RODO. Podstawowe pojęcia

RODO odnosi się m.in. do takich pojęć jak administrator danych osobowych i podmiot przetwarzający dane osobowe.

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).

W poniższym opracowaniu bardziej skupiamy się na obowiązkach administratora danych – największa odpowiedzialność i największy trud wdrożenia RODO ciąży właśnie na administratorach.

Krok pierwszy – sprawdź czy RODO ma zastosowanie do 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

Czy każda organizacja pozarządowa będzie przetwarzała dane osobowe i będzie musiała stosować się do RODO? Trudno wyobrazić sobie organizację, która może stwierdzić, że nie przetwarza żadnych danych, a więc jej RODO nie dotyczy. Często dane po prostu muszą być zbierane – np. stowarzyszenie nie może funkcjonować nie przetwarzając danych swoich członków. Często też przetwarzanie danych jest obowiązkiem, który wynika z przepisów prawa (np. dane pracowników). Ale im mniej danych i mniejszy zakres czynności

wykonywanych w procesie przetwarzania danych tym mniej obowiązków dla organizacji w związku z ochroną danych.

Krok drugi – poznaj 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).

Zgodnie z RODO wszystkie zasady ochrony danych osobowych powinny być uwzględniane już na etapie projektowania usług czy urządzeń (często można się spotkać z angielskojęzycznym określeniem – *privacy by design*) oraz są stosowane domyślnie (*privacy by default*). To oznacza, że np. już w fazie pisania projektu NGO powinno mieć na uwadze zasady przetwarzania danych osobowych, czyli już wtedy trzeba się zastanowić czy dane będą zbierane, a jeśli tak, to mieć na uwadze wszystkie zasady ochrony danych.

Krok trzeci – ustal proces przetwarzania danych w organizacji – „mapowanie”

Na tym etapie trzeba się przyjrzeć „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.

Krok czwarty - 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 („ogarnięcia”) 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).

Krok piąty – ustal podstawę prawną 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 (krok dziewiąty). 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.

Więcej o podstawach prawnych przetwarzania danych osobowych można znaleźć w informacji: „Kiedy NGO może zbierać dane osobowe”. Warto też zapoznać się z webinarium dotyczącym zgody na przetwarzanie danych – są tam nie tylko informacje o zgodach, ale też o pozostałych przesłankach legalizacyjnych.

zobacz nagrania z webinarium:
4 rzeczy, które musisz wiedzieć o RODO
Wszystko o zgodzie na przetwarzanie danych osobowych

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.

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).

Krok szósty – przeprowadź ocenę (analizę) ryzyka i stwórz politykę bezpieczeństwa (art. 32 RODO)

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. O tym jak przeprowadzić ocenę ryzyka, z jakich etapów się składa można przeczytać w informacji: „Nowe zasady ochrony danych osobowych. Analiza ryzyka”. Zobacz też: „4 rzeczy, które musisz wiedzieć o RODO”.

Analiza ryzyka ma prowadzić do wdrożenia środków technicznych i organizacyjnych aby zapewnić odpowiedni poziom bezpieczeństwa (dostosowany do poziomu ryzyka). Te środki powinny zostać opisane w polityce bezpieczeństwa (po to, żeby osoby mające je stosować, wiedziały jak to robić – ponadto realizujemy też w ten sposób zasadę rozliczalności).

Krok siódmy - przeprowadź ocenę skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Pogłębiona analiza ryzyka (art. 35 RODO)

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.

Krok ósmy – powołaj inspektora ochrony danych osobowych (art. 37 RODO)

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.).

Krok dziewiąty – przestrzegaj praw osób, których dane są przetwarzane oraz wypełniaj obowiązek informacyjny (art. 12, 14 RODO)

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 m.in. o następujących okolicznościach:

1. kto przetwarza dane (dane i kontakt do administratora oraz do inspektora ochrony danych osobowych - jeśli inspektor został powołany);
2. cele przetwarzania danych osobowych;
3. podstawy prawne przetwarzania;
4. informacje, 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;
5. informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu;
6. jeżeli przetwarzanie odbywa się na podstawie prawnie uzasadnionych interesów administratora lub strony trzeciej, to należy te realizowane interesy wskazać;
7. informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją (odbiorcami danych może być np. ZUS, urząd skarbowy, ale też podmiot przetwarzający na zlecenie administratora, np. biuro księgowe, firma ewaluacyjna);
8. gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych do państwa trzeciego (poza Unię Europejską) lub organizacji międzynarodowej oraz warunkach tego przekazania;
9. okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
10. informacje o uprawnieniach w związku z przetwarzaniem danych, m.in. o:
    - dostępie do danych;
    - jeżeli przetwarzanie odbywa się na podstawie zgody, informacje o prawie do jej cofnięcia w dowolnym momencie;
    - informacje o prawie do wniesienia sprzeciwu, oraz żądania ograniczenia przetwarzania danych osobowych;
    - informacje o prawie wniesienia skargi do organu nadzorczego;
    - informacje o prawie do przenoszenia danych.

O obowiązku informacyjnym: „Organizacja zbiera dane osobowe i realizuje obowiązek informacyjny”.

Krok dziesiąty – miej świadomość kar (art. 58, 82, 83 RODO)

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.

10 kroków. Na zakończenie

Wdrożenie i przestrzeganie RODO, to proces, co też oznacza, że stale trzeba monitorować co z danymi się dzieje wprowadzać zabezpieczenia i w razie potrzeby je modyfikować.

Jak widać niektóre przedstawione powyżej kroki zazębiają się ze sobą – np. zasady przetwarzania danych z prawami osób, których dane dotyczą czy z analizą ryzyka – ale to tylko może pomóc w dobrym dostosowaniu procedur przetwarzania danych w organizacjach pozarządowych.

Jedna z trudności dotyczących RODO polega na tym, że materiały i opracowania dopiero powstają. Różni specjaliści mają różne interpretacje – dopiero jak zaczną zapadać wyroki w sprawie RODO powstanie orzecznictwo, czyli będzie więcej wiadomo jak interpretować przepisy.

Na wiele pytań nie ma więc jeszcze odpowiedzi, co nie znaczy, że organizacje pozarządowe są zwolnione z obowiązku stosowania RODO. RODO trzeba stosować od 25 maja 2018 r. Na początek skupmy się w naszej organizacji na tym co jest najlepiej rozpoznane i opisane – np. na zbieraniu danych pracowników, danych członków stowarzyszenia, odbiorców newslettera. W ten sposób będziemy uczyć się RODO (jego zasad i „filozofii") i systematycznie zwiększać wiedzę w tym zakresie.

Czym jest ZGODA na przetwarzanie danych osobowych?

Rozporządzenie zawiera definicję legalną zgody. Artykuł 4 punkt 11 RODO stanowi, że zgoda musi łącznie spełniać cztery warunki. Musi być:

1. dobrowolna;
2. konkretna;
3. świadoma;
4. jednoznaczne wyrażać wolę.

Z pomocą w wyjaśnieniu tych przesłanek przychodzi preambuła RODO i wytyczne Grupy Roboczej art. 29 *(odesłanie na końcu artykułu).*

Co oznacza dobrowolność ZGODY?

Dobrowolność zgody jest oceniana w kontekście sytuacyjnym. Jako punkt wyjścia należy przyjąć tezę, że jeżeli odmowa udzielania zgody wywoła negatywne konsekwencje dla odmawiającej osoby, to nie będzie to zgoda dobrowolna. Konsekwencje te mogą być różnorakie: od zwiększenia ceny produktu lub usługi, aż po brak możliwości uczestnictwa w projekcie.

W praktyce powstaje wątpliwość czy jeżeli zgoda jest bezpośrednio związana z daną usługą to odmowa jej wyrażenia jest negatywną konsekwencją. Przykładem może być zapisanie się na szkolenie, które wymaga podania danych do wystawienia faktury. W takiej sytuacji trzeba zwrócić uwagę na dwa aspekty. **Po pierwsze** czy istnieje inna przesłanka niż zgoda, na podstawie której dane osobowe mogą być przetwarzane. Trzeba przeanalizować artykuł 6 RODO. W tym przykładzie (zapisanie się na szkolenie) będzie to przesłanka zawarta w art. 6 ust. 1 lit. b: „przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą". W takim wypadku nie jest konieczne pozyskiwanie zgody. Co więcej nie powinno się tego robić, na co wprost wskazują wytyczne Grupy Roboczej art. 29. **Po drugie** należy zbadać czy ilość pozyskiwanych danych jest minimalna dla realizacji celu. W przypadku szkolenia może być to imię, nazwisko i e-mail lub inny środek kontaktu (raczej nie ma potrzeby pozyskiwania innych danych, np. adresu zamieszkania).

Badając dobrowolność szczególną uwagę należy zwrócić na sytuacje, w których nie ma równowagi między administratorem i osobą, od której pozyskiwane są dane. Taka sytuacja może np. wystąpić podczas pracy z grupami defaworyzowanymi.

Warto również pamiętać, że dobrowolność zgody jest związana z jej formą. Kiedy, przykładowo, uczestnictwo w wycieczce organizowanej przez NGO jest warunkowe - udział w wycieczce zależy od udzielenia zgody na przetwarzanie danych dla celów marketingowych - to w takim przypadku zgoda nie będzie uznawana za dobrowolną. Aby spełnić ten warunek (dobrowolności) konieczne jest takie sformułowanie treści zgody, aby brak jej wyrażenia nie uniemożliwiał uczestnictwa w wydarzeniu (zgoda na zbieranie danych, koniecznych do zorganizowania wyjazdu, oddzielona od zgody na przetwarzanie danych do celów marketingowych).

Co oznacza konkretność ZGODY?

Konkretność zgody odnosi się do jej precyzyjnego sformułowania. Zgoda powinna wprost wskazywać cele, w jakich dane będą przetwarzane. Za konkretną nie jest uważana zgoda, która jest częścią umowy, a także zgoda będąca częścią regulaminów świadczenia usług.

Możliwość wyrażenia zgody na przetwarzanie danych osobowych powinna być wyraźnie rozdzielona od treści normatywnej umów lub innych aktów.

Co oznacza, że ZGODA ma być świadoma?

Zgoda jest świadoma, jeśli osoba, która ją wyraża zostanie poinformowana:

- kto będzie przetwarzał jej dane osobowe,
- w jakim celu będą przetwarzane,
- jakie uprawnienia jej przysługują.

Kiedy wyrażenie woli dotyczące ZGODY jest jednoznaczne?

Jednoznaczne wyrażenie woli oznacza, że **dana osoba będzie musiała podjąć działanie** w celu wyrażenia zgody. Niedopuszczalne jest zatem przyjęcie, że milczenie lub brak działania oznacza zgodę. Podobnie należy ocenić sytuację, w której zgoda na przetwarzanie danych jest domyślnie zaznaczona w formularzu internetowym.

Milczenie lub brak działania nie oznacza zgody. Zgoda nie może być również opcją domyślną (np. domyślnie odznaczona w formularzu internetowym).

Sposób złożenia zgody

Według RODO zgoda może być złożona w innej formie niż pisemna. Dopuszczalna jest forma elektroniczna (np. poprzez e-mail, SMS, portale społecznościowe czy komunikatory). Dopuszczalna jest również forma dokumentowa w rozumieniu art. 773 Kodeksu cywilnego (o formie dokumentowej pisaliśmy w informacji: Czy można zerwać umowę SMS-em?). W pewnych wypadkach możliwa jest zgoda w formie ustnej, ale będzie ona miała charakter wyjątkowy.

Skutecznej zgody będzie mogła udzielić osoba z pełną zdolnością do czynności prawnych. Wyjątkiem są sytuacje dotyczące usług społeczeństwa informacyjnego – chodzi o umowy i inne usługi, które są zawierane lub przekazywane online. Dotyczy to np. gier online, świadczenia usług w chmurze, czy sprzedaży przez internet. RODO przesuwa tu granicę na 16 lat, tzn. przetwarzanie danych osobowych dziecka, które ukończyło 16 lat jest w przypadku usług społeczeństwa informacyjnego zgodne z prawem, ale zezwala też państwom członkowskim na obniżenie granicy wieku. Przetwarzanie danych młodszych osób będzie możliwe wyłącznie po uzyskaniu uprzedniej zgody przedstawiciela ustawowego, albo po niezwłocznym potwierdzeniu przez przedstawiciela zgody wyrażonej przez taką osobę.

Co powinna zawierać ZGODA?

Nie ma żadnego wzoru zgody na przetwarzanie danych osobowych. W wytycznych Grupy Roboczej art. 29 można znaleźć informację, że zgoda powinna zawierać co najmniej:

1. tożsamość administratora – dane podmiotu, który decyduje o celach i zasadach przetwarzania danych. W kontekście NGO będą to dane podmiotu, np. stowarzyszenia lub fundacji, a nie dane zarządu, ponieważ ten działa w imieniu osoby prawnej;
2. cel każdej operacji przetwarzania, dla której prosi się o zgodę – tu wskazujemy po co nam dane określonej osoby: np. dla celów statystycznych, marketingu swoich usług lub wysyłania informacji o zbieraniu 1%;
3. jakie dane będą zbierane i wykorzystywane – wskazujemy te, które osoba dostarcza bezpośrednio (np. wpisując do formularza swoje imię i nazwisko) oraz pozyskiwane pośrednio (np. adres IP);
4. informacje o prawie do wycofania zgody *(o wycofaniu / odwołaniu zgody piszemy poniżej);*
5. informacje na temat wykorzystywania danych do decyzji opartych jedynie na zautomatyzowanym przetwarzaniu, w tym profilowania – jeżeli przetwarzamy dane w ten sposób to należy poinformować o tym osobę, która nam dane przekazuje;

6. jeżeli zgoda dotyczy przekazywania - informacje na temat możliwych zagrożeń związanych z przekazywaniem danych do krajów trzecich. Tę informację należy przekazać tylko w wypadku, gdy brak jest decyzji Komisji Europejskiej stwierdzającej odpowiedni stopień ochrony w kraju, do którego dane są przekazywane.

Odwołanie zgody

RODO w art. 7 ust. 3 wskazuje, że zgoda może być odwołana w każdym momencie. Wycofanie zgody musi być równie łatwe jak jej wyrażenie. Nie można nakładać negatywnych konsekwencji z tytułu cofnięcia zgody.

Odwołanie wywołuje skutek natychmiastowy, czyli od momentu otrzymania oświadczenia woli w tym zakresie nie można przetwarzać danych osoby. Odwołanie nie wywołuje skutków wstecz. To znaczy, że operacje przetwarzania danych, które były dokonane w czasie gdy zgoda obowiązywała, są zgodne z prawem.

Każda zgoda na przetwarzanie danych osobowych, którą organizacja pozarządowa pozyska od danej osoby, może zostać odwołana.

Ważność już pozyskanych zgód po wejściu w życie RODO

Po uchwaleniu RODO powstały wątpliwość czy zgody pozyskane przed 25 maja 2018 r. zachowają dalej swoją ważność. Wątpliwości wynikają m.in. z faktu, że poprzedzające RODO przepisy nie nakładały obowiązku informowania o prawie do cofnięcia zgody - a jest to wymagane przez RODO. Niepewność rozwiało zarówno stanowisko Grupy Roboczej art. 29, jak i opinia polskiego Generalnego Inspektora Ochrony Danych Osobowych. Zgodnie z nimi stare zgody, co do zasady, utrzymają ważność. **Należy jednak zbadać czy były one pozyskane zgodnie z zasadami dobrowolności, konkretności, świadomości i jednoznacznego wyrażenia zgody**. Ponadto jeżeli zmieni się cel przetwarzania zebranych danych lub potrzebne będzie pozyskanie zgody na nowo z innych powodów, konieczne będzie zadośćuczynienie wszystkim obowiązkom wynikającym z RODO.

Niemal każda NGO zbiera lub będzie zbierać dane osobowe. W związku z tym musi stosować się do RODO i wynikających z niego obowiązków. Jednym z nich jest obowiązek informacyjny. Kogo i o czym musimy informować?

25 maja 2018 r. zacznie obowiązywać Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. (RODO). Będzie dotyczyło ono również przetwarzania danych przez organizacje pozarządowe. Od kilku miesięcy przypominamy o tym w portalu ngo.pl.

Zobacz: zebrane informacje dotyczące RODO

Osoby, których dane są zbierane, mają swoje prawa. Przede wszystkim muszą mieć świadomość, kto i do jakich celów zbiera o nich dane, a także jakie to są dane i jak długo będą przechowywane. Mają też m.in. możliwość wglądu w swoje dane czy wyrażenia sprzeciwu – żądania, aby dany podmiot przestał zbierać o nich informacje. Jednym z bardziej znaczących przejawów tego, że osoba, której dane dotyczą decyduje o tym, co można z nimi robić są zgody, o których pisaliśmy wcześniej.

Niezależnie od tego czy organizacja pozarządowa zbiera dane osobowe na podstawie zgód, czy też na innych podstawach (przesłankach legalizujących) – czy pozyskuje dane bezpośrednio od osób, czy z innych źródeł – musi realizować obowiązek informacyjny.

Poniżej przedstawiamy jeden z rozdziałów przygotowywanej przez portal NGO.PL publikacji dotyczącej stosowania RODO przez organizacje pozarządowe. Rozdział ten dotyczy właśnie obowiązku informacyjnego. Całość przygotowywanego przez NGO.PL podręcznika dostępna będzie w formacie PDF już wkrótce!

Obowiązek informacyjny ciąży na administratorze danych osobowych. Zgodnie z zasadą rozliczalności musi on udowodnić, że przekazał informacje wymagane przez RODO osobom, których dane są przetwarzane.

Kolejne zasady rzetelnego i przejrzystego przetwarzania wymagają, by osoba, której dane dotyczą, była informowana o prowadzeniu operacji przetwarzania i o jej celach. Administrator powinien podać osobie, której dane dotyczą, wszelkie inne informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania, uwzględniając konkretne okoliczności i konkretny kontekst przetwarzania danych osobowych (motyw 60 RODO).

Zasadniczym celem obowiązku informacyjnego jest budowanie świadomości osoby, której dane dotyczą o procesie przetwarzania jej danych oraz o związanych z nim prawach w celu ochrony autonomii informacyjnej.

Informacje powinny być przekazane w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem – w szczególności gdy informacje są kierowane do dziecka. Informacje takie można opatrzyć standardowymi znakami graficznymi, które w widoczny, zrozumiały i czytelny sposób przedstawią sens zamierzonego przetwarzania. Informacje te można przekazać na piśmie lub w inny sposób (również elektronicznie).

Informacje są zasadniczo przekazywane bezpłatnie. RODO wprowadza wyjątek od tej zasady, jeżeli żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter. Wówczas administrator może pobrać opłatę lub odmówić podjęcia działań w związku z żądaniem. Należy pamiętać, że obowiązek wykazania, że żądanie ma ewidentnie nieuzasadniony lub nadmierny charakter, spoczywa na administratorze.

Zakres informacji oraz sposób ich udzielenia zależy od tego, jak administrator pozyskał dane osobowe, które przetwarza – czy dane uzyskał bezpośrednio od osoby, której dane dotyczą (art. 13 RODO), czy z innych źródeł (art. 14 RODO).

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

Z pozyskiwaniem danych osobowych od osoby, której dane dotyczą mamy do czynienia w przypadku, gdy osoba ta sama, świadomie dostarcza administratorowi swoje dane.

Zapamiętaj: W przypadku pozyskiwania danych osobowych bezpośrednio obowiązek informacyjny aktualizuje się w momencie gromadzenia tych danych – czyli informacje muszą być przekazane osobie w momencie, kiedy przekazuje ona dane. Informacje takie mogą być połączone ze zgodą lub ujęte w formie dodatkowej klauzuli informacyjnej.

Pomimo że katalog informacji, które administrator jest zobowiązany podać jest szeroki, administrator nie zawsze podaje wszystkie informacje.

Minimalny zakres informacji, które podaje administrator obejmuje:

a. tożsamość i dane kontaktowe administratora;
b. cele oraz podstawę prawną przetwarzania danych;
c. okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
d. informacje o prawie do żądania od administratora:
    - dostępu do danych osobowych dotyczących osoby, której dane dotyczą;
    - sprostowania;
    - usunięcia;
    - ograniczenia przetwarzania;
    - o prawie do wniesienia sprzeciwu wobec przetwarzania;
    - o prawie do przenoszenia danych;
    - o prawie wniesienia skargi do organu nadzorczego.

Zapamiętaj: Są to informacje podstawowe, które administrator jest zobowiązany podać zawsze, każdej osobie, której dane przetwarza.

Ponadto administrator podaje następujące informacje (jeśli go dotyczą):

1. tożsamość i dane kontaktowe swojego przedstawiciela;
2. dane kontaktowe inspektora ochrony danych;
3. oświadczenie o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub nie przez Komisję Europejską odpowiedniego stopnia ochrony danych osobowych w państwie trzecim lub w przypadku przekazania danych wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych;
4. prawnie uzasadnione interesy administratora lub osoby trzeciej, jeśli przetwarzanie odbywa się na tej podstawie;
5. o odbiorcach lub o kategoriach odbiorców danych osobowych;
6. o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;
7. 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;

8. o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, oraz istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą;
9. jeżeli administrator planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym te dane zostały pozyskane, przed takim dalszym przetwarzaniem informuje on osobę, której dane dotyczą, o tym innym celu oraz udziela jej wszelkich innych stosownych informacji.

Administrator ma obowiązek podać wszystkie powyższe informacje – jeśli go dotyczą. Przykładowo: kiedy administrator powołał inspektora ochrony danych, to musi podawać informacje o jego danych kontaktowych.

Zapamiętaj: Jeśli administrator planuje przetwarzać dane w innym celu aniżeli zostały one pierwotnie zebrane, ma obowiązek powiadomić o tym osobę, której dane dotyczą, zanim dokona takiego dalszego przetwarzania w zmienionym celu.

Wyjątek od obowiązku informacyjnego – administrator nie musi udzielać osobie, której dane dotyczą informacji, którymi osoba ta już dysponuje.

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

Z pozyskiwaniem danych osobowych w sposób inny niż od osoby, której dotyczą mamy do czynienia, gdy administrator nie pozyskuje danych bezpośrednio. Np. organizacja kupuje bazę danych z nazwiskami osób, do których zamierza wysłać mailing promujący 1%

W takim przypadku udzielenie informacji w momencie pozyskiwania danych jest niemożliwe. Trzeba więc przekazać informacje w rozsądnym terminie – **najpóźniej w ciągu miesiąca** od pozyskania danych. Jeżeli dane osobowe mają służyć do komunikacji z osobą, administrator spełnia obowiązek informacyjny najpóźniej przy pierwszej takiej komunikacji, np. wysyłając maila do takiej osoby. Natomiast w sytuacji, kiedy administrator planuje ujawnić dane osobowe innemu odbiorcy, spełnia obowiązek informacyjny najpóźniej przy ich pierwszym ujawnieniu.

Zakres podawanych informacji w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą nie różni się znacznie od zakresu informacji, które administrator zobowiązany jest podać w przypadku pozyskiwania danych osobowych bezpośrednio.

Administrator podaje więc:

- informacje wskazane powyżej – opisane w punktach: a, b, c, d oraz 1, 2, 3, 4, 5, 6 i 8

- **oraz dodatkowo** informuje o:
  - kategoriach odnośnych danych osobowych – czyli informacje o rodzaju przetwarzanych danych (np. imię i nazwisko, adres, data urodzenia, ponieważ możemy posiadać ich mniej niż podmiot, od którego dane pozyskaliśmy);

- źródle pochodzenia danych osobowych, a gdy ma to zastosowanie – czy pochodzą one ze źródeł publicznie dostępnych (np. z KRS).

Administrator jest zwolniony z obowiązku przekazywania informacji jeśli:

- osoba, której dane dotyczą, dysponuje już tymi informacjami;
- jeżeli udzielenie takich informacji:
  - okazuje się niemożliwe lub
  - wymagałoby niewspółmiernie dużego wysiłku;
  - może uniemożliwić lub poważnie utrudnić realizację celów takiego przetwarzania;

  W wypadkach wskazanych powyżej administrator podejmuje odpowiednie środki, by chronić prawa i wolności oraz prawnie uzasadnione interesy osoby, której dane dotyczą.

- pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator, przewidującym odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą;
- dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianym w prawie Unii lub w prawie państwa członkowskiego, w tym ustawowym obowiązkiem zachowania tajemnicy.