Pusty rejestr naruszeń RODO - powód do dumy czy niepokoju?

Czy to, że Twoja organizacja jest całkowicie wolna od naruszeń, powinno być traktowane w kategorii sukcesu czy porażki? Postaram się odpowiedzieć na tak postawione pytanie w poniższym tekście. Do jego napisania zainspirowało mnie kilka rozmów w toku pełnienia funkcji IOD. A także najnowsze wyniki raportu naruszeń (wciąż jeszcze nieopublikowanego) przez Związek Firm Ochrony Danych Osobowych.

Ile naruszeń to już dużo?

Dzięki cyklicznie publikowanym przez Związek Firm Ochrony Danych Osobowych raportom, otrzymujemy punkt odniesienia, który wskaże nam, że X to niewiele naruszeń, ale Y to już dużo. Dzisiaj to jedyny taki raport na rynku, który bazuje na relatywnie dużej próbie organizacji i jest cyklicznie powtarzany. Raporty bazujące na danych pochodzących od polskiego czy europejskich regulatorów, odnotowują jedynie naruszenia skutkujące ryzykiem lub wysokim ryzykiem naruszenia praw lub wolności. Takie raporty pomijają zatem wszystkie naruszenia wewnętrzne o niskim poziomie ryzyka, które nie musiały być zgłaszane do organu nadzorczego. Dzięki raportom, ZFODO otrzymuje unikalną szansę analizy anonimowych danych zebranych z dużej liczby organizacji.

Co pokazują dane zbierane przez ZFODO

Okres za który sporządzono raport	Średnia liczba naruszeń przypadających na organizację	Liczba organizacji na której bazuje raport
2019 *maj 2018–maj 2019*	0,46	277
2020 *maj 2019–maj 2020*	0,65	454
2021 *maj 2020 – maj 2021*	0,89	349

W tym momencie w ramach ZFODO trwają właśnie prace nad nowym raportem. Część danych nie została jeszcze zagregowana. Wiemy jednak już teraz, że średnia naruszeń po raz kolejny wzrośnie! Chociaż nie wiadomo jeszcze jak znacząco. Wszystkie osoby zainteresowane pełnymi poprzednimi

raportami, zapraszamy na www.zfodo.org.pl. Najnowszy raport opublikujemy na początku lutego 2023 r., wraz z towarzyszącym mu wydarzeniem.

Warto wskazać, że trend wzrostowy jaki pojawia się w raportach ZFODO odpowiada temu, który notuje nasz organ nadzorczy w kontekście przyjmowanych zgłoszeń. Jak podaje UODO, w 2020 r. zgłoszonych naruszeń było 7,5 tys., podczas gdy rok później już prawie 13 tys.

Jak interpretować powyższe dane?

To co widać na pierwszy rzut oka, to że roczna ilość naruszeń wyraźnie dąży do jednego. Jeśli więc Twoja organizacja odnotowuje rocznie jedno naruszenie, to znaczy, że mieścisz się w statystycznej średniej.

W tym miejscu trzeba odnotować ważne zastrzeżenie. Organizacje uwzględnione w raporcie, pochodzą z bardzo różnych branż i prowadzą działalność na różną skalę. Część z nich to mikroprzedsiębiorstwa, inne to duże globalne korporacje. Ostateczny wynik jest średnią arytmetyczną. Może być więc teoretycznie tak, że jeśli Twoja organizacja odnotowała 12 naruszeń w skali roku, to wynik niekoniecznie powinien być powodem dodatkowego niepokoju. Jeśli taka hipotetyczna organizacja jest duża i działa w branży generującej znaczną ilość naruszeń (np. placówka medyczna), to liczba naruszeń może być znacząco wyższa niż średnia z raportu ZFODO.

Równie istotną informacją, co średnia ilość naruszeń, jest sam trend naruszeń. A ten jest rosnący. Możemy postawić kilka hipotez, dlaczego tak się dzieje. Na przykład:

1) Naruszeń jest więcej, bo organizacje przetwarzają coraz więcej danych i wciąż rozwijają się.
2) Naruszeń jest więcej, bo wzrasta ich wykrywalność. To, co jeszcze rok temu nie byłoby w ogóle odnotowane i zgłoszone, teraz trafia do rejestru naruszeń.
3) Naruszeń jest więcej, bo maleje poziom świadomości, ostrożności i uważności pracowników. Popełniają więcej błędów.

W mojej opinii najbardziej prawdopodobna będzie hipoteza numer dwa. Ilość naruszeń rośnie, ponieważ rośnie poziom świadomości zespołu. Wydarzenia, które wcześniej były zamiatane pod dywan lub w ogóle nie były traktowane w kategorii naruszenia, teraz są właściwie odnotowywane i raportowane.

Hipotezę trzecią ciężko obronić, bo jeśli maleje poziom świadomości, to dlaczego pracownicy raportują więcej naruszeń? Te dwa procesy byłyby ze sobą sprzeczne.

Powyższe wnioski pokrywają się z naszymi doświadczeniami w obsłudze klientów Lex Artist. Podobne procesy odnotowuje też nasza konkurencja zrzeszona w ramach Związku Firm Ochrony Danych Osobowych.

Powodem do niepokoju powinny być zatem skrajne sytuacje. Jeśli Twoja organizacja w ogóle nie odnotowuje naruszeń, to sytuacja może budzić niepokój. Zwłaszcza jeśli organizacja jest duża i rejestr naruszeń pozostaje pusty od kilku lat. Inspektorzy UODO podejrzliwie patrzą na pusty rejestr naruszeń. Podobnie do takiej sytuacji podchodzą również zewnętrzni audytorzy.

Jeśli z kolei niewielka organizacja odnotowuje dziesiątki naruszeń w skali roku, to również warto bliżej przyjrzeć się takiej sytuacji. Zapewne jest tutaj jakiś wspólny mianownik i istnieje możliwość zmniejszenia liczby niepożądanych zdarzeń.

Czy IOD powinien być rozliczany z tytułu ilości naruszeń?

Odpowiedź na to pytanie jest prosta. Nie rozliczaj pracy swojego IOD-a w kontekście ilości odnotowanych naruszeń! W takiej sytuacji IOD może nie mieć motywacji do budowania odpowiedniego poziomu świadomości. Zostanie postawiony przed trudnym dylematem. Rzetelne wykonywanie pracy będzie przez pracodawcę karane jej niższą oceną (być może również finansowo). Jeśli IOD będzie chciał otrzymać pozytywną ocenę pracy to system będzie premiował niewykrywanie naruszeń.

Nieodnotowane naruszenia mogą się bardzo zemścić na organizacji. Kary nałożone przez UODO i inne negatywne konsekwencje będą znacznie surowsze niż w przypadku zaraportowania sytuacji.

W mojej opinii inspektorzy UODO mogliby wręcz uznać system premiowania pracy Inspektora Ochrony Danych (oceny jego pracy czy wysokości wynagrodzenia), za formę wpływu czy instrukcji wydawanej IOD. A takie działanie jest sprzeczne z art. 38 ust. 3 RODO. Niewypowiedziana wprost instrukcja brzmiałaby w takiej sytuacji tak: „oczekujemy od Ciebie jak najmniejszej odnotowywanej liczby naruszeń".

Na ilość naruszeń w organizacji wpływ mają nie tylko działania Inspektora Ochrony Danych. Liczy się przede wszystkim to, czy organizacja jest zdyscyplinowana, pracownicy nie są przeładowani ilością obowiązków, czy wdrożono odpowiednie środki zabezpieczeń, jej wielkość, branża, w której działa, itd. Działania IOD, zmierzające do budowy świadomości to tylko jeden z wielu elementów, które ostatecznie mają wpływ na ilość naruszeń.

Postępowanie z naruszeniami ochrony danych osobowych – praktyczny pakiet procedur, szablonów i instrukcji

Przygotowaliśmy dla Ciebie kompleksowy pakiet wytycznych w zakresie zarządzania naruszeniami ochrony danych osobowych w organizacji.
Nasze dokumenty zostały opracowane w taki sposób, aby ich dostosowanie do działalności Twojej organizacji było jak najbardziej intuicyjne i proste.

SPRAWDŹ

Jaka jest rola Zarządu?

Zarząd powinien być światom tego, że praca IOD (lub po prostu osoby zajmującej RODO), nie polega na zadbaniu o pusty rejestr naruszeń. Osoby decyzyjne powinny stworzyć atmosferę, w ramach której, naruszenie nie będzie rozpatrywane jedynie w kategorii porażki i wyciągania surowej odpowiedzialności. Zbyt surowe karanie naruszeń, może doprowadzić do jeszcze gorszych skutków. Pracownicy bojący się kar, przestaną zgłaszać naruszenia. W ten sposób zabetonujemy rejestr naruszeń na poziomie „pusty". Jednak na pewno nie będzie to korzystne dla organizacji.

Jeśli IOD chwali się całkowitym brakiem naruszeń, może warto zadać mu pytanie z czego brak naruszeń może wynikać? Dlaczego inni popełniają błędy, a my nie? Czy jesteśmy tak doskonali, czy może po prostu zespół nie wie, że pewne sytuacje stanowią naruszenia?

Podsumowanie

Rejestr naruszeń mówi bardzo dużo o Twojej organizacji. Jego zawartość trzeba rozpatrywać zawsze w kontekście całokształtu jej działalności. Jednak w większości przypadków, całkowicie pusty rejestr naruszeń może stanowić większy powód do niepokoju niż rejestr z pewną ilością wpisów.

Wysiłek organizacji powinien koncentrować się na dążeniu do minimalizacji liczby naruszeń i wyciąganiu z nich wniosków, a nie do całkowitej eliminacji niepożądanych zdarzeń.

Autor artykułu:

Przemysław Zegarek, Prezes Zarządu Lex Artist sp. z o.o.

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
- https://www.zfodo.org.pl/typ/raporty/
- https://serwisy.gazetaprawna.pl/orzeczenia/artykuly/8554773,rodo-obsluga-skarg-pieniadze.html