

Ochrona danych osobowych w NGO – proces legislacji i wdrożenia RODO



25 maja 2018 r. wchodzi w życie nowe rozporządzenie o ochronie danych osobowych – RODO, czyli Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (inaczej ogólne rozporządzenie o ochronie danych osobowych - RODO). Dla wielu organizacji pozarządowych dostosowanie się do jego postanowień to poważne i niełatwe wyzwanie. Zmiany obejmują dostosowanie obecnej dokumentacji do wymogów RODO ale też nowości jak powołanie Prezesa UODO, Inspektora ochrony danych osobowych i wprowadzenie rejestrów czynności przetwarzania. Jaki udział w systemie ochrony danych osobowych znajdą organizacje pozarządowe?

Nowy urząd ochrony danych osobowych

W miejsce Generalnego Inspektora Ochrony Danych Osobowych (GIODO), instytucji która od 20 lat zajmuje się w Polsce ochroną danych, powstanie Urząd Ochrony Danych Osobowych (UODO). Na czele urzędu będzie stał Prezes. Nowy organ ochrony danych osobowych będzie miał znacznie szerszy zakres uprawnień niż dzisiejszy GIODO, w tym szerszy zakres uprawnień kontrolnych. Będzie też mógł nakładać znacznie wyższe kary. Jego powołanie i funkcjonowanie określi polska ustawa o ochronie danych osobowych, która właśnie jest na etapie procedowania przez Senat. Postępowanie przed PUODO będzie prowadzone według przywołanej powyżej ustawy oraz znowelizowanego Kodeksu postępowania administracyjnego. Postępowanie to będzie jednoinstancyjne, zatem od decyzji Prezesa UODO będzie przysługiwać od razu skarga do sądu. Przepisy nie przewidują zażaleń na postanowienia jako odrębnych środków odwoławczych, o ma na celu przyspieszyć postępowanie.

Udział organizacji pozarządowych w RODO

Projekt ustawy przewiduje aktywną rolę NGO w działaniach przed Prezesem UODO. Organizacja społeczna może występować z żądaniem wszczęcia postępowania lub dopuszczenia jej do udziału w postępowaniu, jeżeli jest to uzasadnione celami statutowymi tej organizacji i gdy przemawia za tym interes osoby, której prawa zostały naruszone. NGO będą więc mogły wspierać osoby poszkodowane w dochodzeniu ich praw. Projekt przewiduje także powołanie **Rady do Spraw Ochrony Danych Osobowych**, której członków zgłaszają m.in. fundacje i stowarzyszenia wpisane do KRS, których clem statutowym jest działalność na rzecz ochrony danych osobowych.

Poufność w NGO

Organizacje, które prowadzą działalność gospodarczą będą mogły skorzystać z możliwości zastrzeżenia poufności dokumentów przekazywanych Prezesowi Urzędu. Będzie to dotyczyło informacji chronionych tajemnicą przedsiębiorstwa. Ma to zapobiec wyciekowi informacji i chronić ważne zasoby organizacji pozarządowej jako przedsiębiorcy.

Zasady kontroli

Projekt ustawy reguluje zasady prowadzenia kontroli przez Prezesa UODO. Postępowanie kontrolne może być prowadzone zgodnie z zatwierdzonym przez Prezesa Urzędu planem kontroli, bądź poza planem, na podstawie uzyskanych przez Prezesa Urzędu informacji albo przeprowadzonych analiz. W pierwszym przypadku będzie dotyczyło wytypowanych wcześniej kategorii podmiotów np. przedszkoli czy szkół językowych. W drugim mogą być to kontrole ad hoc - np. na podstawie doniesień medialnych lub donosu. Kontrola nie może przekroczyć 30 dni. Urzędnicy dostaną szerokie uprawnienia, np.: prawo wstępu na grunt oraz do budynków, lokali lub innych pomieszczeń w godz. 6-22, wglądu do wszelkich dokumentów i wszelkich informacji mających bezpośredni związek z przedmiotem kontroli oraz przeprowadzania oględzin urządzeń, nośników i systemów informatycznych lub teleinformatycznych służących do przetwarzania danych. Ponadto będą mogli żądać złożenia pisemnych lub ustnych wyjaśnień oraz wzywać i przesłuchiwać świadków.

Odpowiedzialność cywilna i karna, kary

Rozporządzenie unijne przewiduje maksymalną karę za naruszenie przepisów o ochronie danych osobowych w wysokości 20.000.000 EUR lub 4 % „całkowitego rocznego światowego obrotu” przedsiębiorstwa z poprzedniego roku oraz 100.000 zł dla instytucji publicznych. Projekt ustawy oprócz kar nakładanych przez Prezesa UODO przewiduje sankcje cywilne i karne. W przypadku sankcji cywilnych zastosowanie będą miały ogólne zasady Kodeksu cywilnego. To znaczy, że granicą odpowiedzialności jest wyrządzona szkoda. Należy jednak pamiętać, że dane osobowe są chronione jako dobra osobiste. Dlatego sąd może przyznać zadośćuczynienie pieniężne niezależnie od innych środków potrzebnych do usunięcia skutków naruszenia (np. nakazania publikacji przeprosin). Dodatkowo każda osoba, której prawa zostały naruszone, może żądać, zaniechania tego działania, a także może żądać ażeby ten, kto dopuścił się naruszenia, dopełnił czynności potrzebnych do usunięcia jego skutków. Inaczej mówiąc nie tylko PUODO, ale też sąd może zakazać przetwarzania danych osobowych. W projekcie ustawy przewidziane są też przepisy karne. Penalizowane są: utrudnianie lub udaremnianie kontroli, zagrożonym karą pozbawienia wolności do lat dwóch (art. 108 projektu ustawy o ochronie danych osobowych z dnia 10 maja 2018 r.), przetwarzanie danych bez podstawy prawnej, które będzie zagrożone karą do dwóch lat pozbawienia wolności (art. 107) i przetwarzanie danych szczególnych bez podstawy prawnej – do trzech lat pozbawienia wolności.

Jakie dane osobowe może posiadać organizacja?

Organizacje pozarządowe mogą posiadać różne zbiory danych, m.in. mogą to być dane osobowe: członków, pracowników, podopiecznych i beneficjentów (np. uczestników warsztatów terapii zajęciowej, osób korzystających z porad prawnych, osób oczekujących na adopcję dziecka itd.), często mogą to być dane „wrażliwe”, wolontariuszy, darczyńców, osób, które przekazały danej organizacji pożytku publicznego 1%, partnerów i współpracowników.

Obowiązki związane z przetwarzaniem danych osobowych

Biorąc pod uwagę niejasne kryteria i nieostre zwroty z Rozporządzenia nie zawsze łatwo zinterpretować granice obowiązków ADO. Przetwarzanie danych osobowych, zarówno w systemie informatycznym jak i w tradycyjnych papierowych zbiorach danych, nakłada na

organizację (jako administratora) różne obowiązki, m.in. obowiązek organizacyjnego i technicznego zabezpieczenia danych, obowiązek informacyjny, obowiązek przestrzegania zasad: rzetelności, minimalizmu, rozliczalności, wykorzystywania danych jedynie do czasu osiągnięcia wyznaczonego celu, prowadzenia dokumentacji, zapewnienia kontroli nad tym, jakie dane osobowe są zbierane i komu są przekazywane, prowadzenia ewidencji osób upoważnionych do przetwarzania danych itp. ale też te kontrowersyjne – ustalenia skali przetwarzania, analizy skutków przetwarzania, szacowania ryzyka przetwarzania. Przydatne w tym zakresie mogą się okazać wytyczne roboczej grupy art. 29 publikowane na stronie www.giodo.gov.pl.

Zgody w NGO

Zgoda osoby, której dane posiada organizacja, jest jednym z warunków dopuszczalności przetwarzania danych. Nie jest konieczna jeżeli przetwarzanie jest niezbędne do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa, np. osoba przekazała darowiznę na rzecz organizacji, organizacja przetwarza jej dane do celów sprawozdawczych przed urzędem skarbowym; w celu realizacji umowy, np. umowy pracownicze, umowy cywilnoprawne; jeżeli przetwarzanie jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego; czy też w celu wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych.

„Gotowi na RODO”

Kampania informacyjna Narodowego Instytutu Wolności – Centrum Rozwoju Społeczeństwa Obywatelskiego i Generalnego Inspektora Ochrony Danych Osobowych dotycząca wdrożenia RODO.

W zakresie relacji NGO z RODO warto również wspomnieć o nowym projekcie Narodowego Instytutu Wolności, który we współpracy z Generalnym Inspektorem Ochrony Danych Osobowych uruchamia kampanię informacyjną pn. „Gotowi na RODO”, która wyjaśnia zachodzące zmiany i uczy, jak stosować nowe przepisy w praktyce (www.rodod.niw.gov.pl).