Warszawa, 26.05.2021 r.

Czy powinienem wyznaczyć Inspektora Ochrony Danych?

Zacznijmy od przepisów

Rozporządzenie 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 (RODO) określa przypadki, w których wyznaczenie Inspektora Ochrony Danych (IOD) przez Administratora Danych Osobowych (ADO) jest obowiązkowe.

„Przetwarzania dokonuje organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości"

Każdy podmiot, wskazany w art. 9 pkt 1–14 ustawy z 27.08.2009 r. o finansach publicznych, a także podmiot, któremu podmiot publiczny zlecił realizację zadania publicznego, związanego z przetwarzaniem danych osobowych, zobowiązany jest do wyznaczenia IOD. Dotyczy to oczywiście również sądów, ale wyłącznie w przypadku przetwarzania danych innych niż związanych ze sprawowaniem przez sądy wymiaru sprawiedliwości, czyli obszaru spraw sądowych, wyroków, itp.

„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"

Główna działalność ADO to ta, która jest celem powstania organizacji. Przykładem może być firma zajmująca się doradztwem personalnym. Głównym celem jej działalności jest rekrutacja pracowników dla swoich klientów i związane z tym zyski. Główną działalnością w tym przypadku nie będzie rekrutacja i zatrudnienie pracowników na własne potrzeby, czyli np. rekrutera czy księgowej, ale rekrutacja księgowej dla klienta już takim celem będzie.

Jeżeli chodzi o monitorowanie osób to motyw 24 RODO wskazuje, że mogą to być wszelkie formy profilowania, obserwowania osób fizycznych w Internecie, zwłaszcza w celu prognozowania jej osobistych preferencji, zachowań i postaw. Grupa Robocza Art. 29 wskazuje jednak, że monitorowania nie powinno się ograniczać jedynie do środowiska online i śledzenie w sieci powinno być traktowane jedynie jako jeden z przykładów monitorowania zachowań osób, których dane dotyczą.

Pamiętajmy tu jednak, że przepis ten (czyli obowiązek wyznaczenia IOD) dotyczy regularnego i systematycznego monitorowania. Nie znajdziemy w przepisach o ochronie danych osobowych definicji regularności czy systematyczności, jednak i w tym przypadku wypowiedziała się Grupa Robocza Art. 29:

- „regularne" jako jedno lub więcej z następujących pojęć:
    - stałe albo występujące w określonych odstępach czasu przez ustalony okres,
    - cykliczne albo powtarzające się w określonym terminie,
    - odbywające się stale lub okresowo.
- „systematyczne" jako jedno lub więcej z następujących pojęć:
    - występujące zgodnie z określonym systemem,
    - zaaranżowane, zorganizowane lub metodyczne,
    - odbywające się w ramach generalnego planu zbierania danych,
    - przeprowadzone w ramach określonej strategii.

Grupa Robocza Art. 29 wskazała również konkretne przykłady działań, które mogą stanowić regularne i systematyczne monitorowanie osób. Są to m. in.: obsługa sieci telekomunikacyjnej; świadczenie usług telekomunikacyjnych; przekierowywanie poczty elektronicznej; działania marketingowe oparte na danych; profilowanie i ocenianie dla celów oceny ryzyka (na przykład dla celów oceny ryzyka kredytowego, ustanawiania składek ubezpieczeniowych, zapobiegania oszustwom, wykrywania prania pieniędzy); śledzenie lokalizacji, na przykład przez aplikacje mobilne; programy lojalnościowe; reklama behawioralna; monitorowanie danych dotyczących zdrowia i kondycji fizycznej za pośrednictwem urządzeń przenośnych; monitoring wizyjny; urządzenia skomunikowane np. inteligentne liczniki, inteligentne samochody, automatyka domowa.

Jeżeli chodzi o dużą skalę, to w tym przypadku również możemy sięgnąć do motywów RODO, a dokładnie do 91, który wskazuje, że operacje przetwarzania na „dużą skalę" to operacje, które służą do przetwarzania znacznej ilości danych osobowych na szczeblu regionalnym, krajowym lub ponadnarodowym, które mogą wpłynąć na dużą liczbę osób, których dane dotyczą, oraz które mogą

powodować wysokie ryzyko. Nie jest możliwe wskazanie konkretnej wartości, np. liczby osób, których dane dotyczą, która określiłaby konkretnie „dużą skalę".

Grupa Robocza Art. 29 zaleca, aby przy określaniu rozmiaru skali uwzględnić:

- liczbę osób, których dane dotyczą – konkretna liczba albo procent określonej grupy społeczeństwa,
- zakres przetwarzanych danych osobowych,
- okres, przez jaki dane są przetwarzane,
- zakres geograficzny przetwarzania danych osobowych.

Grupa Robocza Art. 29 podała nawet przykłady przetwarzania, które można zaliczyć do przetwarzania danych na „dużą skalę":

- przetwarzanie danych pacjentów przez szpital w ramach prowadzonej działalności (z wyłączeniem przetwarzanie danych pacjentów, dokonywane przez pojedynczego lekarza),
- przetwarzanie danych dotyczących podróży osób korzystających ze środków komunikacji miejskiej (np. śledzenie za pośrednictwem kart miejskich),
- przetwarzanie danych geolokalizacyjnych klientów w czasie rzeczywistym przez wyspecjalizowany podmiot na rzecz międzynarodowej sieci fast food do celów statystycznych,
- przetwarzanie danych klientów przez banki albo ubezpieczycieli w ramach prowadzonej działalności,
- przetwarzanie danych do celów reklamy behawioralnej przez wyszukiwarki,
- przetwarzanie danych (dotyczących treści, ruchu, lokalizacji) przez dostawców usług telefonicznych lub internetowych.

„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"

Główną działalność oraz dużą skalę omówiliśmy już powyżej, więc tutaj skupimy się na drugiej części tego przepisu.

Definicje szczególnych kategorii danych osobowych oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa zostały określone odpowiednio w Art. 9 i 10 RODO.

W związku z tym, gdy główną działalnością administratora jest przetwarzanie na dużą skalę 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, wyroków skazujących oraz naruszeń prawa, administrator będzie zobowiązany do wyznaczenia Inspektora Ochrony Danych.

Niestety mimo zastosowania w tym przepisie słów „oraz" i „i" nie możemy tu założyć, że przepis ten będzie nas dotyczył wyłącznie w przypadku przetwarzania szczególnych kategorii danych osobowych **oraz** danych osobowych dotyczących wyroków skazujących **i** naruszeń prawa.

Gdy przepisy konkretnie nie nakładają obowiązku wyznaczenia IOD

Nawet gdy przepisy nie nakładają konkretnego obowiązku wyznaczenia IOD lub gdy nie jesteśmy do końca pewni czy obowiązek dotyczy naszej organizacji czy też nie, zaleca się rozważenie dobrowolnego wyznaczenia takiej osoby, chociażby z niżej wymienionych powodów:

- na tzw. wszelki wypadek, bo gdyby się okazało, że jednak mamy taki obowiązek (np. źle doszacowaliśmy „dużą skalę"), to nie ma problemu kary, która grozi za jego niepowołanie (Art. 83 ust. 4 lit. a),
- ułatwienia przestrzegania przepisów w organizacji w postaci wyznaczenia konkretnej osoby odpowiedzialnej za **pomoc w ich przestrzeganiu** (**odpowiedzialność** za przetwarzanie danych osobowych zgodnie z przepisami zawsze będzie spoczywać na ADO).

Oczywiście ADO może wyznaczyć osobę odpowiedzialną za nadzorowanie tematu ochrony danych osobowych w swojej organizacji i niekoniecznie musi się to wiązać z wyznaczeniem IOD. Samo wyznaczenie IOD, czy gdy jest taki obowiązek, czy gdy jest to dobrowolne, wiąże się z obowiązkiem spełnienia wszystkich obowiązków, o których mowa w Art. 37 RODO.

Maria Lothamer, Wiceprezes Zarządu iSecure Sp. z o.o.