RODO w organizacji pozarządowej.

Od 25 maja 2018 r. zaczęło obowiązywać unijne Ogólne Rozporządzenie o Ochronie Danych Osobowych (RODO), które zastąpiło przepisy dotychczasowej ustawy o ochronie danych osobowych. Przepisy RODO dotyczą wszystkich, którzy przetwarzają dane osobowe, w tym również organizacji pozarządowych.

Europejskie rozporządzenie o ochronie danych nie wskazuje wprost żadnych konkretnych sposobów zabezpieczeń danych osobowych ani dokumentów jakie trzeba posiadać, aby wypełnić obowiązki związane z RODO. To oznacza, że każda organizacja pozarządowa musi samodzielnie opracować dokumenty i procedury ochrony danych – stosując podejście oparte na szacowaniu ryzyka i w oparciu o zasady wynikające z RODO.

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).

RODO w NGO – jak się przygotować?

KROK 1. Sprawdź czy RODO ma zastosowanie do twojej organizacji.

- 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.

KROK 2. 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).

KROK 3. Ustal proces przetwarzania danych w organizacji.

- 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.

KROK 4. 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.

KROK 5. Ustal podstawę prawną przetwarzania danych osobowych.

- 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.

KROK 6. 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.

- 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 7. Przeprowadź ocenę 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.

KROK 8. Powołaj inspektora 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.

KROK 9. Przestrzegaj 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).

KROK 10. Miej 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.

Postępowanie dotyczące ochrony danych osobowych w organizacji pozarządowej zależy m.in. od tego czyje, jakie dane są przetwarzane, jakie czynności są wykonywane przy przetwarzaniu, komu są przekazywane, jakie jest ryzyko utraty danych, ich wycieku i jaki to może mieć konsekwencje dla osób których dane dotyczą. Dlatego w różnych organizacjach zasady ochrony danych będą różnie wyglądały.

Na wiele pytań nie ma jeszcze odpowiedzi, co nie znaczy, że organizacje pozarządowe są zwolnione z obowiązku stosowania RODO. RODO trzeba stosować od 25 maja 2018 r.

Przydatne linki i materiały:

- Podstawa prawna: 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 (zwane również RODO).
- Strona Urzędu Ochrony Danych Osobowych - https://uodo.gov.pl
- Poradnik RODO Fundacji Panoptykon - https://panoptykon.org/poradnik-RODO
- Informacje o RODO na portalu ngo.pl - http://poradnik.ngo.pl/wiadomosci/podobne/2176884.html

Opracowała: Karolina Furmańska
Doradca dla organizacji pozarządowych

Opracowano na podst. artykułu „Ochrona danych osobowych w ngo. RODO w organizacji pozarządowej w 10 krokach”
źródło: http://poradnik.ngo.pl/ochrona-danych-osobowych-w-NGO