RODO incydenty 2020 - nowy raport ZFODO i co z niego wynika

Przedstawiam Ci najnowszą edycję raportu ZFODO. A także moje własne wnioski praktyczne płynące z analizy raportu. Na koniec swoimi wnioskami podzielą się z Tobą nasi eksperci – praktycy którzy na pierwszej linii frontu, pomagali naszym klientom radzić sobie z naruszeniami RODO.

Pierwszy raport ZFODO powstawał bardzo powoli. Projekt wymagał koordynacji i wymiany informacji między na co dzień konkurującymi ze sobą firmami. Warto było jednak przełamać lody i wspólnie przygotować wartościowy zestaw informacji dla każdego IODa.

Poprzedni raport został opublikowany na stronie ZFODO i na naszym blogu w marcu 2020 roku.

Najnowszy raport w formacie PDF znajdziesz na stronie ZFODO.

*Jeśli trafiłeś/aś tutaj przypadkiem, szukając pomocy przy incydencie RODO w Twojej organizacji, zacznij od lektury tego tekstu.

Co się zmieniło w stosunku do poprzedniego raportu?

Raport zawiera dokładnie te same kategorie informacji za analogiczny okres, tylko rok później. Dzięki temu możesz porównać zmiany w stosunku do poprzedniego roku i wychwycić ich trend. W nowym raporcie zebraliśmy znacznie większą próbę. Poprzedni raport (2019) obejmował 277 administratorów danych. Najnowsza edycja bazuje na znacznie większej próbie 454 organizacji.

Szansa, że Twoja organizacja padnie ofiarą RODO incydentu to… 65%

Statystycznie w skali 12 miesięcy, na jedną badaną organizację przypada 0,65 incydentu ochrony danych osobowych. Wobec tego szansa na pojawienie się jednego incydentu w Twojej organizacji to 65%. Jeszcze rok temu było to 46%.

Prawdopodobieństwo wystąpienia naruszeń rośnie więc prawie o 20 punktów procentowych.. Z czego to wynika? Firmy uczestniczące w badaniu wskazywały na fakt rosnącej świadomości. Zdarzenia, które rok temu nie zostały zauważone, teraz zostały już odnotowane.

Szansa na zaistnienie incydentu w Twojej organizacji w tym roku jest relatywnie duża. Statystyka pokazuje jednak, że będzie to tylko jeden incydent. Przy takiej ilości incydentów, trudno o nabranie wprawy i rutyny przy podejmowaniu kluczowych decyzji tj. informowaniu regulatora oraz osób, których dane dotyczą.

Jednocześnie, jeśli jedyny incydent w Twojej organizacji będzie tak poważny, jak ten dotyczący spółki Morele.net, to może przynieść dotkliwe konsekwencje finansowe. Co więc zrobić? Po pierwsze zapobiegaj (Jak? O tym za chwilę), a po drugie w sytuacjach bardziej ryzykownych i skomplikowanych,

poszukaj wsparcia na zewnątrz. Koniecznie zapoznaj się też z drugą częścią artykułu – czyli komentarzami praktyków.

Powyższa statystyka daje Ci ważny punkt odniesienia. Już wiesz jak wypadasz na tle innych. Jeśli w Twoim rejestrze znalazło się już 20 naruszeń – to dużo. Może warto podjąć dodatkowe działania zapobiegawcze? Pamiętaj też o tym, że branża branży nie równa. Z uwagi na skalę i charakter działania, niektóre branże generują więcej naruszeń, niż inne. W takim przypadku większa średnia naruszeń może być niemożliwa do uniknięcia.

UODO informujemy o naruszeniach rzadziej niż rok temu, za to osoby poszkodowane, nieco częściej

Rok temu informowaliśmy UODO w przypadku 41% naruszeń. W tym roku administratorzy podejmowali decyzje o informowaniu UODO znacznie ostrożniej. Organowi nadzorczemu zgłoszono jedynie 33% przypadków naruszeń.

Co może oznaczać ten trend? W mojej opinii podchodzimy do tematu bardziej selektywnie, zgłaszając Prezesowi UODO tylko najpoważniejsze naruszenia. Interpretujemy przesłankę małego prawdopodobieństwa naruszenia praw lub wolności w sposób bardziej wąski niż rok temu.

Jeśli chodzi o osoby poszkodowane, to kierunek jest dokładnie odwrotny. W tym roku informowaliśmy poszkodowanych o naruszeniach nieco częściej niż rok temu (70% vs. 76%).

Sama statystyka niestety nie da nam jednoznacznej odpowiedzi na dwa kluczowe przy każdym naruszeniu pytania. Czy informować Prezesa UODO? Czy informować osoby poszkodowane?

Tutaj pomaga trening, praktyka i dobra procedura analizy ryzyka naruszenia praw i wolności. O tym pisaliśmy już w naszym cyklu poświęconym naruszeniom RODO:

- Zgłoszenie naruszenia RODO do Urzędu Ochrony Danych Osobowych
- Zgłaszanie naruszenia ochrony danych osobowych osobom poszkodowanym

Branże najbardziej narażone na naruszenia

W tym zestawieniu, podobnie jak rok temu, szczególnie zwraca uwagę branża handlowa/e-commerce. Jeśli Twoja organizacja dostarcza usługi lub towary osobom fizycznym, to szansa na incydent znacząco rośnie. Pokrywa się to z moją obserwacją, wskazującą, że część firm działająca w obszarze b2b, w ogóle nie generuje naruszeń ochrony danych.

Źródła naruszeń ochrony danych osobowych

Najskuteczniejsza metoda radzenia sobie z naruszeniami ochrony danych osobowych, to zapobieganie! Z raportu dowiesz się dużo na temat źródeł naruszeń. Na pewno już nie raz słyszałeś/aś hasła o tym, że najsłabszym ogniwem jest człowiek. Albo, że czynnik ludzki generuje największą liczbę błędów i naruszeń. Jeśli w to nie wierzyłeś/aś albo brakowało Ci konkretnych dowodów – to dane z raportu stanowią twardy dowód, potwierdzający tezę, którą większość z nas czuje intuicyjnie.

W ogólnej liczbie naruszeń, zwraca uwagę także wysoki udział incydentów z udziałem procesorów. W pierwszym raporcie było to aż 20%. W najnowszej edycji to 12%. Jeśli potraktujemy procesora jako źródło wewnętrze, to okaże się, że aż 80% incydentów jest generowanych przez naszą organizację lub jej podwykonawców (procesorów). Czy to znaczy, że powinniśmy zabezpieczać się jedynie od wewnątrz, marginalizując udział stron trzecich (np. hakerów?). Niekoniecznie, ataki hakerskie, mimo, że dość rzadkie, powodują jednak ogromne straty wizerunkowe. Raz jeszcze odwołam się tutaj do przypadku Morele.net, który skutkował nałożeniem przez Prezesa UODO najwyższej, jak dotychczas, kary finansowej (więcej informacji o tej karze znajdziesz tutaj).

Po raz kolejny dochodzimy zatem do wniosku, że najsłabszym ogniwem jest człowiek. Przeważnie człowiek pracujący w naszej organizacji. Hasła „świadomość" i „czynnik ludzki" mogą budzić pewne obawy związane ze swoją niedookreślonością. Jestem jednak zdania, że świadomość też może być RODO rozliczalna!

Wiemy już jaki dokładnie udział wśród incydentów mają te związane z czynnikiem ludzkim. Wiemy jaka część jest świadoma, a jaka nieświadoma.

Zachęcamy też do diagnozowania i monitorowania poziomu świadomości pracowników. Pisaliśmy już o tym na naszym blogu. Takie badanie poziomu świadomości może dać Twojej organizacji twarde dane, które pomogą skutecznie przeszkolić zespół.

Jak minimalizujemy ryzyko związane z czynnikiem ludzkim? Oczywiście szkolimy. W obszarze szkoleniowym, dokonuje się od dłuższego czasu ważna zmiana. Szkolenia są coraz mocniej profilowane pod kątem konkretnych zagrożeń. Coraz częściej bazują na uprzednio zdiagnozowanych zagrożeniach i ryzykach. Mniej czasu poświęca się na kwestie teoretyczne, więcej na praktyczne sposoby radzenia sobie z zagrożeniami.

Poza lepszą diagnostyką, systemami szkoleniowymi czy wykorzystaniem szkoleń zdalnych, praca z ludźmi wciąż wymaga dużej systematyczności, jest żmudna i nie daje natychmiastowych efektów. Ale to jedyny sposób, żeby ustrzec się przed aż 96% naruszeń!

Głos naszych ekspertów - praktyków

Wszyscy stale udoskonalamy swój warsztat pracy, uczymy się. Kolejne naruszenia i sposoby radzenia sobie z nimi rewidują nasze poglądy, zmuszają do szukania nowych rozwiązań. Zapraszam Cię do zapoznania się z doświadczeniem osób, które na co dzień pomagają w usuwaniu ich skutków.

Podsumowanie

Incydenty bezpieczeństwa nie są nowym zjawiskiem, zdarzały się też przed 25 maja 2018 r. W tamtym czasie wystarczyło sporządzić raport ze sprawdzenia incydentu. Jednak realia dotyczące naruszeń zmieniły się gruntownie w momencie rozpoczęcia obowiązywania RODO. Teraz należy dokonać szczegółowej analizy, na czym incydent polegał, kto wie najwięcej na jego temat, a przede wszystkim ustalić, czy doszło do naruszenia praw i wolności podmiotów danych. Jeśli stwierdzimy, że istnieje nawet niskie ryzyko naruszenia praw, musimy o tym powiadomić organ nadzorczy. Incydent bezpieczeństwa w naszej organizacji nie jest tylko wyzwaniem dla IODa, ale też dla osób zaangażowanych w czynności wyjaśniające. W określonym przez RODO czasie 72h trudno jest uzyskać pełną wiedzę na temat naszego incydentu, bardzo często trzeba opierać się na przypuszczeniach… i na koniec ważna decyzja do podjęcia: zgłaszać czy nie? Można powiedzieć szekspirowski dylemat. Od roku 2019 nabieramy w tym zakresie wprawy- mamy już wypracowane praktyki co do kategorii incydentów, które należy zgłaszać, a które nie.

Bogna Tchórzewska, Starszy specjalista ds. ochrony danych osobowych

Incydenty 2020

Wśród naszych klientów występowało wiele incydentów podobnych do tych, które występowały w 2019 r. Świadczy to o tym, że najsłabszym elementem systemu ochrony danych osobowych jest właśnie człowiek – pracownik, który mimo szkoleń zapomina o ciążących na nim obowiązkach bądź samodzielnie próbuje ocenić, że nie doszło do naruszenia ochrony danych i nie informuje przełożonych o zdarzeniu. Często te naruszenia z punktu widzenia pracownika były błahe, natomiast z punktu widzenia wymagań RODO wymagały poinformowania właściwych osób zajmujących się ochroną danych w organizacji.

Nie mniej, porównując z 2019 r., zgłoszenia były i są przekazywane do IOD czy osób odpowiedzialnych za ten obszar, zdecydowanie szybciej, co świadczy o tym, że większość pracowników zdaje sobie sprawę z obowiązujących przepisów i wagi obowiązku zgłaszania naruszeń.

W tym roku w mojej praktyce doszło do kilku sytuacji, w których potencjalne naruszenia były „niejednoznaczne", że tylko gruntowna analiza danego przypadku pozwoliła podjąć właściwą decyzję przez Administratora Danych.

Nasze zeszłoroczne doświadczenia pozwalały także ciut szybciej klasyfikować dane naruszenie i wdrażać rozwiązania, które ograniczą takie sytuacje w przyszłości.

Pamiętajmy o ścisłej współpracy z osobami zajmującymi się ochroną danych w naszej organizacji. Dzięki temu, nawet jeśli dojdzie do naruszenia, będziemy w stanie sobie z nimi poradzić i zadziałać właściwie.

Krystian Dobosz, Starszy specjalista ds. ochrony danych osobowych

Obsługa incydentów to bez wątpienia jedno z najtrudniejszych zadań z którymi mierzą się podmioty stosujące RODO.

Trudności jest wiele. Przede wszystkim właściwa ocena incydentu. Niejednokrotnie ustalenie czy naruszenie wymaga zgłoszenia do organu nadzorczego, czy może także dodatkowo zawiadomienia osób których dotyczył incydent wymaga pogłębionej analizy. Aby ją prawidłowo przeprowadzić potrzebna jest pełna wiedzą o okolicznościach w jakich do niego doszło. Na tym etapie niezwykle istotna jest sprawna komunikacja. Uzyskanie wiedzy na temat okoliczności incydentu często wymaga zaangażowania wielu osób wewnątrz organizacji (np. osób odpowiedzialnych za proces od strony biznesowej, informatyków, prawników, a nawet przedstawicieli spółki matki (centrali) czy zarządu. Jeśli incydent dotyczy danych powierzonych do przetwarzania, konieczne będzie także zaangażowanie osób po stronie procesora.

Mimo rosnącej świadomości na temat czynników zagrażających bezpieczeństwu danych osobowych, w dalszym ciągu najsłabszym ogniwem jest człowiek. Niezamierzony błąd, nieuwaga zdecydowanie dominują wśród przyczyn incydentów. **Administratorzy danych nie mogą zapominać, że nawet najlepsze zabezpieczenia techniczne nie uchronią ich przed naruszeniami ochrony danych jeśli jego pracownicy nie będą mieli odpowiedniej wiedzy i świadomości zagrożeń. Poza tym, doświadczenie z wielu organizacji pokazuje, że działania podnoszące świadomość (np. szkolenia, kampanie informacyjne, pozorowane incydenty) odnoszą efekty wyłącznie wtedy, gdy są regularnie powtarzane.**

Wystąpienie incydentu w organizacji, poza oczywistym ryzykiem prawnym i biznesowym może mieć także pozytywny skutek. Niewątpliwie taka sytuacja podnosi świadomość wśród pracowników, szczególnie wśród tych którzy przyczynili się do jego wystąpienia. Poza tym, niejednokrotnie dopiero pojawienie się incydentu wymusza na zarządach wprowadzenie „odkładanych na później" zmian organizacyjnych (np. wdrożenie procedur, wyznaczenie IOD) czy wdrożenie nowych, zapewniających wyższy poziom bezpieczeństwa technologii informatycznych.

Marcin Szkutnik, Radca prawny

Każdy z podmiotów, który przetwarza dane osobowe powinien być przygotowany na wystąpienie naruszenia ochrony danych. Niezależnie od swojej wielkości, ilości zatrudnianych pracowników, czy firm z którymi współpracuje. Incydent RODO może wystąpić tam, gdzie najmniej się go spodziewamy.

Doświadczenie pokazuje, że naruszenie, zwłaszcza to pierwsze, potrafi być szokiem dla organizacji. Zachowanie pracowników w takich przypadkach niejednokrotnie odbiega od tego wzorcowego, przedstawionego w procedurze. Jeszcze przed analizą całej sytuacji padają pytania o zgłoszenie zdarzenia do UODO, wysokość ewentualnych kar czy odpowiedzialność wewnątrz organizacji. Takie zachowanie rodzi niepotrzebny stres, negatywnie wpływa na przepływ informacji i wydłuża prowadzenie postępowania wyjaśniającego. Dobra organizacja współpracy IOD z osobami przetwarzającymi dane jest tutaj kluczowa. Kluczowa będzie też współpraca na linii IOD – administrator danych. Żadna ze stron nie powinna działać bez wiedzy drugiej strony.

Z każdego incydentu, który miał miejsce w naszej organizacji należy wyciągnąć wnioski. Na pewno nie powinniśmy dopuszczać do sytuacji, gdzie dany rodzaj naruszenia powtarza się cyklicznie. Jeżeli tak się dzieje, to jest to jasny sygnał, że wdrożony system ochrony danych nie działa tak jak powinien i musimy wdrożyć w nim zmiany. Może wystarczy sama zmiana procedur albo dodatkowe przeszkolenie pracowników. Może się jednak zdarzyć, że całkowitej reorganizacji wymagać będzie prowadzony przez nas proces przetwarzania. I na takie działania powinniśmy być przygotowani.

Małgorzata Zdunek, Ekspert ds. ochrony danych osobowych

Autor artykułu:

Przemysław Zegarek, Prezes Zarządu Lex Artist

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)