RODO incydent... każdemu zdarzyć się może

Mamy przyjemność zaprezentować Państwu pierwszy, zebrany na tak dużej próbie organizacji raport, dotyczący RODO incydentów. Jakie wnioski możemy z niego wyciągnąć?

Zapraszam do lektury!

Jak powstawał raport?

Duże słowa uznania kieruję do wszystkich firm, które zdecydowały się wziąć udział w tworzeniu raportu. Ogromną pomocą była tutaj platforma Związku Firm Ochrony Danych Osobowych (www.zfodo.org.pl), która umożliwiła podjęcie współpracy przez konkurujące ze sobą na co dzień podmioty. ZFODO jest bowiem organizacją zrzeszającą profesjonalne firmy zajmujące się doradztwem z zakresu ochrony danych osobowych, które zdecydowały się działać razem zgodnie z wypracowanymi standardami.

Informacje, które udało nam się zebrać, będą pomocne dla wszystkich osób zajmujących się ochroną danych osobowych.

W mojej opinii publikacja raportu ma szansę przyczynić się do lepszej ochrony prywatności i zwrócenia uwagi na szereg zjawisk i problemów z tym związanych.

Dane, które pozwoliły opracować raport, pochodzą z 277 organizacji przetwarzających dane osobowe, obsługiwanych przez członków ZFODO w okresie maj 2018 – maj 2019.

Polacy nie gęsi... swój raport mają

Naruszenia danych osobowych nie są tematem nowym, związanym z wejściem w życie RODO. Każdy Administrator Bezpieczeństwa Informacji (poprzednik IODa), stykał się w swojej pracy z tym problemem.

My w naszych szkoleniach, realizowanych za czasów poprzedniego stanu prawnego, często powoływaliśmy się np. na raporty Infowatch. Publikowane przez tę amerykańską agencję badawczą wyniki mocno akcentowały czynnik ludzki przy wyciekach danych.

Nie mogliśmy powołać się na polskie dane i statystyki, ponieważ zwyczajnie ich... nie było.

Idea przygotowania polskiego raportu, koncentrującego się wokół naruszeń polskiej ustawy o ochronie danych osobowych z 1997 roku, pojawiła się wkrótce po zapoznaniu się przeze mnie z raportem Infowatch.

W oparciu o funkcjonujące rejestry incydentów, prowadzone przez Administratorów Bezpieczeństwa Informacji, można było opracować większą statystykę, obrazującą zagadnienie z perspektywy polskiego rynku.

Problemem był jednak brak możliwości zebrania odpowiedniej ilości danych, która byłaby reprezentatywna.

Możliwość taka pojawiła się wraz z utworzeniem Związku Firm Ochrony Danych Osobowych.

A teraz zapraszam do sedna artykułu – zobacz w jaki sposób możesz skorzystać z lektury raportu.

Gdzie znajdę raport?

Raport w formacie pdf znajdziesz na stronie internetowej Związku Firm Ochrony Danych Osobowych (link do raportu).

Raport możesz rozpowszechniać i wykorzystywać do własnych potrzeb (np. szkoląc pracowników). Warunkiem jest jedynie wskazanie źródła pochodzenia statystyk i oczywiście niewprowadzanie własnych modyfikacji.

Zapraszam Cię do zapoznania się z raportem i dzielenia się własnymi wnioskami – np. w postaci komentarzy na blogu.

A poniżej moja interpretacja kluczowych statystyk oraz wnioski dla wszystkich osób zajmujących się ochroną danych osobowych.

W mojej firmie zdarzyło się 15 incydentów - czy to już dużo?

Do tej pory w praktyce trudno było odpowiedzieć jednoznacznie na to pytanie. Dzięki raportowi uzyskujemy ważny punkt odniesienia!

Średnia roczna ilość incydentów RODO w 277 organizacjach wyniosła dokładnie 0,46. Jeśli więc w Twojej organizacji miało już miejsce 15 incydentów to zdecydowanie dużo i czas wdrożyć działania naprawcze.

Warto mieć na uwadze jeszcze jedną okoliczność. Większość firm, które objęliśmy badaniem to firmy działające w obszarze b2b. Podmioty działające w obszarach nastawionych na sprzedaż produktów lub usług osobom fizycznym, mogłyby znacząco zawyżyć tę statystykę. Jeśli 15 incydentów zdarzyłoby się w ciągu roku w dużym banku, obsługującym osoby fizyczne, raczej nie uznalibyśmy tej liczby za wygórowaną.

Podsumowując, jeśli Twoja organizacja znacząco odbiega od ww. średniej i nie jesteś np. dużym bankiem, czas podjąć działania zaradcze!

Jeśli do tej pory zarząd odmawiał Ci środków na realizację szkoleń z zakresu RODO – to dobry moment na pokazanie liczb zawartych w raporcie. Nikt nie lubi w negatywny sposób zawyżać średniej.

Kto powoduje większość incydentów?

Kolejne ważne statystki potwierdzają obiegowe opinie i coś o czym teoretycznie wszyscy wiedzą. No właśnie, niby o tym wiemy, ale trudno o potwierdzenie tego w postaci obiektywnych liczb.

Teraz mamy już potwierdzenie w liczbach. Zdecydowana większość, bo aż 89% incydentów jest powodowana przez tzw. czynnik ludzki. Dodajmy do tego zestawienie mówiące o tym, że aż 71% naruszeń ma charakter wewnętrzny (pracownicy lub współpracownicy).

Powyższe sumuje nam się w ważny wniosek. Szkolenia, szkolenia i raz jeszcze szkolenia!

Jednocześnie o ile jesteśmy skłonni inwestować znaczące środki w technologię, to często nie doceniamy potrzeby budowania świadomości i szkolenia personelu z zakresu właściwego obchodzenia się z danymi osobowymi.

O praktycznych rozwiązaniach z zakresu budowania RODO świadomości pisaliśmy już na naszym blogu tutaj.

Zgłaszać incydent organowi nadzorczemu czy nie zgłaszać?

Ciekawa statystyka dotyczy ilości zgłoszonych incydentów. Z raportu wynika, że do Prezesa UODO zgłosiliśmy jedynie 41% wszystkich incydentów. Pozostałe 59% incydentów zostało odnotowanych jedynie w wewnętrznym rejestrze naruszeń.

Sam temat zgłaszania incydentów i sposobu ich kwalifikacji na te wymagające zgłoszenie i te, które tego nie wymagają, będzie jeszcze przedmiotem nowego artykułu na naszym blogu.

Informować osobę, której dotyczy incydent czy nie?

W 76% przypadków, kiedy incydent został zgłoszony do Prezesa UODO, o jego wystąpieniu informowane były też osoby, których dane dotyczą. Pamiętajmy, że do organu zgłaszamy incydent, który może powodować jakiekolwiek ryzyko naruszenia praw i wolności osób fizycznych. Jeżeli ryzyko to określimy jako wysokie, o naruszeniu równocześnie informujemy też podmiot danych.

Aż 1/5 incydentów jest powodowana przez działania procesora!

Nie tylko pracownicy, ale i procesorzy mają dostęp do naszych danych osobowych. Nie zapominajmy o nich.

Dobrze skonstruowana umowa powierzenia oraz prowadzenie audytów procesorów, powinno zminimalizować skutki nastąpienia naruszenia po stronie podmiotu przetwarzającego.

Lepiej jednak zapobiegać niż naprawiać szkody. Dlatego już na etapie nawiązywania współpracy z procesorem warto zweryfikować jego wiarygodność w obszarze RODO.

O tym w jakiś sposób audytować procesora pisaliśmy już na naszym blogu tutaj.

Podsumowanie

Zapraszam do lektury i wyciągania własnych wniosków z zaprezentowanych zestawień. My tymczasem działając w ramach ZFODO, już zbieramy dane do nowego raportu z okres maj 2019 – maj 2020.

Autor artykułu:

Przemysław Zegarek, Prezes Zarządu Lex Artist sp. z o.o. oraz Związku Firm Ochrony Danych Osobowych

Źródła:

- 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 (ogólne rozporządzenie o ochronie danych)
- praktyczne doświadczenie budowania systemów ochrony danych osobowych od 2008 roku (jako ABI) i po 2018 (jako IOD)
- Raport Związku Firm Ochrony Danych Osobowych (ZFODO)