkowe zadania nie przewidziane wprost w art. 39 ust.1 RODO (np. prowadzenia rejestru czynności przetwarzania). Jednym z zadań IOD jest pełnienie funkcji punktu kontaktowego dla osób, których dane dotyczą. W ramach tego zadania osoby, których dane dotyczą mogą kontaktować się z IOD we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem przysługujących im praw. W tym zakresie administrator zobowiązany jest do opublikowania danych kontaktowych IOD (np. adres korespondencyjny, dedykowany numer telefony lub adres email przeznaczony tylko do kontaktu z IOD) i przekazania ich organowi nadzorczemu. Wskazuje się, że do celów kontaktu podmiotów danych z IOD, można także stworzyć specjalny formularz kontaktowy na stronie internetowej administratora.

UPRAWNIENIA OSOBY, KTÓREJ DANE DOTYCZĄ

Oprócz prawa do informacji, które zostało omówione powyżej, osobie, której dane dotyczą, przysługują uprawnienia, o których mowa w art. 15-22 RODO. Należą do nich:

• prawo dostępu, w tym prawo do uzyskania kopii danych osobowych podlegających przetwarzaniu (art. 15 RODO);

• prawo do sprostowania lub uzupełnienia danych (art. 16 RODO);

• prawo do usunięcia danych (prawo do bycia zapomnianym) (art. 17 RODO);
• prawo do ograniczenia przetwarzania (art. 18 RODO);

• obowiązek powiadomienia o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania (art. 19 RODO);

• prawo do przenoszenia danych (art. 20 RODO);

• prawo do sprzeciwu (art. 21 RODO);

• prawo do niepodlegania zautomatyzowanej decyzji, w tym profilowaniu (art. 22 RODO).

RODO określa nie tylko rodzaje uprawnień przysługujących osobom, których dane dotyczą, lecz również tryb, w jakim administrator powinien je realizować. Art. 12 RODO wskazuje, w jaki sposób administrator powinien prowadzić komunikację z podmiotami danych oraz wprowadza terminy, w jakich administrator zobowiązany jest do podjęcia działań w odpowiedzi na żądanie podmiotu danych dotyczące przyznanych mu praw.

Przede wszystkim, administrator komunikując się z osobą, której dane dotyczą w zakresie przysługujących jej na mocy art. 15-22 RODO uprawnień, powinien udzielać jej niezbędnych informacji w zwięzłej, przejrzystej i łatwo zrozumiałej formie. Powinien używać jasnego i prostego języka oraz unikać skomplikowanych struktur językowych, tak aby dla osoby, której dane dotyczą, jasny był sens kierowanego do niej komunikatu.

Administrator może udzielić informacji osobie, której dane dotyczą, na piśmie lub w inny sposób, w tym elektronicznie. Na wyraźne żądanie osoby, której dane dotyczą, administrator może udzielić jej informacji ustnie, pod warunkiem, że potwierdzi jej tożsamość w inny sposób tj. nie ustnie. Co do zasady, jeżeli osoba, której dane dotyczą, zgłasza swoje żądanie na podstawie art. 15-22 RODO elektronicznie, to administrator powinien udzielić jej odpowiedzi w tej samej formie, chyba że osoba ta zażąda innej formy. W odpowiedzi na żądanie osoby, której dane dotyczą, administrator powinien bez zbędnej zwłoki – nie później jednak niż w terminie 1 miesiąca od otrzymania żądania – udzielić jej informacji o działaniach podjętych w związku z tym żądaniem. Administrator powinien zatem w terminie 1 miesiąca dokonać oceny zasadności żądania i je zrealizować np. dokonać sprostowania danych lub odmówić realizacji.
Ze względu na skomplikowany charakter żądania lub liczbę żądań, jednomiesięczny termin można wydłużyć o dodatkowe dwa miesiące. Administrator ma zatem maksymalnie 3 miesiące na udzielenie odpowiedzi na żądanie podmiotu danych. Powinien on jednak poinformować osobę, której dane dotyczą, o przedłużeniu terminu i jego przyczynach w ciągu 1 miesiąca od otrzymania żądania. Jeżeli w związku z żądaniem osoby, której dane dotyczą, administrator nie podejmuje żadnych działań, to zobowiązany jest do niezwłocznego najpóźniej w terminie miesiąca od otrzymania żądania poinformowania osoby, której dane dotyczą, o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem.

Jeżeli administrator ma uzasadnione wątpliwości co do tożsamości osoby fizycznej, która zgłasza żądanie na podstawie art. 15–21 RODO, może zażądać od niej dodatkowych informacji niezbędnych do potwierdzenia jej tożsamości.

UPRAWNIENIA OSOBY, KTÓREJ DANE DOTYCZĄ

Co do zasady, komunikacja i działania podejmowana na podstawie art. 15-22 RODO przez administratora są wolne od opłat. Od tej zasady RODO przewiduje dwa wyjątki. Jeżeli żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, administrator może:

• pobrać rozsądną opłatę, uwzględniając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań; albo

• odmówić podjęcia działań w związku z żądaniem.

Ciężar wykazania, że zgłoszone żądanie ma ewidentnie nieuzasadniony lub nadmierny charakter spoczywa na administratorze. Jeżeli administrator zdecydował się odmówić podjęcia działań objętych treścią żądania, powinien wskazać przyczyny takiej decyzji i poinformować o nich osobę, która zgłosiła żądanie.

Administrator może odmówić podjęcia działań w odpowiedzi na żądanie osoby, której dane dotyczą, w dwóch przypadkach:

1. jeśli mają one ewidentnie nieuzasadniony lub nadmierny charakter, lub

2. jeżeli administrator dokonuje przetwarzania niewymagającego identyfikacji i wykaże, iż nie jest w stanie zidentyfikować występującej z takim żądaniem osoby.

Zgodnie z art. 15 RODO, osoba, której dane dotyczą, jest uprawniona do uzyskania od administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do tych danych oraz następujących informacji:

a) cele przetwarzania;

b) kategorie odnośnych danych osobowych;

c) informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;

d) w miarę możliwości planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu;

e) informacje o prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania;

f) informacje o prawie wniesienia skargi do organu nadzorczego;

g) jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle;

h) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą;

i) jeżeli dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej – informacji o odpowiednich zabezpieczeniach, o których mowa w art. 46 RODO, związanych z przekazaniem.

UPRAWNIENIA OSOBY, KTÓREJ DANE DOTYCZĄ

Elementem prawa dostępu jest także również prawo do uzyskania od administratora kopii danych osobowych podlegających przetwarzaniu. Co do zasady, realizacja prawa do uzyskania kopii danych osobowych nie powinna wiązać się z koniecznością ponoszenia opłat przez osobę, której dane dotyczą. Niemniej jednak, administrator może pobrać opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych za wszelkie kolejne kopie, o które zwróci się podmiot danych. Realizując prawo dostępu do danych osobowych, osoba, której dane dotyczą, może uzyskać kopię danych osobowych we wskazanym przez siebie formacie. Jeżeli jednak zwróci się ona o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, administrator udziela informacji powszechnie stosowaną drogą elektroniczną. Prawo do uzyskania kopii nie może jednak niekorzystnie wpływać na prawa i wolności innych.

W zakresie danych osobowych przetwarzanych w związku z funkcjonowaniem NGO będących administratorami są zobowiązani do realizacji uprawnień osoby, której dane dotyczą, wskazanych w art. 15 RODO.

Wykonanie obowiązku
W odniesieniu do danych osobowych przetwarzanych w związku z funkcjonowaniem NGO, w zależności od zakresu żądania osoby, której dane dotyczą, organizacja jako administrator danych zobowiązany jest do:

• udzielenia osobie, której dane dotyczą, informacji, czy przetwarzane są jej dane osobowe, a także innych informacji wskazanych w art. 15 ust. 1-2 RODO;
• udzielenia tej osobie dostępu do tych danych;
• dostarczenia tej osobie kopii danych osobowych podlegających przetwarzaniu.

W zakresie prawa do uzyskania kopii, organizacja powinna zweryfikować czy realizacja tego uprawnienia nie będzie niekorzystnie wpływać na prawa i wolności innych osób i na tej podstawie zdecydować o realizacji albo odmowie realizacji tego prawa.
Jeżeli organizacja nie przetwarza danych osobowych osoby, która zgłasza żądanie, musi ją o tym poinformować tj. nie może pozostawić jej żądania bez odpowiedzi.

Zgodnie z art. 16 RODO, osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe. Z uwzględnieniem celów przetwarzania, osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.

Przepis ten przyznaje zatem osobie, której dane dotyczą, dwa typy uprawnień:

1) uprawnienie do sprostowania nieprawidłowych danych osobowych,

2) uprawnienie do uzupełnienia niekompletnych danych osobowych.

Związany z omawianym uprawnieniem obowiązek administratora nie ma charakteru bezwzględnego - administrator w określonych sytuacjach może odmówić sprostowania danych. Dla przykładu, stosownie do art. 11 ust. 2 RODO administrator nie musi realizować żądania sprostowania, jeżeli może wykazać, że nie jest w stanie zidentyfikować osoby, której dane dotyczą, a która zgłasza żądanie. W takiej sytuacji art. 16 RODO nie znajdzie zastosowania, chyba że osoba, której dane dotyczą, w celu wykonania przysługującego jej prawa dostarczy dodatkowe informacje, które pozwolą ją zidentyfikować.

UPRAWNIENIA OSOBY, KTÓREJ DANE DOTYCZĄ

W zakresie danych osobowych przetwarzanych w związku z funkcjonowaniem organizacji NGO będących administratorami są one zobowiązane do sprostowania lub uzupełnienia danych osobowych na żądanie osoby, której dane dotyczą.

Jeżeli żądanie osoby, której dane dotyczą, obejmuje:

• dane osobowe przetwarzane w związku z funkcjonowaniem organizacji, jak również

• dane osobowe przetwarzane w ramach wykonywania działalności lub czynności, dla których przepisy szczególne nie przewidują odrębnego trybu sprostowania, a żądanie to jest uzasadnione, organizacja jako administrator danych musi sprostować lub uzupełnić dane objęte żądaniem i poinformować o tym osobę, która wniosła żądanie. Jeżeli natomiast żądanie osoby, której dane dotyczą, jest nieuzasadnione, należy poinformować o tym osobę, która wniosła żądanie i wskazać przyczyny odmowy jego realizacji.

Art. 17 RODO przyznaje osobie, której dane dotyczą, prawo żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, tzw. prawo do bycia zapomnianym. Administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe objęte żądaniem, jeżeli:

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 na mocy art. 21 ust. 1 RODO sprzeciw wobec przetwarzania danych osobowych jej dotyczących i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania lub wnosi sprzeciw wobec przetwarzania danych osobowych jej dotyczących na potrzeby marketingu bezpośredniego zgodnie z art. 21 ust. 2 RODO;

d) dane osobowe były przetwarzane niezgodnie z prawem;

e) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w przepisach prawa, którym podlega administrator;

f) dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego, o których mowa w art. 8 ust. 1 RODO.

Jeżeli administrator upublicznił dane osobowe (np. opublikował je na ogólnodostępnej stronie internetowej), a na mocy art. 17 RODO ma obowiązek je usunąć, to zobowiązany jest do podjęcia rozsądnych działań, aby 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. Obowiązek powiadomienia dotyczy przy tym nie tylko osób trzecich, którym dane zostały ujawnione przez administratora, ale także administratorów, którzy uzyskali dane w inny sposób.

Zgodnie z art. 17 ust 3 RODO, powyższe obowiązki są wyłączone 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 przepisów prawa, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;

UPRAWNIENIA OSOBY, KTÓREJ DANE DOTYCZĄ

c) z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego zgodnie z art. 9 ust. 2 lit. h) oraz i) i art. 9 ust. 3 RODO;

d) do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1 RODO, o ile prawdopodobne jest, że prawo, o którym mowa w ust. 1, uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania; lub

e) do ustalenia, dochodzenia lub obrony roszczeń.

Na mocy art. 18 RODO, osoba, której dane dotyczą, ma prawo żądania od administratora ograniczenia przetwarzania, jeżeli:

a) kwestionuje prawidłowość danych osobowych – na okres pozwalający administratorowi sprawdzić prawidłowość tych danych;

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

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

d) osoba, której dane dotyczą, wniosła sprzeciw na mocy art. 21 ust. 1 RODO wobec przetwarzania – do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie administratora są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.

Zgodnie z art. 4 pkt 3 RODO, przez ograniczenie przetwarzania należy rozumieć oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania. Sprowadza się to do tego, że jeżeli przetwarzanie zostało ograniczone to administrator nie może dokonywać na danych innych operacji niż przechowywanie.

Dane osobowe mogą być w takim przypadku przetwarzana 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.

W przypadku ograniczenia przetwarzania, dane osobowe nie mogą być przetwarzane w celu, dla którego dane zostały zebrane.
Przed uchyleniem ograniczenia przetwarzania administrator zobowiązany jest do poinformowania o tym osobę, która zgłosiła żądanie ograniczenia przetwarzania.

W zakresie danych osobowych przetwarzanych w związku z funkcjonowaniem organizacji będących administratorami są one zobowiązane do ograniczenia przetwarzania danych na żądanie osoby, której dane dotyczą.

Na mocy art. 19 RODO, jeżeli administrator dokona, na żądanie osoby, której dane dotyczą:
- sprostowania nieprawidłowych danych osobowych,
- uzupełnienia niekompletnych danych osobowych,
- usunięcia danych osobowych, lub
- ograniczenia przetwarzania danych osobowych,

zobowiązany jest do poinformowania każdego odbiorcy, któremu ujawniono dane osobowe, o dokonanej zmianie.

UPRAWNIENIA OSOBY, KTÓREJ DANE DOTYCZĄ

Przez odbiorcę danych rozumie się przy tym osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią (w tym podmiot przetwarzający lub inny administrator, któremu udostępniono dane osobowe). Odbiorcami danych nie są natomiast organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania na mocy przepisów prawa (np. sąd). Obowiązek ten skorelowany jest z innym obowiązkiem administratora wyrażonym w art. 5 ust. 1 lit. d RODO, tj. zapewnieniem prawidłowości przetwarzanych danych osobowych, w tym również w zakresie, w jakim dane te zostały ujawnione odbiorcom. Stąd jeżeli treść lub zakres danych osobowych przetwarzanych przez administratora ulega zmianie, powinien o tym wiedzieć również odbiorca tych danych osobowych. Obowiązek ten nie znajdzie jednak zastosowania, jeżeli powiadomienie okaże się niemożliwe lub będzie wymagać od administratora niewspółmiernie dużego wysiłku. Warto jednak pamiętać, że ciężar wykazania, że powiadomienie odbiorców jest niemożliwe lub wymaga niewspółmiernie dużego wysiłku obciąża administratora. Jednocześnie administrator zobowiązany jest również do poinformowania osoby, której dane dotyczą, o tych odbiorcach, jeżeli tego zażąda.

W zakresie danych osobowych przetwarzanych w związku z funkcjonowaniem organizacje NGO jako administratorzy danych są zobowiązane do realizacji obowiązku z art. 19 RODO, w następstwie dokonania sprostowania, usunięcia lub ograniczenia przetwarzania zgodnie z art. 16, art. 17 oraz art. 18 RODO.

Art. 20 RODO przyznaje osobie, której dane dotyczą, prawo do otrzymania w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła administratorowi, oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe.

Prawo to znajduje zastosowanie wyłącznie jeżeli:
a) przetwarzanie odbywa się na podstawie zgody lub na podstawie umowy oraz
b) przetwarzanie odbywa się w sposób zautomatyzowany.

Wykonując prawo do przenoszenia danych, osoba, której dane dotyczą, ma prawo żądania, by dane osobowe zostały przesłane przez administratora bezpośrednio innemu administratorowi, o ile jest to technicznie możliwe. Prawo do przenoszenia danych nie może jednocześnie niekorzystnie wpływać na prawa i wolności innych osób. Wykonanie prawa do przenoszenia danych, pozostaje bez uszczerbku dla prawa do usunięcia danych, o którym mowa w art. 17 RODO.

Prawo do przenoszenia danych nie znajdzie zastosowania do przetwarzania, które jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.

Organizacja NGO jako administrator danych osobowych jest zobowiązana do realizacji prawa do przenoszenia danych jedynie w sytuacji, gdy przetwarza dane osobowe na podstawie zgody lub umowy z osobą, której dane dotyczą i wyłącznie pod warunkiem, że przetwarzanie to odbywa się w sposób zautomatyzowany.

Jeżeli jednak obie przesłanki zostaną spełnione administrator danych będzie zobowiązany do realizacji prawa do przenoszenia danych, powinien on, w zależności od żądania osoby, której dane dotyczą:

- przekazać tej osobie w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego, dane osobowe jej dotyczące, jednak wyłącznie te, które sama dostarczyła administratorowi;
- przesłać te dane bezpośrednio innemu administratorowi, wskazanemu przez osobę której dane dotyczą, o ile będzie to technicznie możliwe.

UPRAWNIENIA OSOBY, KTÓREJ DANE DOTYCZĄ

Art. 21 RODO przyznaje osobie, której dane dotyczą, uprawnienie do wniesienia sprzeciwu wobec przetwarzania jej danych osobowych. Osoba, której dane dotyczą, może wnieść sprzeciw:

1) wobec przetwarzania danych osobowych, w tym profilowania, którego podstawą prawną jest:

a) niezbędność przetwarzania do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi bądź

b) niezbędność przetwarzania do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z przyczyn związanych z jej szczególną sytuacją. W razie wniesienia sprzeciwu, administrator nie może już przetwarzać tych danych osobowych, chyba że wykaże on istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.

2) wobec przetwarzania danych osobowych na potrzeby marketingu bezpośredniego, w tym profilowania, w dowolnym momencie, w zakresie, w jakim przetwarzanie jest związane z takim marketingiem bezpośrednim. Jeżeli osoba, której dane dotyczą, wniesie sprzeciw wobec przetwarzania do celów marketingu bezpośredniego, danych osobowych administrator nie może dalej przetwarzać ich do takich celów.

3) wobec przetwarzania danych osobowych do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1 RODO, z przyczyn związanych z jej szczególną sytuacją, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.

Skorzystanie przez osobę, której dane dotyczą, z prawa do sprzeciwu co do zasady uniemożliwia przetwarzanie danych o osobie, której dane dotyczą.

W przypadku sprzeciwu wobec przetwarzania danych osobowych do celów marketingu bezpośredniego, w tym związanego z nim profilowania, administrator zobowiązany jest bezwzględnie do zaprzestania przetwarzania danych objętych sprzeciwem w celach marketingowych (art. 21 ust. 2 RODO). W pozostałych sytuacjach administrator (art. 21 ust. 1 RODO) może wykazać istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, które są nadrzędne wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń (dochodzi zatem do ważenia podstaw do przetwarzania, na które powołuje się administrator, z interesami, prawami i wolnościami osoby, której dane dotyczą). Najpóźniej przy okazji pierwszej komunikacji z osobą, której dane dotyczą, administrator wyraźnie informuje się ją o prawie do sprzeciwu, oraz przedstawia je jasno i odrębnie od wszelkich innych informacji.

Osoba, której dane dotyczą, może wykonać prawo do sprzeciwu za pośrednictwem zautomatyzowanych środków wykorzystujących specyfikacje techniczne.

W odniesieniu do danych osobowych przetwarzanych w związku z funkcjonowaniem organizacji, jeżeli osoba, której dane dotyczą, zgłosiła sprzeciw na zasadach wskazanych w art. 21 ust. 2 RODO, organizacja jako administrator musi bezwzględnie zaprzestać przetwarzania danych osobowych objętych żądaniem. W przypadkach pozostałych sprzeciwów, może albo uczynić zadość żądaniu i zaprzestać przetwarzania danych osoby zgłaszającej żądanie, albo dalej przetwarzać przedmiotowe dane osobowe, jeżeli stwierdzi i jest w stanie wykazać, że istnieją ważne prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstawy do ustalenia, dochodzenia lub obrony roszczeń.

UPRAWNIENIA OSOBY, KTÓREJ DANE DOTYCZĄ

Stosownie do art. 22 RODO, osoba, której dane dotyczą, ma prawo do tego, by nie podlegać decyzji, która:

• opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, oraz

• wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa.

Uprawnienie to nie znajdzie zastosowanie, jeżeli ta decyzja:

a) jest niezbędna do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a administratorem;

b) jest dozwolona prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator i które przewiduje właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą; lub

c) opiera się na wyraźnej zgodzie osoby, której dane dotyczą.

W przypadku, gdy decyzja jest niezbędna do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a administratorem lub gdy opiera się ona na wyraźnej zgodzie osoby, której dane dotyczą, administrator zobowiązany jest do wdrożenia właściwych środków ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą, a co najmniej prawa do uzyskania interwencji ludzkiej ze strony administratora, do wyrażenia własnego stanowiska i do zakwestionowania tej decyzji.

W przypadku szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1, RODO przewiduje generalny zakaz podejmowania zautomatyzowanych decyzji w oparciu o takie dane. Niemniej jednak dozwolone jest zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach w oparciu o szczególne kategorie danych, pod warunkiem że istnieją właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą, a przetwarzanie takich danych odbywa się na podstawie art. 9 ust. 1 lit. a RODO (wyraźna zgoda osoby, której dane dotyczą) lub art. 9 ust. 2 lit. g RODO przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym.

ŚRODKI OCHRONY PRAWNEJ

Za naruszenie przepisów o ochronie danych osobowych należy rozumieć naruszenie przepisów RODO, jak również aktów delegowanych i wykonawczych przyjętych na mocy Rozporządzenia oraz prawa państwa członkowskiego UE doprecyzowującego RODO.

W przepisach RODO prawodawca unijny przewiduje dwa rodzaje odpowiedzialności za naruszenie przepisów o ochronie danych osobowych:

• odpowiedzialność administracyjnej (art.77, 78, 83) oraz

• odpowiedzialność cywilnoprawnej (art.79,82).

Niezależnie od powyższych zasad odpowiedzialności, w RODO dopuszczono również wprowadzenie w porządkach krajowych państw członkowskich – sankcji karnych (art.84 RODO). Z możliwości takiej skorzystał polski ustawodawca w PrUODO).

Przepisy RODO nie określają zasad proceduralnych w postępowaniach dotyczących poszczególnych rodzajów odpowiedzialności, pozostawiając w tym zakresie swobodę ustawodawcy krajowemu.

Wszystkie potencjalne możliwości dochodzenia odpowiedzialności za naruszenie przepisów o ochronie danych osobowych, w tym ich podstawy materialnoprawne oraz proceduralne możliwości zostały przedstawione w formie graficznej w podsumowaniu (punkt VI poniżej).

Postępowanie administracyjne w sprawie naruszenia przepisów o ochronie danych osobowych, zwane dalej ”postępowaniem”, jest prowadzone przez PUODO (art. 61 PrUODO). W postępowaniu tym stosują się – subsydiarnie - przepisy kodeksu postępowania administracyjnego, które znajdują zastosowanie w sprawach nieuregulowanych w uodo (art. 8 ust. 1 PrUODO).

Postępowanie przed PUODO może zostać wszczęte z urzędu lub w wyniku skargi podmiotu danych (osoby, której dane dotyczą). Szczególne uprawnienia przyznano organizacji społecznej, o której mowa w art. 31 § l ustawy z dnia 14 czerwca 1960 r. - Kodeks postępowania administracyjnego i która może występować w postępowaniu za zgodą osoby, której dane dotyczą, działając w jej imieniu i na jej rzecz (art.62 PrUODO).

Jeżeli w toku postępowania zostanie uprawdopodobnione, że przetwarzanie danych osobowych narusza przepisy o ochronie danych osobowych, a dalsze ich przetwarzanie może spowodować poważne i trudne do usunięcia skutki, PUODO, w celu zapobieżenia tym skutkom, może, w drodze postanowienia, zobowiązać podmiot, któremu jest zarzucane naruszenie przepisów o ochronie danych osobowych, do ograniczenia przetwarzania danych osobowych wskazując dopuszczalny zakres tego przetwarzania (art.71 ust.1 PrUODO). W postanowieniu, Prezes Urzędu określa termin obowiązywania ograniczenia przetwarzania danych osobowych nie dłuższy niż do dnia wydania decyzji kończącej postępowanie w sprawie, a na orzeczenie to przysługuje skarga do sądu administracyjnego (art.71 ust.2 PrUODO).

W art.8 ust.2 PrUODO przesądzono, że postępowanie przed PUODO jest postępowaniem jednoinstancyjnym. a wydane w jego toku rozstrzygnięcia mają podlegać zaskarżeniu w toku dwuinstancyjnego postępowania sądowoadministracyjnego. W przypadku decyzji o nałożeniu administracyjnej kary pieniężnej wniesienie skargi do sądu administracyjnego skutkować ma wstrzymaniem jej wykonania (art. 75 PrUODO natomiast w stosunku do decyzji przewidujących inne środki prawne, konieczne jest złożenie – do PUODO lub sądu administracyjnego – wniosku o wstrzymanie decyzji.

ŚRODKI OCHRONY PRAWNEJ

Z odpowiedzialnością administracyjną administratora lub podmiotu przetwarzającego składają się następujące środki prawne przewidziane w RODO:

a) prawo wniesienia skargi do organu nadzorczego (art. 77 RODO),
b) uprawnienia naprawcze organu nadzorczego (art. 58 ust. 2 RODO),
c) administracyjne kary pieniężne (art. 83 RODO).

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

Zgodnie z RODO, bez uszczerbku dla innych administracyjnych lub sądowych środków ochrony prawnej, w przypadku naruszenia ochrony danych osobowych, osoba której dane dotyczą, ma prawo zwykłego pobytu, swojego miejsca pracy lub miejsca popełnienia domniemanego naruszenia (art.77 ust.1).

Rozpatrywanie skarg złożonych przez podmioty uprawnione należy do kompetencji, a jednocześnie do obowiązków organu nadzorczego (art. 57 ust. 1 lit. f RODO).
Rozpatrując skargę, organ nadzorczy może podjąć działania naprawcze, określone w art.58 ust.2 lit.a-h oraz j), jak również nałożyć kary pieniężne (art.83).
Warto wskazać, że zgodnie z art. 83 ust. 2 zd. 1 RODO administracyjne kary pieniężne mogą być stosowane oprócz lub zamiast środków, o których mowa w art. 58 ust. 2 lit. a–h oraz j) RODO. Organ nadzorczy może więc zastosować kary pieniężne oprócz lub zamiast środków prawnych, które stanowią odzwierciedlenie tzw. uprawnień naprawczych organów nadzorczych (art. 58 ust. 2 lit. a–h i lit. j RODO). Wynika to między innymi z motywu nr 150 RODO, zgodnie z którym nałożenie administracyjnej kary pieniężnej lub wydanie ostrzeżenia nie wpływa na stosowanie innych uprawnień organów nadzorczych ani innych sankcji na mocy RODO.

Przepisy RODO przewidują możliwość korzystania przez organy kontrolne z uprawnień naprawczych, które stanowią rodzaj sankcji administracyjnych. Warto w związku z tym podkreślić, że RODO rozszerza zakres uprawnień naprawczych organu nadzorczego, w porównaniu do obecnie przysługujących GIODO na gruncie ustawy o ochronie danych osobowych (art. 18 uodo).

Zgodnie art. 58 ust. 2 RODO, organowi nadzorczemu przysługiwać będą następujące uprawnienia naprawcze:
a) wydawanie ostrzeżeń administratorowi lub podmiotowi przetwarzającemu dotyczących możliwości naruszenia przepisów RODO poprzez planowane operacje przetwarzania;
b) udzielanie upomnień administratorowi lub podmiotowi przetwarzającemu w przypadku naruszenia przepisów RODO przez operacje przetwarzania;
c) nakazanie administratorowi lub podmiotowi przetwarzającemu spełnienia żądania osoby, której dane dotyczą, wynikającego z praw przysługujących jej na mocy niniejszego rozporządzenia;
d) nakazanie administratorowi lub podmiotowi przetwarzającemu dostosowania operacji przetwarzania do przepisów niniejszego rozporządzenia, a w stosownych przypadkach wskazanie sposobu i terminu;
e) nakazanie administratorowi zawiadomienia osoby, której dane dotyczą, o naruszeniu ochrony danych;
f) wprowadzanie czasowego lub całkowitego ograniczenia przetwarzania, w tym zakazu przetwarzania;
g) nakazanie na mocy art. 16, 17 i 18 RODO sprostowania lub usunięcia danych osobowych lub ograniczenia ich przetwarzania oraz nakazanie na mocy art. 17 ust. 2 i art. 19 RODO powiadomienia o tych czynnościach odbiorców, którym dane osobowe ujawniono;
h) cofnięcie certyfikacji lub nakazanie podmiotowi certyfikującemu cofnięcia certyfikacji udzielonej na mocy art. 42 lub 43 RODO, lub nakazanie podmiotowi certyfikującemu nieudzielania certyfikacji, jeżeli jej wymogi nie są spełnione lub przestały być spełniane;
i) zastosowanie, oprócz lub zamiast środków, o których mowa w art. 58 ust. 2 RODO, administracyjnej kary pieniężnej na mocy art. 83 RODO, zależnie od okoliczności konkretnej sprawy;
j) nakazanie zawieszenia przepływu danych do odbiorcy w państwie trzecim lub do organizacji międzynarodowej.

KARY PIENIĘŻNE

Nieprzestrzeganie nakazu orzeczonego przez organ nadzorczy na podstawie art. 58 ust. 2 RODO podlega zgodnie z art. 83 ust. 6 RODO administracyjnej karze pieniężnej w wysokości do 20 000 000 EUR, a w przypadku przedsiębiorstwa – w wysokości do 4 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa. Jest to tzw. niesamoistna kara pieniężna, którą odróżnić należy od kar pieniężnych niesamoistnych.

Jedną z najistotniejszych zmian, które przyniosła europejska reforma prawa ochrony danych, jest wprowadzenie do katalogu sankcji z tytułu naruszenia przepisów o ochronie danych osobowych administracyjnej kary pieniężnej nakładanej w każdym państwie członkowskim przez organy nadzorcze zgodnie z art. 83 RODO. Przepis art. 83 RODO określa przesłanki zastosowania administracyjnej kary pieniężnej, wyznacza jej wysokość oraz wskazuje wpływające na nią okoliczności. Warto wskazać, że do elementów, które pośrednio będą oddziaływać na proces miarkowania wysokości administracyjnej kary pieniężnej, należą wytyczne, które w tym przedmiocie wydawać będzie Europejska Rada Ochrony Danych (art. 70 ust. 1 lit. k RODO).

W artykule 83 ust. 2 RODO zawarty jest katalog okoliczności, które organ nadzorczy musi uwzględnić rozstrzygając o nałożeniu sankcji administracyjnej, a także określając jej wysokość.

Okoliczności wskazane w tym przepisie można podzielić na te dotyczące:

1) działań lub zaniechań podmiotu w ramach tej konkretnej sprawy i ich skutków dla osób poszkodowanych (lit. a–d, k), czyli:
a) charakteru, wagi i czasu trwania naruszenia przy uwzględnieniu charakteru, zakresu lub celu danego przetwarzania, liczby poszkodowanych osób, których dane dotyczą, oraz rozmiaru poniesionej przez nie szkody,
b) umyślnego lub nieumyślnego charakteru naruszenia,
c) działań podjętych przez administratora lub podmiot przetwarzający w celu zminimalizowania szkody poniesionej przez osoby, których dane dotyczą,
d) stopnia odpowiedzialności administratora lub podmiotu przetwarzającego z uwzględnieniem środków technicznych i organizacyjnych wdrożonych przez nich na mocy art. 25 i 32 RODO,
e) wszelkich innych obciążających lub łagodzących czynników mających zastosowanie do okoliczności sprawy, takich jak osiągnięte bezpośrednio lub pośrednio w związku z naruszeniem korzyści finansowe lub uniknięte straty,

2) kategorii naruszonych danych osobowych (lit. g);

3) współpracy z organem nadzorczym w ramach tej konkretnej sprawy (lit. f, i), tj.:
a) stopnia współpracy z organem nadzorczym w celu usunięcia naruszenia oraz złagodzenia jego ewentualnych negatywnych skutków,
b) jeżeli wobec administratora lub podmiotu przetwarzającego, których sprawa dotyczy, zostały wcześniej zastosowane w tej samej sprawie środki, o których mowa w art. 58 ust. 2 RODO– przestrzegania tych środków;

4) uprzedniej działalności podmiotu (lit. e, h, j), czyli:
a) wszelkich stosownych wcześniejszych naruszeń ze strony administratora lub podmiotu przetwarzającego,
b) sposobu, w jaki organ nadzorczy dowiedział się o naruszeniu, w szczególności, czy i w jakim zakresie administrator lub podmiot przetwarzający zgłosili naruszenie,
c) stosowania zatwierdzonych kodeksów postępowania na mocy art. 40 RODO lub zatwierdzonych mechanizmów certyfikacji na mocy art. 42 RODO.

KARY PIENIĘŻNE

Należy podkreślić, że wskazany powyżej katalog nie ma charakteru zamkniętego, gdyż art. 83 ust. 2 lit. k RODO nakazuje w analizowanym procesie uwzględnić wszelkie inne obciążające lub łagodzące czynniki mające zastosowanie do okoliczności sprawy, wskazując dla przykładu korzyści finansowe osiągnięte bezpośrednio lub pośrednio w związku z naruszeniem lub uniknięte straty.

Odnosząc się do okoliczności decydujących o wysokości administracyjnej kary pieniężnej, odwołać się także należy do dyrektywy skuteczności, proporcjonalności i odstraszającego charakteru sankcji, której adresatem jest organ nadzorczy. Zgodnie z art. 83 ust. 1 RODO, organ nadzorczy zapewnia bowiem, aby administracyjne kary pieniężne były w każdym indywidualnym przypadku skuteczne, proporcjonalne i odstraszające.

W art. 83 RODO przewidziano trzy rodzaje kar pieniężnych i dwa pułapy ich wysokości, z czego dwa rodzaje (wyższa i niższa) mają charakter samoistny, a ich maksymalna wysokość jest zależna od rodzaju stwierdzonego przez organ naruszenia oraz charakteru podmiotu, wobec którego ma być ona zastosowana, a trzeci rodzaj – jest następczy w stosunku do uprzednio już zastosowanego przez organ środka prawnego z art. 58 ust. 2 RODO (charakterem jest więc zbliżony do obowiązującej na gruncie UODO grzywny w celu przymuszenia, gdyż dotyczy egzekwowania obowiązków o charakterze niepieniężnym).

Na gruncieRODO możemy zatem wyróżnić:

1) karę samoistną niższą (art. 83 ust. 4 RODO),
2) karę samoistną wyższą (art. 83 ust. 5 RODO).
3) karę niesamoistną (art. 83 ust. 6).

Administracyjnej karze pieniężnej w wysokości do 10 000 000 EUR, a w przypadku przedsiębiorstwa - w wysokości do 2 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa, podlegają naruszenia przepisów, o których mowa w art. 83 ust. 4 RODO, tj.:
a) obowiązków administratora i podmiotu przetwarzającego, o których mowa w art. 8, 11, 25-39 oraz 42 i 43 RODO;
b) obowiązków podmiotu certyfikującego, o których mowa w art. 42 oraz 43 RODO;
c) obowiązków podmiotu monitorującego, o których mowa w art. 41 ust. 4 RODO;
Z treści tego przepisu wynika, że kara niższa może zostać nałożona na: (1) administratora, (2) podmiot przetwarzający, (3) podmiot certyfikujący, (4) podmiot monitorujący.

Administracyjnej karze pieniężnej w wysokości do 20 000 000 EUR, a w przypadku przedsiębiorstwa - w wysokości do 4 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa, podlegają naruszenia przepisów, o których mowa w art. 83 ust. 5 RODO, tj.:
a) podstawowych zasad przetwarzania, w tym warunków zgody, o których to zasadach i warunkach mowa w art. 5, 6, 7 oraz 9 RODO;
b) praw osób, których dane dotyczą, o których mowa w art. 12–22 RODO;
c) przekazywania danych osobowych odbiorcy w państwie trzecim lub organizacji międzynarodowej, o którym to przekazywaniu mowa w art. 44–49 RODO;
d) wszelkich obowiązków wynikających z prawa państwa członkowskiego przyjętego na podstawie rozdziału IX RODO;
e) nieprzestrzegania nakazu, tymczasowego lub ostatecznego ograniczenia przetwarzania lub zawieszenia przepływu danych orzeczonego przez organ nadzorczy na podstawie art. 58 ust. 2 lub niezapewnienia dostępu skutkującego naruszeniem art. 58 ust. 1 RODO.

Administracyjna kara pieniężna w wyższej wysokości może zostać nałożona na:
1) administratora,
2) podmiot przetwarzający,
3) współadministratora,
4) przedstawicieli.

KARY PIENIĘŻNE

Kara ta może być nałożona przez organ nadzorczy w przypadku stwierdzenia, że administrator lub podmiot przetwarzający nie wykonał nakazów z art. 58 ust. 2 RODO. W takim przypadku organ nadzorczy może nałożyć administracyjną karę pieniężną w wysokości do 20 000 000 euro, a w przypadku przedsiębiorstwa – w wysokości do 4% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa (art. 83 ust. 6 RODO).
Pomimo że nie wynika to wprost z treści przepisu, wydaje się, że przepis ten powinien być stosowany łącznie z art. 83 ust. 1 i 2 RODO, a więc organ nadzorczy powinien stosować przy jej nakładaniu ogólne kryteria nakładania kar (art. 83 ust. 1 RODO), jak i okoliczności wskazane w art. 83 ust. 2 oraz określony w tym przepisie zakres zastosowania kar.

Zgodnie z art. 83 ust. 7 RODO, każde państwo członkowskie może określić, czy i w jakim zakresie administracyjne kary pieniężne można nakładać na organy i podmioty publiczne ustanowione w tym państwie członkowskim.

W przypadku zbiegu naruszeń, zgodnie z art. 83 ust. 3 RODO, całkowita wysokość kary pieniężnej nie może przekroczyć wysokości kary za najpoważniejsze naruszenie. Do wyżej wymienionego zbiegu naruszeń dochodzić może w sytuacji, gdy w ramach tych samych lub powiązanych operacji przetwarzania danych, administrator danych lub procesor, dopuszcza się naruszeń umyślnie lub nieumyślnie.
Należy wskazać, że podstawowym warunkiem zastosowania art. 83 ust. 3 RODO jest to, by do naruszeń doszło w ramach tych samych lub powiązanych operacji przetwarzania danych. Nie dojdzie więc do jego zastosowania w przypadku popełnienia przez ten sam podmiot (administratora lub processora) wielu naruszeń, ale w ramach różnych, niepowiązanych ze sobą procesów przetwarzania danych.

Na odpowiedzialność cywilnoprawną administratora lub podmiotu przetwarzającego składają się:
a) prawo do dochodzenia przed sądem swoich praw, z pominięciem postępowania skargowego przed organem nadzorczym (art. 79 RODO),
b) prawo do dochodzenia odszkodowania lub zadośćuczynienia (art.82 RODO).

Wystąpienie z roszczeniami określonymi w art.79 nie wyłącza możliwości wystąpienia z innymi roszczeniami z tytułu naruszenia przepisów o ochronie danych osobowych (np. roszczeń określonych w art.82 RODO).

Dochodzenie roszczeń cywilnoprawnych dotyczących naruszenia przepisów o ochronie danych osobowych.
Zgodnie z art.93 PrUODO, w zakresie nieuregulowanym w RODO do roszczeń z tytułu naruszenia przepisów o ochronie danych osobowych, o których mowa w art. 79 i 82 Rozporządzenia, stosuje się przepisy KC.

Bez względu na wartość przedmiotu sporu sądem właściwym do orzekania w sprawach roszczeń określonych w art.79 ust.1 oraz art.82 ma być w pierwszej instancji sąd okręgowy (art.94 PrUODO). W zakresie nieuregulowanym przepisami uodo, subsydiarnie mają znaleźć zastosowanie przepisy KPC (art.101 PrUODO).

W PrUODO zawarto przepisy regulujące wzajemny związek spraw administracyjnych i cywilnoprawnych o naruszenie przepisów o ochronie danych osobowych.
Po pierwsze, sąd zawiesza postępowanie, jeżeli sprawa dotycząca tego samego naruszenia przepisów o ochronie danych osobowych, została wszczęta przed PUODO (art.96 PrUODO).
Po drugie, sąd umarza postępowanie w zakresie, w jakim prawomocna decyzja Prezesa Urzędu lub prawomocny wyrok wydany w wyniku wniesienia skargi, o której mowa w art. 145a PPSA uwzględnia roszczenie dochodzone przed sądem (art.97 PrUODO).
Po trzecie, ustalenia prawomocnej decyzji Prezesa Urzędu o stwierdzeniu naruszenia przepisów o ochronie danych osobowych lub prawomocnego wyroku wydanego w wyniku wniesienia skargi, o której mowa w art. 145a § 3 PPSA, wiążą sąd w postępowaniu o naprawnienie szkody wyrządzonej przez naruszenie przepisów o ochronie danych osobowych co do stwierdzenia naruszenia tych przepisów (art.98 PrUODO).

KARY PIENIĘŻNE

W przypadku roszczenia cywilnoprawnego z art.79 RODO na podkreślenie zasługuję jego oderwanie od materialnoprawnych podstaw roszczeń o naruszenie dóbr osobistych (art.23 i n. KC). Dla występowania na drogę sądową z tymi roszczeniami nie jest również konieczne wyczerpanie drogi w postaci przeprowadzenia postępowania skargowego przed organem nadzorczym, określonego w art.78 RODO.

Realizację uprawnień określonych w art.79 RODO urzeczywistniają przepisy art.78 i n. PrUODO. Zgodnie z nimi, w przypadku naruszenia praw przysługujących podmiotowi danych na podstawie przepisów o ochronie danych osobowych, może on może żądać: a) zaniechania tego działania, a także b) aby ten, kto dopuścił się naruszenia, dopełnił czynności potrzebnych do usunięcia jego skutków. Zgodnie z art.80 RODO, podmiot danych, niezależnie od możliwości samodzielnego działania, może również ustanowić swoim pełnomocnikiem organizacje społeczne, wyspecjalizowane w ochronie danych osobowych. Uprawnienie to nie wyłącza możliwości powoływania profesjonalnych pełnomocników.

W przepisie art.82 określono zasady odpowiedzialności odszkodowawczej administratora i podmiotu przetwarzającego. Podobnie, jak w przypadku art.79 RODO, chodzi tutaj o roszczenia kierowane do tych podmiotów przez osobę, których dane dotyczą (podmiot danych).

Warunkiem odpowiedzialności jest łączne spełnienie następujących przesłanek:
a) poniesienia przez podmiot danych szkody majątkowej lub niemajątkowej,
b) naruszenia przez administratora lub procesora przepisów RODO (tj. wystąpienia zdarzenia, w wyniku którego doszło do powstania szkody),
c) zaistnienia związku pomiędzy szkodą a naruszeniem oraz
d) wystąpienia winy w naruszeniu przepisów RODO (przepisów o ochronie danych osobowych).

Ciężar dowodu wystąpienia naruszenia, poniesienia szkody oraz związku przyczynowego spoczywa na podmiocie danych. Z art.82 ust.3 wynika domniemanie winy sprawy naruszenia. Ciężar dowodu, że do naruszenia nie doszło z winy administratora lub podmiotu przetwarzającego (procesora) spoczywa więc na tych podmiotach. Sposób sformułowania tego przepisu przypomina więc przepisy kodeksu cywilnego, wprowadzające tzw. odwrócony ciężar dowodu w sprawach o naruszenie dóbr osobistych.

Zgodnie z art.82 ust.4 RODO w przypadku, gdy w przetwarzaniu bierze udział więcej niż jeden administrator, więcej niż jeden procesor lub razem uczestniczą administrator i procesor, odpowiedzialność wszystkich tych podmiotów jest solidarna. W przepisach RODO nie określono zasad odpowiedzialności karnej, pozostawiając jedynie taką możliwość ustawodawcy krajowemu. Z możliwości tej skorzystał polski projektodawca, który w rozdziale 11 PrUODO wprowadził trzy przestępstwa karne za naruszenie przepisów o ochronie danych osobowych. Stanowi to istotne ograniczenie katalogu środków karnych, w stosunku do przepisów aktualnie obowiązującej ustawy. Dochodzenie odpowiedzialności karnej dotyczącej naruszenia przepisów o ochronie danych osobowych. Postępowanie w sprawach o czyny, określony w art.108-109 PrUODO, następuje na podstawie przepisów kodeksu postępowania karnego (kpk).

Zgodnie z art.108 PrUODO spenalizowano sytuację przetwarzania danych osobowych bez podstawy prawnej. Ustęp 2 tego przepisu zawiera kwalifikowaną postać przestępstwa, elementem różnicującym i kwalifikującym jest tutaj rodzaj danych (dane wrażliwe, których katalog określony został w art.9 RODO). Z uwagi na zagrożenie (grzywna, kara ograniczenia wolności albo pozbawienia wolności do roku), przestępstwo określone w art.108 zaliczyć należy do występków.

Przestępstwo to ma charakter powszechny, dopuścić się go może każda osoba, a nie tylko administrator danych, czy podmiot przetwarzający (procesor). Sposób sformułowania art.108 pozwala również na stwierdzenie, że opisany w nim czyn zabroniony może być popełnione jedynie z winy umyślnej.
Z kolei, w art. 109 PrUODO wprowadzono inny występek, które zgodnie z tym przepisem polegać ma na „udaremnieniu lub utrudnieniu kontrolującemu prowadzenie kontroli przestrzegania przepisów o ochronie danych osobowych".

HARMONOGRAM WDROŻENIA RODO

Należy zidentyfikować wszystkie osoby, jakie mogą być zaangażowane w proces przetwarzania danych osobowych, aby ustalić zasady współpracy w przedmiocie ochrony danych osobowych na poziomie analizy:

➢ Administrator i współadministrator danych osobowych,
➢ Osoba upoważniona do przetwarzania danych osobowych,
➢ Podmiot przetwarzający,
➢ Odbiorca danych osobowych,
➢ Inspektor ochrony danych,
➢ Firma IT/Informatyk/Księgowa,
➢ Pracownicy
➢ Dane osobowe zwykłe,
imię i nazwisko, adres, numer telefonu, adres e-mail, nick, PESEL, IP, zdjęcia, zapis z kamery, nagranie głosu, tablice rejestracyjne, informacje o aktywności w sieci, informacje o odwiedzanych miejscach, rozmiar ubrania, a nawet informacje o stylu jazdy zapisane w komputerze samochodu.
➢ Dane osobowe szczególne (dane osobowe szczególnie chronione),
➢ Dane osobowe pracowników,

Określenie zbiorów danych osobowych:

➢ Nazwa zbioru danych
➢ Zawarte dane osobowe
np. baza klientów, baza partnerów biznesowych, baza zleceniobiorców, ewidencja obiegu dokumentów, rejestr korespondencji wychodzącej i przychodzącej, rejestr zapytań itp.), ale również zbiór „tradycyjny", w postaci papierowej (np. kartoteka klientów, wykaz dłużników, rejestr osób wchodzących na teren zakładu).
➢ Sposób pozyskiwania danych do zbioru (bezpośrednio od Klienta/ od osób trzecich)

Ustalenie, w jakich celach i na jakiej podstawie dane są przetwarzane
➢ Rodzaje czynności podejmowanych w ramach przetwarzania danych osobowych
➢ Ustalenie, czy Klient korzysta z profilowania:
(cele profilowania, rodzaje, metody, osoby poddawane profilowaniu oraz decyzje podejmowane w ramach profilowania)
➢konieczność spełnienia przesłanki uprawniającej do przetwarzania: art. 5, 6, 7 i 9 RODO.

10 PODSTAWOWYCH ZASAD DLA NGO

CZY RODO MA ZASTOSOWANIE DO NASZEJ ORGANIZACJI?

Żeby sobie odpowiedzieć, czy organizacja pozarządowa musi przygotować się do RODO trzeba sprawdzić, czy NGO posiada dane osobowe.

Przykładowe grupy osób, których dane mogą być przetwarzane:
- członkowie stowarzyszenia
- pracownicy i współpracownicy
- wolontariusze
- darczyńcy
- użytkownicy serwisu internetowego
- odbiorcy newsletterów
- klienci/beneficjenci
- stypendyści
- uczestnicy szkoleń

MAPOWANIE

Należy przyjrzeć się „drodze" przetwarzania danych – jak obecnie wygląda zbieranie, gdzie są zapisywane, kto ma do nich wgląd, komu są przekazywane i udostępniane oraz w jaki sposób.

Proces przetwarzania danych będzie wyglądał inaczej w każdej organizacji pozarządowej w stosunku do różnych grup osób i różnych kategorii danych.

Do mapowania oraz sprawdzenia zgodności z zasadami przetwarzania danych pomocne może być wykorzystanie – rejestru przetwarzania danych (patrz krok czwarty). Tworzenie rejestru nie jest obowiązkowe dla każdej organizacji, ale może być przydatny, do przyjrzenia się danym w organizacji.

PODSTAWOWE ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

RODO wskazuje szereg zasad, których należy przestrzegać przy przetwarzaniu danych osobowych. Zasady te mają przełożenie na cały proces przetwarzania danych osobowych, więc warto je mieć uświadomione na samym początku wdrażania RODO. Ponadto zasady przekładają się na kolejne wymienione kroki – np. na obowiązek informacyjny, czy na odpowiednie zabezpieczenie danych.

1. Zgodność z prawem, przejrzystość, rzetelność – sposób przetwarzania danych powinien być oparty na podstawach prawa, być jasny i czytelny dla osoby, której dane dotyczą, która ma prawo wiedzieć po co dane są zbierane i co się z nimi dzieje. Więcej na ten temat podstaw prawnych do zbierania i przetwarzania danych jest opisana w kroku piątym. Zasada ta ma też przełożenie na wywiązywanie się z obowiązku informacyjnego (opisany w kroku dziewiątym).
2. Ograniczenie celem - przetwarzanie danych odbywa się tylko w konkretnych i uzasadnionych celach (trzeba umieć dookreślić po co, w jakim celu dane są przetwarzane – czy faktycznie muszą być zbierane).
3. Adekwatność, niezbędność i minimalizacja - zbierane i przetwarzane są tylko te dane, które niezbędne do ustalonych celów przetwarzania danych. To też oznacza, że zbierając konkretne dane osobowe trzeba mieć pewność, że faktycznie są one niezbędne (np. czy w danym przypadku jest potrzebny PESEL).
4. Prawidłowość - dane są prawidłowe, co też oznacza np. ich prostowanie w razie potrzeby.
5. Maksymalny czas przetwarzania - trzeba ustalić przez jaki okres dane będą przetwarzane. Okres ten jest ustalany m.in. ze względu na podstawę prawną i cele przetwarzania. Po ustalonym czasie dane trzeba usunąć.
6. Poufność i integralność - oznacza odpowiednie zabezpieczenie danych osobowych. Należy dbać o ochronę przed niedozwolonym czy niezgodnym z prawem przetwarzaniem; utratą danych, zniszczeniem lub uszkodzeniem. W tym celu należy dobrać odpowiednie środki techniczne lub organizacyjne zabezpieczające dane osobowe.
7. Rozliczalność – trzeba móc wykazać, że dane są przetwarzane zgodnie z zasadami wymienionymi powyżej (1-7).

10 PODSTAWOWYCH ZASAD DLA NGO

REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH (ART. 30 RODO)

RODO nie nakłada obowiązku prowadzenia tego rejestru przez wszystkie organizacje pozarządowe.

Rejestr powinien być prowadzony jeśli:
• zatrudnienie w organizacji wynosi powyżej 250 osób,
• istnieje ryzyko naruszenia praw i wolności osób, których dane dotyczą,
• przetwarzanie danych nie jest sporadyczne,
• przetwarzane są tzw. dane wrażliwe oraz wyroki skazujące i dotyczące naruszeń prawa.

Nawet jeśli organizacja uważa, że nie ma obowiązku prowadzenia rejestru czynności przetwarzania danych, to warto rozważyć używanie tego narzędzia - może być pomocne do zebrania w jednym miejscu wszystkich przetwarzanych danych osobowych oraz informacji nt. procesu przetwarzania danych. Przykładowy rejestr czynności przetwarzania danych osobowych można znaleźć na stronach UODO (Urzędu Ochrony Danych Osobowych (można tu też znaleźć rejestr kategorii czynności przetwarzania danych – ten rejestr dotyczy podmiotów przetwarzających, a nie administratorów danych osobowych).

USTALENIE PODSTAWY PRAWNEJ PRZETWARZANIA DANYCH OSOBOWYCH (PRZESŁANKI LEGALIZACYJNE)

Określenie podstawy prawnej przetwarzania danych osobowych jest jedną z podstawowych zasad przetwarzania danych, ale jest konieczne m.in. do wywiązania się z obowiązku informacyjnego wobec osób, których dane organizacja przetwarza („9"). RODO wskazuje odrębne podstawy prawne do przetwarzania tzw. danych zwykłych oraz danych wrażliwych.

DANE ZWYKŁE (ART. 6 RODO)

RODO wymienia 6 podstaw prawnych uprawniających do przetwarzania danych osobowych tzw. „zwykłych":
1. zgoda osoby, której dane dotyczą (o zgodzie zobacz: „Kiedy i jaka zgoda na przetwarzanie danych osobowych");
2. umowa (wtedy, gdy z osobą, której dane dotyczą łączy organizację jakaś umowa, która określa strony umowy, a więc i dane osoby);
3. obowiązek prawny (określony innymi przepisami, np. kodeksem pracy, ustawą o systemie ubezpieczeń społecznych, itp.);
4. żywotne interesy osoby, której dane dotyczą - trzeba móc te interesy wykazać, np. ochrona zdrowia, życia;
5. zadanie realizowane w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
6. prawnie uzasadniony interes administratora.

DANE WRAŻLIWE (ART. 9 RODO)

Do przetwarzania szczególnych kategorii danych osobowych (tzw. danych wrażliwych) RODO wskazuje odrębne podstawy prawne.
Szczególne kategorie danych osobowych dotyczą: pochodzenia rasowego lub etnicznego, zdrowia, seksualności, poglądów politycznych, religii, światopoglądu, przynależności do związków zawodowych, danych genetycznych, danych biometrycznych służących do jednoznacznego zidentyfikowania osoby fizycznej.

10 PODSTAWOWYCH ZASAD DLA NGO

Zgodnie z RODO dane wrażliwe można przetwarzać wyłącznie w następujących przypadkach:

a. na podstawie wyraźnej zgody;

b. w celu wypełnienia obowiązków przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej;

c. ze względu na ochronę żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej (w sytuacji gdy osoba, której dane dotyczą nie ma możliwości wyrażenia zgody);

d. w ramach uprawnionej działalności fundacji, stowarzyszeń (oraz innych niezarobkowych podmiotów o celach politycznych, światopoglądowych, religijnych lub związkowych) - pod warunkiem że przetwarzanie dotyczy wyłącznie członków lub byłych członków tego podmiotu lub osób utrzymujących z nim stałe kontakty w związku z jego celami oraz że dane osobowe nie są ujawniane poza tym podmiotem bez zgody osób, których dane dotyczą;

e. dane zostały upublicznione przez osobę, której dane dotyczą;

f. ustalenie, dochodzenie lub obrona roszczeń oraz sprawowanie wymiaru sprawiedliwości przez sądy;

g. w związku z ważnym interesem publicznym (na podstawie prawa Unii lub prawa państwa członkowskiego);

h. do celów profilaktyki i opieki zdrowotnej, zabezpieczenia społecznego, do celów medycyny pracy, zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego (na podstawie przepisów prawa lub zgodnie z umową z pracownikiem służby zdrowia);

i. w interesie publicznym w dziedzinie zdrowia publicznego, np. w związku z ochroną przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych (na podstawie przepisów prawa, po spełnieniu określonych wymogów);

j. przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych (na podstawie określonych przepisów prawa, po spełnieniu odpowiednich wymogów).

PRZEPROWADZENIE OCENY RYZYKA, POLITYKA BEZPIECZEŃSTWA

Analiza ryzyka jest kluczowym etapem do wdrożenia RODO w organizacji. Można powiedzieć, że ochrona danych osobowych wg RODO opiera się na analizie ryzyka - postępowanie z danymi osobowymi oparte jest na oszacowaniu ryzyka.

Analiza ryzyka ma pokazać niebezpieczeństwa i zagrożenia dla danych osobowych - do wyników tej oceny powinien być dostosowany tryb postępowania i wybór odpowiednich środków zaradczych.

Analiza ryzyka ma prowadzić do wdrożenia środków technicznych i organizacyjnych aby zapewnić odpowiedni poziom bezpieczeństwa (dostosowany do poziomu ryzyka).

10 PODSTAWOWYCH ZASAD DLA NGO

OCENA SKUTKÓW PLANOWANYCH OPERACJI PRZETWARZANIA DLA OCHRONY DANYCH OSOBOWYCH. POGŁĘBIONA ANALIZA RYZYKA

Analiza skutków planowanych działań nie zawsze jest obowiązkowa (w przeciwieństwie do analizy ryzyka która zawsze powinna być dokonana).

Analizę skutków należy przeprowadzić jeśli w organizacji:

• istnieje wysokie ryzyko naruszenia praw lub wolności (tak wyszło z oceny ryzyka);

• następuje systematyczne, zautomatyzowane przetwarzanie czynników osobowych, np. profilowanie;

• następuje przetwarzanie na dużą skalę szczególnych kategorii danych osobowych (danych „wrażliwych" opisanych w art. 9 RODO), lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa;

• jest prowadzone systematyczne monitorowania na dużą skalę miejsc dostępnych publicznie

Analiza skutków ma zagwarantować dobór środków technicznych i organizacyjnych, które zapewnią przetwarzanie danych w zgodzie z przepisami RODO.

POWOŁANIE INSPEKTORA OCHRONY DANYCH OSOBOWYCH

Powołanie inspektora ochrony danych osobowych (podobnie jak pogłębiona analiza ryzyka z kroku siódmego) też nie zawsze jest obowiązkowe.

Obowiązek powołania inspektora ochrony dany osobowych dotyczy:

• podmiotów publicznych;

• administratorów i podmiotów, których główna działalność polega na operacjach przetwarzania, które wymagają regularnego i systematycznego monitorowania na dużą skalę osób, których dane dotyczą;

• główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych;

• w sytuacjach, gdy przepisy szczególne tego wymagają (np. polskie ustawy)

W pozostałych przypadkach powołanie inspektora jest fakultatywne. Jednak nawet jeśli organizacja pozarządowa nie musi powołać inspektora, może uznać z innych względów, że jest to wskazane. Inspektor może być pomocny w większych organizacjach pozarządowych, które zatrudniają wielu pracowników i przetwarzają dużą ilość danych. Inspektor może być też osobą wynajętą – osoba, z której usług korzystamy (podobnie jak np. przy korzystaniu z usług biura księgowego etc.).

10 PODSTAWOWYCH ZASAD DLA NGO

PRZESTRZEGANIE PRAW OSÓB, KTÓRYCH DANE SĄ PRZETWARZANE ORAZ WYPEŁNIAJ OBOWIĄZEK INFORMACYJNY

Osoby, których dane dotyczą mają prawo wiedzieć, co dzieje się z ich danymi i na co mają wpływ – powinni być o tym powiadomieni w sposób zrozumiały, prostym językiem.

Spełnienie obowiązku informacyjnego jest jednym z ważniejszych obowiązków administratora.

Zakres obowiązku informacyjnego jest uzależniony m.in. od podstawy prawnej przetwarzania danych osobowych oraz od tego, czy dane zostały pozyskane bezpośrednio od osoby, której dotyczą, czy z innych źródeł (np. z jakiegoś oficjalnego rejestru).

W ramach wypełniania tego obowiązku, należy poinformować osoby, których dane są przetwarzane.

ŚWIADOMOŚĆ KAR

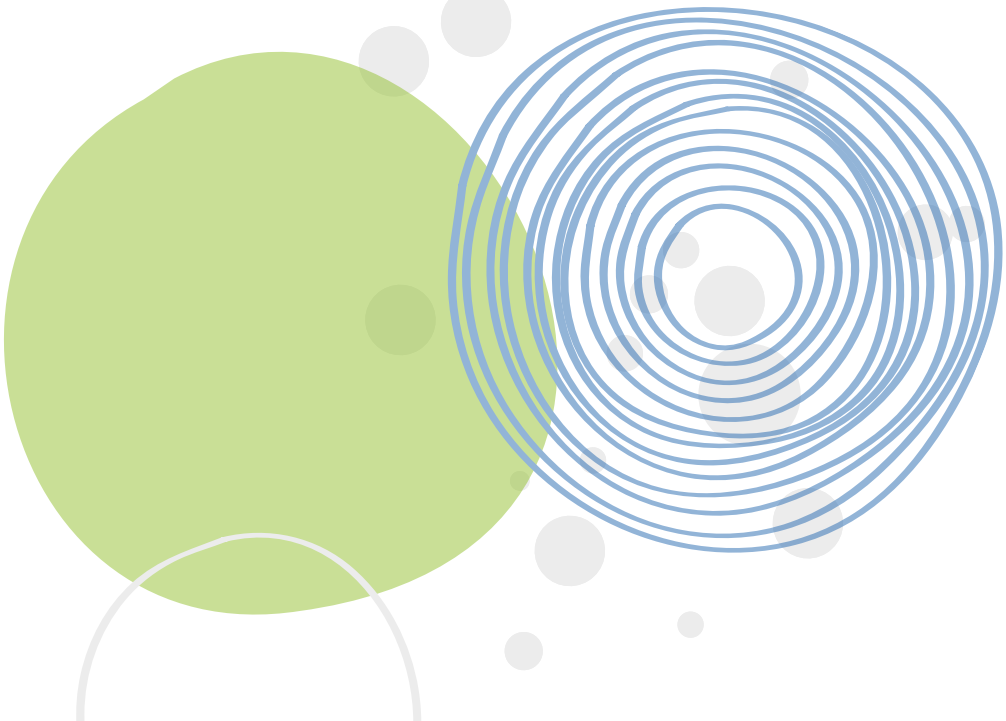
RODO wprowadza możliwość nakładania sankcji i kar administracyjnych i odpowiedzialność cywilną w związku z nieprzestrzeganiem wymogów RODO.

Sankcje i kary administracyjne może nakładać organ nadzoru (Urząd Ochrony Danych Osobowych). Sankcji administracyjne, to m.in.:

- ostrzeżenie;
- upomnienie;
- nakazanie spełnienia żądania osoby, której dane dotyczą, wynikającego z praw;
- nakazanie dostosowania operacji przetwarzania do przepisów niniejszego rozporządzenia, a w stosownych przypadkach wskazanie sposobu i terminu;
- nakazanie administratorowi zawiadomienia osoby, której dane dotyczą, o naruszeniu ochrony danych;
- wprowadzanie czasowego lub całkowitego ograniczenia przetwarzania, w tym zakazu przetwarzania;

Kary administracyjne finansowe sięgają nawet 20 milionów euro lub do 4% wartości rocznego światowego obrotu przedsiębiorstwa.

Odpowiedzialność cywilna wiąże się z możliwością żądania zapłaty odszkodowania od osoby, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia przepisów RODO.



WZORY PODSTAWOWYCH DOKUMENTÓW ZWIĄZANYCH Z PRZETWARZANIEM DANYCH OSOBOWYCH

KLAUZULA INFORMACYJNA

Na podstawie art. 13 ust. 1–2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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 (Dz.Urz. UE L 2016, Nr 119) - w dalszej części: RODO - informujemy, że:

1. Administratorem Państwa danych osobowych jest Stowarzyszenie/Fundacja „.....” (dalej .....) zwana dalej również Administratorem.
2. Państwa dane osobowe będą przetwarzane w celu:
a) zawarcia i realizacji umowy – art. 6 ust. 1 lit.b) RODO
b) w celu przygotowania wstępnej oferty współpracy, założenia profilu/konta na stronach należących do Administratora, rozpatrzeniu przez Administratora wniosku złożonego przez Państwa,
c) realizacji działań marketingowych/promocyjnych dotyczących usług własnych oraz świadczonych przez podmioty z nami współpracujące (partnerów) w zakresie przesyłania informacji za pośrednictwem środków komunikacji elektronicznej i telefonicznej, po uprzednim wyrażeniu przez Państwa dobrowolnej zgody na podstawie Art. 6 ust. 1 lit. a) RODO
d) ewentualnego dochodzenia lub obrony przed roszczeniami, jako realizacja naszego prawnie uzasadnionego interesu, na podstawie art. 6 ust. 1 lit. f RODO;
3. Przysługuje Państwu prawo do wniesienia sprzeciwu wobec przetwarzania Państwa danych osobowych, na podstawie którego przestaniemy przetwarzać Państwa dane w celach określonych w punkcie 3, z wyłączeniem sytuacji gdy wykażemy, że w stosunku do Państwa danych przysługują nam prawnie uzasadnione podstawy, nadrzędne wobec Państwa interesów, praw i wolności, w szczególności w ramach naszego prawnie uzasadnionego interesu oraz gdy dane będą niezbędne do ustalenia, dochodzenia lub obrony roszczeń.
4. Informujemy, iż Państwa dane przetwarzane w celu niezbędnym do wykonania umowy/rozpatrzenia wniosku będą przechowywane przez okres, w którym mogą ujawnić się roszczenia związane z umową/projektem/wnioskiem wynikające z przepisów kodeksu cywilnego i / lub prawa podatkowego.
5. Informujemy, że Państwa dane zgromadzone przez Administratora mogą być również przetwarzane w sposób zautomatyzowany oraz mogą być profilowane. (wariantowo)
6. Państwa dane osobowe mogą być udostępniane innym podmiotom, tj. podmiotom świadczącym usługi na rzecz Administratora, portalom ogłoszeniowym z którymi współpracuje Administrator, dostawcom usług IT, doradcom, na podstawie umów o powierzenie przetwarzania danych osobowych oraz innym uprawnionym podmiotom, wyłącznie w zakresie określonym w przepisach prawa przez okres przedawnienia roszczeń przysługujących Administratorowi oraz w stosunku do niego.
7. Jako podmioty danych mają Państwo prawo do:
- dostępu do swoich danych oraz możliwość otrzymania ich kopii;
- przenoszenia danych;
- wniesienia sprzeciwu wobec przetwarzania danych;
- sprostowania swoich danych;
- ograniczenia przetwarzania danych; usunięcia danych;
- wniesienia skargi do organu nadzorczego tj. Prezesa Urzędu Ochrony Danych Osobowych.
8. Podanie przez Państwa danych osobowych ma charakter dobrowolny, ale jest konieczne do świadczenia usług przez Administratora.

ZAWIADOMIENIE O NARUSZENIU OCHRONY PANI DANYCH OSOBOWYCH

Szanowna Pani,
W ostatnich dniach doszło do incydentu, wskutek którego Pani dane osobowe mogły znaleźć się w posiadaniu osób nieupoważnionych. Poniżej przekazujemy informacje dotyczące tego incydentu, a także działań, jakie w związku z tym podejmujemy. Podajemy też informacje o krokach, które Pani może podjąć w związku z incydentem. Prosimy o uważną lekturę niniejszego zawiadomienia.

Co się stało?
Dnia ... omyłkowo wysłaliśmy wystawioną na Panię fakturę za nasze usługi do innego klienta. Chodzi tutaj o fakturę dotyczącą ..... .
Faktura zawierania następujące dane osobowe dotyczące Pani: imię i nazwisko, numer NIP, adres zamieszkania, informację na temat świadczonych przez nas usług, oraz kwotę do zapłaty.

Możliwe konsekwencje dla Pani
Wskutek wysłania faktury wystawionej na Pani może dojść do tego, że dostęp do tych danych uzyska osoba nieupoważniona. Osoba ta miałaby więc informacje o Pani imieniu i nazwisku, adresie zamieszkania, numerze NIP, a także informacje o tym, że ..... . Ponadto na fakturze widnieje kwota do zapłaty, co może pośrednio dotyczyć Pani zobowiązań finansowych.
Na chwilę obecną nie mamy żadnych sygnałów, że dokument z Pani danymi został gdzieś upubliczniony lub jest wykorzystywany przez osobę niepowołaną. Istnieje jednakże ryzyko, że ktoś będzie próbował wykorzystać Pani dane osobowe w celu podszycia się pod Panią (tzw. kradzież tożsamości). Rozumiemy także, że upublicznienie Pani danych osobowych mogłoby wywołać u Pani stres lub inne negatywne odczucia.

Działania podjęte przez nas
Wysłaliśmy zawiadomienie do naszego klienta, któremu omyłkowo wysłaliśmy fakturę przeznaczoną dla Pani. Wyjaśniliśmy klientowi , że faktura została do niego wysłana omyłkowo i poprosiliśmy o jej zniszczenie lub odesłanie do nas. Jak tylko otrzymamy odpowiedź od naszego klienta z potwierdzeniem zniszczenia faktury lub jeśli klient odeśle nam fakturę, poinformujemy Panią o tym.
Na bieżąco monitorujemy, czy Pani dane zostały gdzieś upublicznione lub wykorzystane przez osobę nieuprawnioną. Na chwilę obecną nie mamy żadnych sygnałów o takim nieuprawnionym wykorzystaniu Pani danych lub o ich upublicznieniu.

Co może Pani zrobić?
W związku z ryzykiem kradzieży tożsamości, prosimy o ostrożność przy podawaniu Pani danych osobowych innym osobom. Dotyczy to szczególnie podawania danych za pośrednictwem Internetu lub przez telefon. Jeżeli dowie się Pani o upublicznieniu lub wykorzystaniu Pani danych przez osobę nieuprawnioną, bardzo prosimy o natychmiastowe przekazanie nam tej informacji.

Więcej informacji
Jeżeli ma Pani jakiekolwiek pytania, lub chciałaby nam Pani przekazać dodatkowe informacje w związku z zagubieniem dokumentu z Pani danymi osobowymi, prosimy o kontakt z nami/ naszym inspektorem ochrony danych – p. Janem Nowakiem. Poniżej podajemy dane kontaktowe inspektora ochrony danych:
Adres email:
Numer telefonu:
Adres korespondencyjny:
DW: Inspektor ochrony danych

WYZNACZENIE INSPEKTORA OCHRONY DANYCH W (PODAĆ NAZWĘ PODMIOTU)

W imieniu (podać nazwę podmiotu(na podstawie art. 37 ust. 1 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) dalej jako „RODO", wyznacza Panią/Pana imię i nazwisko na inspektora ochrony danych (dalej jako „Inspektor") w (podać nazwę podmiotu)

Inspektor będzie wykonywał zadania określone w RODO, w szczególności w art. 39 i art. 47 ust. 2 pkt h) oraz zadania określone na podstawie art. 38 ust. 6 RODO wymienić zadania IOD inne niż wykonywane na podstawie art. 39 i art. 47 ust. 2 pkt h) RODO, jeżeli dotyczy.

Inspektor pełni swoją funkcję do data wygaśnięcia lub aż do wyraźnego odwołania przez administratora danych z innych przyczyn niż wypełnianie zadań Inspektora lub aż do wyraźnej rezygnacji Inspektora z tej funkcji.

Niniejsze wyznaczenie wchodzi w życie z dniem ..... 2018 r.

.....
Imię, nazwisko i podpis
/zgodnie z zasadami reprezentacji/

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

....., dnia ..... 20..... r.
UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH
Nr .....

Niniejszym, zgodnie z art. 5 ust.1 lit f) w zw. z 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 dyrektywy 95/46/WE (dalej RODO),

upoważniam
Panią/Pana: .....
Stanowisko: .....
do przetwarzania danych osobowych w podać nazwę podmiotu(dalej jako „NGO") w następującym zakresie:

A. Okres upoważnienia:
• na okres zatrudnienia w NGO */ do dnia ..... włącznie*

B. Zakres upoważnienia:
• dane przetwarzane na nośnikach papierowych:
.....
• system informatyczny oraz urządzenia wchodzące w jego skład:
.....
(bez ograniczeń*, podgląd danych*, wprowadzanie danych*, opracowywanie danych*, zmienianie danych*, usuwanie danych*, na komputerach przenośnych*).
• dane osobowe przetwarzane w ramach udziału w następujących czynności przetwarzania danych:
a) podać nazwę czynności (procesu) zgodnie z rejestrem czynności
b) .....
c) .....

.....
Imię, nazwisko i podpis
/zgodnie z zasadami reprezentacji/

*niepotrzebne usunąć

UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

zawarta w _____
pomiędzy

_____, zwanym dalej „Administratorem”
a
_____, zwanym dalej „Powierzającym”

1. DEFINICJE
Dla potrzeb niniejszej umowy, Administrator i Przetwarzający ustalają następujące znaczenie niżej wymienionych pojęć:

1) Umowa Powierzenia – niniejsza umowa;
2) Umowa Główna – [umowa, w związku z którą zawierana jest umowa powierzenia – przetwarzanie danych jest konieczne do wykonania Umowy Głównej]
3) RODO - 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) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1).

2. OŚWIADCZENIA STRON
Strony oświadczają, że niniejsza Umowa Powierzenia została zawarta w celu wykonania obowiązków, o których mowa w art. 28 RODO w związku z zawarciem Umowy Głównej,

3. PRZEDMIOT UMOWY
3.1. W trybie art. 28 ust. 3 RODO, Administrator powierza Przetwarzającemu do przetwarzania dane osobowe wskazane w pkt 4.1.-4.2. poniżej, a Przetwarzający zobowiązuje się do ich przetwarzania zgodnego z prawem i niniejszą Umową Powierzenia.
3.2. Przetwarzający może przetwarzać dane osobowe wyłącznie w zakresie i celu przewidzianym w Umowie Powierzenia, oraz zgodnie z innymi udokumentowanymi poleceniami Administratora, przy czym za takie udokumentowane polecenia uważa się postanowienia Umowy Powierzenia oraz ewentualne inne polecenia przekazywane przez Administratora drogą elektroniczną na adres _____ lub na piśmie.

4. CEL, ZAKRES I CHARAKTER PRZETWARZANIA
4.1. Przetwarzający zobowiązuje się do przetwarzania danych osobowych następujących kategorii osób, których dane dotyczą:
a) _____
b) _____
4.2. Zakres powierzonych Przetwarzającemu do przetwarzania danych osobowych obejmuje:
a) co do [kategoria osób]:
i. _____
b) co do [kategoria osób]:
i. _____

4.3. Celem przetwarzania danych osobowych wskazanych w pkt 4.1.-4.2. powyżej jest wykonanie Umowy Głównej, w szczególności _____.
4.4. Przetwarzający zobowiązuje się do przetwarzania danych osobowych w sposób stały. Przetwarzający będzie w szczególności wykonywał następujące operacje dotyczące powierzonych danych osobowych: _____. Dane osobowe będą przez Przetwarzającego przetwarzane w formie elektronicznej w systemach informatycznych oraz w formie papierowej.
4.5. Przetwarzający będzie zbierał/otrzymywał dane osobowe od _____ [sposób, źródła zbierania danych].

5. ZASADY POWIERZENIA PRZETWARZANIA
5.1. Przed rozpoczęciem przetwarzania danych osobowych Przetwarzający musi podjąć środki zabezpieczające dane osobowe, o których mowa w art. 32 RODO, a w szczególności:
a) uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, obowiązany jest zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku. Przetwarzający powinien odpowiednio udokumentować zastosowanie tych środków, a także uaktualniać te środki w porozumieniu z administratorem,
b) zapewnić, by każda osoba fizyczna działająca z upoważnienia Przetwarzającego, która ma dostęp do danych osobowych, przetwarzała je wyłącznie na polecenie administratora w celach i zakresie przewidzianym w Umowie Powierzenia,
c) prowadzić rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu Administratora, o którym mowa w art. 30 ust. 2 RODO i udostępniać go Administratorowi na jego żądanie, chyba że Przetwarzający jest zwolniony z tego obowiązku na podstawie art. 30 ust. 5 RODO.
5.2. Przetwarzający zapewnia, aby osoby mające dostęp do przetwarzanych danych osobowych zachowały je oraz sposoby zabezpieczeń w tajemnicy, przy czym obowiązek zachowania tajemnicy istnieje również po realizacji Umowy Powierzenia oraz ustaniu zatrudnienia u Przetwarzającego.

6. DALSZE OBOWIĄZKI PRZETWARZAJĄCEGO
6.1. Przetwarzający zobowiązuje się pomagać Administratorowi w wywiązywaniu się z obowiązków określonych w art. 32-36 RODO.
6.2. W sytuacji podejrzenia naruszenia ochrony danych osobowych, Przetwarzający zobowiązuje się do:
a) przekazania Administratorowi informacji dotyczących naruszenia ochrony danych osobowych w ciągu 24 godzin od jego wykrycia, w tym informacji, o których mowa w art. 33 ust. 3 RODO,
b) przeprowadzenia wstępnej analizy ryzyka naruszenia praw i wolności osób, których dane dotyczą, i przekazania wyników tej analizy do Administratora w ciągu 36 godzin od wykrycia zdarzenia stanowiącego naruszenie ochrony danych osobowych,
c) przekazania Administratorowi – na jego żądanie – wszystkich informacji niezbędnych do zawiadomienia osoby, której dane dotyczą, zgodnie z art. 34 ust. 3 RODO, w ciągu 48 godzin od wykrycia zdarzenia stanowiącego naruszenie ochrony danych osobowych.
6.3. Przetwarzający zobowiązuje się pomagać Administratorowi poprzez odpowiednie środki techniczne i organizacyjne, w wywiązywaniu się z obowiązku odpowiadania na żądania osób, których dane dotyczą, w zakresie wykonywania ich praw określonych w art. 15-22 RODO. W szczególności Przetwarzający zobowiązuje się – na żądanie Administratora – do przygotowania i przekazania Administratorowi informacji potrzebnych do spełnienia żądania osoby, której dane dotyczą, w ciągu 3 dni od dnia otrzymania żądania Administratora.

6.4. Przetwarzający zobowiązuje się stosować się do ewentualnych wskazówek lub zaleceń, wydanych przez organ nadzoru lub unijny organ doradczy zajmujący się ochroną danych osobowych, dotyczących przetwarzania danych osobowych, w szczególności w zakresie stosowania RODO.
6.5. Przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania powierzonych danych osobowych przez Przetwarzającego, o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania powierzonych danych osobowych, skierowanej do Przetwarzającego, a także o wszelkich kontrolach i inspekcjach dotyczących przetwarzania powierzonych danych osobowych przez Przetwarzającego, w szczególności prowadzonych przez organ nadzorczy.

7. PODPOWIERZENIE PRZETWARZANIA
[Komentarz: Jeżeli nie przewiduje się możliwości podpowierzenia przetwarzania, należy usunąć postanowienia pkt 7.]
7.1. Administrator dopuszcza możliwość podpowierzenia przetwarzania powierzonych danych osobowych podwykonawcom Przetwarzającego (tzw. subprocesorom). Jeżeli Przetwarzający zamierza podpowierzyć przetwarzanie danych osobowych swoim podwykonawcom, musi uprzednio poinformować Administratora o zamiarze podpowierzenia oraz o tożsamości (nazwie) podmiotu, któremu ma zamiar podpowierzyć przetwarzanie danych, a także o charakterze podpowierzenia, zakresie danych, celu i czasie trwania podpowierzenia. O ile Administrator nie wyrazi sprzeciwu wobec podpowierzenia w terminie 7 dni od daty zawiadomienia, Przetwarzający uprawniony będzie do dokonania podpowierzenia.
7.2. W przypadku podpowierzenia przetwarzania danych osobowych, podpowierzenie przetwarzania będzie mieć za podstawę umowę, na podstawie której podwykonawca (subprocesor) zobowiąże się do wykonywania tych samych obowiązków, które na mocy niniejszej Umowy Powierzenia nałożone są na Przetwarzającego. Umowa będzie zawarta w tej same formie co niniejsza Umowa Powierzenia.
7.3. Administratorowi będą przysługiwały uprawnienia wynikające z umowy podpowierzenia bezpośrednio wobec podwykonawcy (subprocesora). W przypadku wypowiedzenia lub rozwiązania umowy podpowierzenia, Przetwarzający poinformuje o tym fakcie Administratora w terminie 3 dni od wypowiedzenia lub rozwiązania umowy.
7.4. Przetwarzający nie może przekazywać powierzonych mu przetwarzania danych osobowych do podmiotów znajdujących się w państwach spoza Europejskiego Obszaru Gospodarczego.

8. AUDYT PRZETWARZAJĄCEGO
8.1. Administrator jest uprawniony do weryfikacji przestrzegania zasad przetwarzania danych osobowych wynikających RODO oraz niniejszej Umowy Powierzenia przez Przetwarzającego, poprzez prawo żądania udzielenia wszelkich informacji dotyczących powierzonych danych osobowych.
8.2. Administrator ma także prawo przeprowadzania audytów lub inspekcji Przetwarzającego w zakresie zgodności operacji przetwarzania z prawem i z Umową Powierzenia. Audyty lub inspekcje, o których mowa w zdaniu poprzedzającym, mogą być przeprowadzane przez podmioty trzecie upoważnione przez Administratora.
8.3. Przetwarzający zobowiązuje się niezwłocznie informować Administratora, jeżeli zdaniem Przetwarzającego wydane jemu polecenie stanowi naruszenie RODO lub innych przepisów o ochronie danych.

9. ZAKOŃCZENIE POWIERZENIA PRZETWARZANIA
9.1. Po zakończeniu świadczenia usług związanych z przetwarzaniem danych osobowych Przetwarzający zależnie od decyzji Administratora usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie.

10. POSTANOWIENIA KOŃCOWE

MATERIAŁY POMOCNICZE

1) Opinia 1/2010 w sprawie pojęć „administrator danych" i „przetwarzający" (WP 169), wersja po zmianach z dnia 16 lutego 2010 r.

2) Wytyczne dotyczące prawa do przenoszenia danych (WP 242), wersja po zmianach z dnia 5 kwietnia 2017 r.

3) Wytyczne dotyczące inspektorów ochrony danych (WP 243), wersja po zmianach z dnia 5 kwietnia 2017 r.

4) Wytyczne dotyczące ustalenia wiodącego organu nadzorczego właściwego dla administratora lub podmiotu przetwarzającego (WP 244), wersja po zmianach z dnia 5 kwietnia 2017 r.

5) Wytyczne dotyczące oceny skutków dla ochrony danych (DPIA) i ustalenia, czy przetwarzanie „może powodować wysokie ryzyko" do celów rozporządzenia 679/2016 (WP 248), wersja po zmianach z dnia 4 października 2017 r.

6) Opinia 2/2017 w sprawie przetwarzania danych w pracy (WP 249), wersja po zmianach z dnia 8 czerwca 2017 r.

7) Wytyczne w sprawie zautomatyzowanego podejmowania decyzji i profilowania (WP 251), wersja po zmianach z dnia 6 lutego 2018 r.

8) Wytyczne w sprawie powiadomień o naruszeniu ochrony danych osobowych na mocy rozporządzenia 2016/679 (WP 250), wersja po zmianach z dnia 6 lutego 2018 r.

9) Wytyczne w sprawie stosowania i ustalania administracyjnych kar pieniężnych do celów rozporządzenia nr 2016/679 (WP 253), wersja po zmianach z dnia 3 października 2017 r.

10) Wytyczne dotyczące zgody na mocy rozporządzenia 2016/679 (WP259), wstępna wersja z dnia 12 grudnia 2017 r.

11) Wytyczne dotyczące przejrzystości na mocy rozporządzenia 2016/679 (WP260), wstępna wersja z dnia 12 grudnia 2017 r.

12) Wyjaśnienia i wskazówki GIODO dotyczące sposobu realizacji określonego w art. 30 RODO obowiązku prowadzenia rejestru czynności oraz kategorii czynności wraz szablonami obu typów rejestrów i przykładami ich uzupełnienia, dostępne pod adresem: https://giodo.gov.pl/pl/1520281/10449.

13) Ministerstwo Cyfryzacji, Informator RODO, dostępny pod adresem: https://www.gov.pl/documents/31305/436699/RODO.pdf/9b7e519b-0d5c-1ef8-4caf-02f8d247aa1d

ZAGADNIENIA PRAKTYCZNE

Dane osobowe pracowników możemy znaleźć w następujących przykładowych zbiorach danych osobowych:
➢ rekrutacja,
➢ przebieg zatrudnienia,
➢ monitoring,
➢ postępowania sądowe,
➢ księga gości czy rejestr osób wchodzących/wychodzących do/z budynków,
➢ serwisy internetowe,
➢ dane powierzone.

W ramach zbioru danych dotyczących przebiegu zatrudnienia możemy wskazać następujące przykładowe procesy:
➢ realizacja praw i obowiązków pracowniczych w ramach zatrudnienia,
➢ przetwarzanie danych w ramach zakładowego funduszu świadczeń socjalnych,
➢ korzystanie przez pracowników z dodatkowych benefitów (kart sportowych, ubezpieczenia, opieki medycznej),
➢ konkursy pracownicze,
➢ wykorzystywanie wizerunku pracowników,
➢ monitorowanie aktywności pracowników w sieci teleinformatycznej,
➢ podnoszenie kwalifikacji i szkolenia pracowników,
➢ prowadzenie floty samochodów.

Od 25 maja 2018 r. zmianie ulegną między innymi przepisy ustawy Kodeks pracy, w zakresie dotyczącym gromadzenia danych osobowych pracowników i kandydatów do pracy, w tym art. 22(1) § 1 k.p.

Pracodawca będzie mógł żądać od kandydata do pracy podania:
• imienia (imion) i nazwiska,
• daty urodzenia,
• wykształcenia
• adresu do korespondencji,
• adresu poczty elektronicznej albo numeru telefonu,
• informacji o przebiegu dotychczasowego zatrudnienia

Wobec swoich pracowników pracodawca musi wypełnić obowiązek informacyjny określony w art. 13 ust. 1 i 2 RODO.

Zatrudniający nie jest jednak zobligowany do zrealizowania w/w obowiązku informacyjnego w takim zakresie, w jakim podwładni już posiadają dane wymienione w powołanym przepisie RODO.

Pracodawca musi podać wówczas jedynie te brakujące dane (m.in. wskazując jako odbiorcę danych – biuro rachunkowe). Wynika to z art. 13 ust. 4 RODO.

ZAGADNIENIA PRAKTYCZNE

W świetle art. 13 ust. 1 RODO pracodawca zobligowany jest podać:

➢ swoją tożsamość i dane kontaktowe oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe swojego przedstawiciela;
➢ gdy ma to zastosowanie – dane kontaktowe inspektora ochrony danych;
➢ cele przetwarzania danych osobowych, oraz podstawę prawną przetwarzania;
➢ jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f RODO – należy wskazać prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią;
➢ informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją (tu – m.in. biuro rachunkowe);
➢ gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi RODO, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych.

Przepis art. 13 ust. 2 RODO stanowi, z kolei, iż, poza informacjami, o których mowa w ust. 1, pracodawca musi podać:

➢ okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu,
➢ informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;
➢ jeżeli przetwarzanie odbywa się na podstawie:
1) art. 6 ust. 1 lit. a RODO (czyli osoba, które dane dotyczą wyraziła zgodę na przetwarzanie danych osobowych w co najmniej jednym określonym celu) lub
2) art. 9 ust. 2 lit. a RODO (czyli osoba, której niżej wymienione szczególne kategorie danych osobowych dotyczą, wyraziła zgodę na ich przetwarzanie w co najmniej jednym określonym celu) – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;
➢ informację o prawie wniesienia skargi do organu nadzorczego (czyli do Prezesa Urzędu Ochrony Danych Osobowych);
➢ informację, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;
➢ gdy ma to zastosowanie- informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO, 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.

PRZYKŁADOWE PODSTAWOWE ZALECENIA

1. w komputerze hasło dostępu zmieniamy raz w miesiącu,

2. nie trzymamy dokumentów na biurku – zasada czystego biurka, zasada „czystego biurka" dotyczy także pulpitu komputerowego

3. dokumenty są przechowywane w zamykanych na klucz szafach,

4. klucz zapasowy do szafy z dokumentami przechowujemy w ustalonym z Dyrekcją miejscu, podobnie jak klucz zapasowy do pokoju,

5. archiwizujemy dokumenty elektroniczne w ten sposób, że tworzymy zewnętrzna kopię zapasową, która aktualizujemy raz w miesiącu. Kopia zapasowa przechowywana jest w ustalonym i zabezpieczonym miejscu

6. na komputerze nie przechowujemy plików spraw zakończonych – dotyczy także pulpitu

7. na bieżąco sprawdzamy zasoby znajdujące się na pulpicie komputera w przypadku braku uzasadnienia do utrzymywania zbioru danych – archiwizujemy go i usuwamy,
8. monitor komputerowy w pokoju musi być tak ustawiony, aby nie było możliwości odczytania danych przez osobę wchodząca do pomieszczenia,

9. pobieramy oświadczenia o zgodzie na przetwarzanie danych osobowych od osób fizycznych – tzw. prywatnych (np. ekshumacje, interwencje), przedsiębiorców prowadzących działalność gospodarczą na podstawie wpisu do CEiDG, wspólników spółek cywilnych i osobowych wpisanych do KRS. Poza tym przekazujemy tym osobom klauzulę informacyjną wg. wzoru. Zgoda na przetwarzanie nie może znajdować się w treści innego dokumentu. Wymaga się, aby była wyrażona wyraźnie i świadomie, co oznacza że zaleca się uzyskiwanie jej w formie odrębnego, pisemnego dokumentu chociaż dopuszcza się jej zamieszczenie np. w protokole, jako odrębny zapis wymagający odrębnego podpisu,

10. należy przywiązywać szczególną wagę do bezpieczeństwa nośników takich jak laptop czy pendrive. W przypadku ich zagubienia, bądź innej utraty – np. kradzież koniecznym jest powiadomienie osób, których dane znajdowały się nanośniku, o zdarzeniu niepożądanym a następnie w czasie 72 godzin od utraty powiadomienie UODO o zaistniałej sytuacji, jej opisanie i wskazanie czynności naprawczych jakie zamierza się wdrożyć aby zapobiec takiej utracie w przyszłości.

Sektor 3 Szczecin
centrum wspierania organizacji

www.sektor3.szczecin.pl
al. Wojska Polskiego 63, Szczecin, 91 350 82 99
biuro@sektor3.szczecin.pl
FB/sektor3szczecin

współfinansowane z budżetu
Województwa Zachodniopomorskiego