Pierwsza kara finansowa RODO – czy jest się czego obawiać?

W dniu 15 marca br., Edyta Bielak-Jomaa, prezes Urzędu Ochrony Danych Osobowych, wydała decyzję o nałożeniu kary w wysokości blisko 1 mln zł za nieprawidłowe przetwarzanie danych osobowych oraz nakazała dopełnić obowiązku informacyjnego w terminie 3 miesięcy od daty otrzymania decyzji. Tak dotkliwa sankcja spowodowała, że wielu przedsiębiorców zaczęło zastanawiać się, czy liczba nakładanych kar finansowych zacznie rosnąć? Pojawiły się też pytania: czy był to najodpowiedniejszy środek penalizacji, a jeśli tak - to czy był proporcjonalny?

W tym miejscu należy przypomnieć, że obok kar finansowych, będących pewnego rodzaju ostatecznością, organ ochrony danych dysponuje również innymi sankcjami, które służą do zwrócenia uwagi przedsiębiorców na występujące naruszenia. To szereg uprawnień naprawczych w postaci wydania ostrzeżeń, upomnień czy nakazania określonych zachowań (jak np. naprawienie szkody czy dopełnienie obowiązku informacyjnego).

Kar nakładanych przez UODO będzie coraz więcej

Jeśli wziąć pod uwagę powyższe, jak również fakt, że do UODO wpłynęło do tej pory już około 3000 skarg na nieprawidłowe przetwarzanie danych osobowych – na pierwsze z pytań przytoczonych na wstępie niniejszego artykułu należy odpowiedzieć twierdząco. Możemy spodziewać się wzmożonej aktywności UODO w zakresie penalizacji, w tym nakładania kar finansowych.

Przedsiębiorcy powinni przy tym pamiętać, że od decyzji UODO (jak od każdej decyzji administracyjnej) przysługuje im odwołanie do Sądu Administracyjnego w terminie 30 dni od dnia doręczenia decyzji, co jednocześnie pozbawia ją wykonalności do czasu wydania prawomocnego wyroku przez sąd.

Przetwarzanie danych pozyskanych z publicznie dostępnych źródeł

W kontekście opisywanej kary trzeba zaznaczyć, że podmiot nią obciążony działa w sektorze prywatnym i zajmuje się analityką danych, czyli – poniekąd - zarabia na przetwarzaniu danych pozyskując je z publicznie dostępnych źródeł, takich jak np.: KRS, CEIDG czy

REGON GUS. Rodzi się więc kolejne pytanie: czy dane przedsiębiorców widniejących w powszechnych rejestrach podlegają ochronie prawnej oraz czy trzeba wobec takich osób prawnych spełniać obowiązek informacyjny? Odpowiedź brzmi: tak, jeżeli pozyskiwane są po to, żeby przetwarzać je w zupełnie innym celu, który sami sobie obraliśmy, np. aby prowadzić sprzedaż tych danych, ich obróbkę, lub by stworzyć portal, gdzie zostaną umieszczone i będą udostępniane użytkownikom, którzy uiszczą opłatę abonamentową.

Taka forma wykorzystania danych powszechnie dostępnych w rejestrach przez przedsiębiorcę zobowiązuje go, aby dopełnił obowiązku informacyjnego, o którym mowa w art. 14 RODO. Należy pamiętać, że ustawodawca przewidział również wyłączenia od powyższej reguły, określone w art. 14 ust. 5 RODO. Takim wyłączeniem jest np. sytuacja gdy osoba, której dane dotyczą, dysponuje już tymi informacjami.

Jak można spełnić obowiązek informacyjny?

Obowiązek informacyjny może zostać spełniony na różne sposoby: drogą mailową, telefonicznie czy przy użyciu tradycyjnej poczty. Nie można zatem powoływać się na niedopełnienie obowiązku informacyjnego z uwagi na brak adresu e-mail podmiotów, których dane są przetwarzane oraz na fakt, że wykorzystanie tradycyjnej poczty jest zbyt kosztowne i wymaga niewspółmiernie dużego wysiłku (właśnie taką argumentację we własnej obronie zastosowała obciążona Spółka).

Co w sytuacji, gdy przedsiębiorstwo nie ma poczty elektronicznej? Klauzulę informacyjną można nadać Pocztą Polską. Brakuje aktualnego adresu korespondencyjnego? W takim przypadku można zadzwonić, pamiętając o poinformowaniu, że rozmowa jest nagrywana.

W omawianym przypadku Spółka zdecydowała, że obowiązek informacyjny dopełni jedynie wobec ok. 700 000 osób, których adresy e-mail posiadała. Przy czym dysponowała bazą ponad 7 milionów rekordów zawierających dane osobowe przedsiębiorców oraz osób będących wspólnikami lub członkami organów spółek, fundacji czy stowarzyszeń. Znamiennym jest, że ok. 12 000 osób z 700 000 osób poinformowanych, wniosło sprzeciw na przetwarzanie ich danych osobowych. Na marginesie: Spółka została również zobligowana do dopełnienia obowiązku informacyjnego wobec pozostałych podmiotów –

co, jak możemy się domyślać, będzie łączyło się kosztami mogącymi przerosnąć kwotę samej kary finansowej.

Czy w tym przypadku tak wysoka kara finansowa była zasadna?

W mojej opinii, na to pytanie nie da się odpowiedzieć jednoznacznie. Uważam, że znaczący był fakt, iż u podstaw działania Spółki leży obrót danymi osobowymi, jak również liczba rekordów z danymi osobowymi, tj. skala ich przetwarzania. Istnieje prawdopodobieństwo, że przy mniejszej liczbie rekordów, organ ochrony danych osobowych zastosowałaby jedynie uprawnienie naprawcze skatalogowane w at. 58 RODO.

Prawie rok po wejściu w życie RODO przedsiębiorcy powinni sami sobie odpowiedzieć na kilka pytań: czy spełnili obowiązek informacyjny? Czy poprawnie wydają upoważnienia do przetwarzania danych? Czy szyfrują komunikację? Czy stosują się do wdrożonych procedur z zakresu ochrony danych osobowych?

W firmach, które audytujemy pod kątem zgodności z RODO, obserwujemy nieprawidłowości w zakresie realizacji obowiązku informacyjnego względem osób kontaktowych u kontrahentów lub potencjalnych kontrahentów w przypadku zbierania danych bezpośrednio od nich (art. 13 RODO), a także w razie zbierania tych danych z innych źródeł (art. 14 RODO). Obowiązek ten dotyczy także wszystkich osób fizycznych, których dane już się posiada. Należy go zatem spełnić np. wobec osób, których dane posiada się w bazie klientów, czy też pracowników. Spełnianie obowiązku informacyjnego powinno mieć miejsce już w chwili otrzymania danych osobowych. Jednocześnie powinno to zostać wykonane w sposób pozwalający na spełnienie zasady rozliczalności (art. 5 ust. 2 RODO). Powinien zatem zostać zastosowany system pozwalający na łatwe odszukanie dowodu spełnienia obowiązku informacyjnego.

Piotr Ubych, Menedżer ds. usług ochrony danych i assessmentów, Grupa DEKRA w Polsce

Mając na uwadze ostatnie wydarzenie, namawiam przedsiębiorców do rewizji wdrożonych procedur na gruncie RODO. Jest to jedyny realny sposób, dzięki któremu będą w stanie zminimalizować prawdopodobieństwo nałożenia nań kary finansowej.

Prezentowana podczas audytów dokumentacja ochrony danych osobowych często wymaga uzupełnienia w celu osiągnięcia zgodności z dokumentacją wymaganą przez RODO, wskazaną przez UODO, np. o analizę ryzyka, czy też rejestr czynności przetwarzania. W firmach obserwujemy brak procedur na wypadek wystąpienia naruszeń mogących powodować wysokie ryzyko naruszenia praw i wolności osób, w zakresie ich informowania o działaniach, jakie należy wykonać, aby ryzyko to ograniczyć (art. 34 RODO) oraz brak procedur pozwalających na wykonywanie uprawnień osób, których dane dotyczą, wynikających z RODO, np. prawo do bycia zapomnianym, co do danych osobowych przetwarzanych w organizacji.

Piotr Ubych, Menedżer ds. usług ochrony danych i assessmentów, Grupa DEKRA w Polsce

Dane liczbowe dotyczące obciążonej Spółki pozyskane zostały ze strony: https://uodo.gov.pl/decyzje/ZSPR.421.3.2018?fbclid=IwAR1ZmelVNsPCo1_PW5V8o1IHAZHYq89o8KEkVWs_AFh0uxoP-qZUXGkJe6Q

Hanna Korol,

Radca prawny