Zgłaszanie naruszenia ochrony danych osobowych osobom poszkodowanym

Artykuł stanowi część cyklu publikacji poświęconych postępowaniu z naruszeniami ochrony danych osobowych. Zapraszamy do lektury pozostałych części:

- Część I: Ups… mamy naruszenie ochrony danych osobowych
- Część II: Zgłaszanie naruszenia RODO do Urzędu Ochrony Danych
- Część III: Zgłaszanie naruszenia ochrony danych osobowych osobom poszkodowanym – właśnie go czytasz 😊

Zapraszam Cię do przeczytania trzeciego artykułu poświęconego naruszeniom RODO. Po lekturze poprzednich treści umiesz już prawidłowo kwalifikować naruszenia. Wiesz też jak je wykrywać i znasz ich najczęstsze przyczyny. Z części drugiej dowiedziałeś/aś się, czy i w jaki sposób zgłosić naruszenie do Urzędu Ochrony Danych Osobowych. Teraz przyszedł czas na ostatni krok – czyli na poinformowanie samych poszkodowanych!

Dlaczego informowanie poszkodowanych o naruszeniach ochrony danych osobowych jest potrzebne

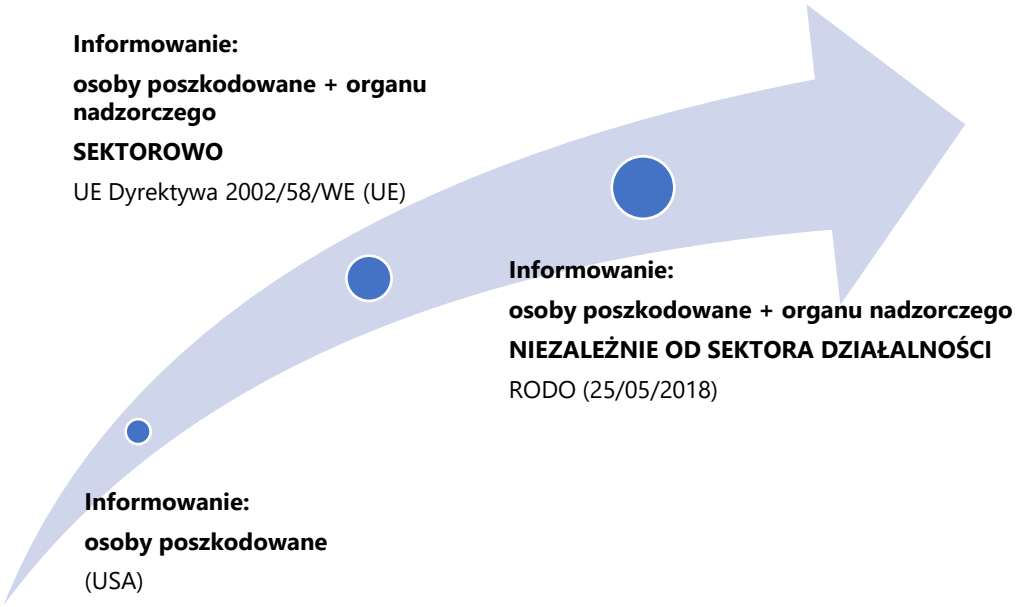
Dzisiaj informowanie o naruszeniach to wymóg prawny. Jednak nie zawsze tak było.

Pierwsze większe wycieki danych osobowych pojawiły się w Stanach Zjednoczonych. Amerykanie dość szybko wprowadzili do swojego systemu prawnego obowiązek informowania poszkodowanych o tego typu zdarzeniach. Odpowiednie przepisy były nieregularnie wprowadzane we wszystkich 50 stanach od 2002 roku. W USA, termin na zgłoszenie naruszenia ochrony danych osobowych, w zależności od stanu, wynosi od 5 dni do nawet 30 dni. Adresatem zgłoszenia o naruszeniu jest co do zasady osoba, której danych dotyczy incydent. Niektóre przepisy stanowe nakładają jednak obowiązek powiadomienia o naruszeniu, również stanowych prokuratorów lub agencji federalnych, a także w uzasadnionych przypadkach, biur kredytowych,

Na gruncie europejskim, pierwsze przepisy dotyczące zawiadamiania osób poszkodowanych naruszeniem pojawiły się ponad 10 lat później. 25 sierpnia 2013 r. w życie weszły przepisy unijne nakładające dodatkowe obowiązki na dostawców publicznie dostępnych usług telekomunikacyjnych.

W świetle tych przepisów, odpowiednio zaimplementowanych w Polsce poprzez przepisy Ustawy Prawo telekomunikacyjne, przedsiębiorca telekomunikacyjny, w przypadku stwierdzenia naruszenia bezpieczeństwa danych osobowych, zobowiązany został do powiadomienia o tym właściwego organu ds. ochrony danych, a także abonenta lub użytkownika końcowego, którego dane zostały naruszone. Warto dodać, że przepisy te nadal obowiązują.

RODO poszło jeszcze dalej, nakazując informowanie i osób, których dane dotyczą i organu nadzorczego **bez względu na to, w jakiej branży działa sprawca naruszenia**.



Twórcy powyższych przepisów wyszli ze słusznego założenia, że nie wszyscy administratorzy poinformują swoich klientów o tym, że z danymi osobowymi wydarzyło się coś złego.

Transparentność dotycząca wycieków danych ma umożliwić poszkodowanym odpowiednio szybką reakcję, która powstrzyma dalsze szkody. Na przykład w sytuacji wycieku bazy danych z numerami kart kredytowych, ich szybkie zastrzeżenie może ograniczyć lub wręcz wyeliminować szkody.

Co mówi RODO na temat informowania osób?

Obowiązek zawiadamiania o naruszeniu osób, których dane dotyczą, wynika z art. 34 ust. 2 RODO:

*„Jeżeli naruszenie ochrony danych osobowych **może powodować wysokie ryzyko** naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu."*

Obowiązek ten nie ma charakteru bezwzględnego. Zawiadomienia należy dokonać tylko w ściśle określonym przypadku. Chodzi o sytuację, kiedy ryzyko naruszenia praw i wolności osób fizycznych zostało oszacowane na poziomie wysokim.

Co za tym idzie, nie każde naruszenie, będzie powodowało konieczność wysyłania informacji do osób, których dane dotyczą. Poziom zagrożenia, który generuje taki obowiązek musi być zatem wyższy niż w przypadku notyfikacji naruszenie do organu nadzorczego.

Przykłady sytuacji, w których będzie występowała konieczności poinformowania osób o naruszeniu zostały przedstawione przez Europejską Rade Ochrony Danych. Do takich sytuacji zaliczają się na przykład:

- niedostępność przez 30 godzin szpitalnej dokumentacji medycznej w wyniku cyberataku,

- cyberatak i publikacja w Internecie identyfikatorów użytkownika, haseł i historii zakupów klientów platformy internetowej.

Wskazówki w tym zakresie przygotował także Urząd Ochrony Danych Osobowych w publikacji „*Obowiązki administratorów związane z naruszeniami ochrony danych osobowych*". W opinii organu nadzorczego do takich sytuacji należą te prowadzące do dyskryminacji, kradzieży tożsamości, oszustw, straty finansowej albo te powodujące uszczerbek na reputacji. W poradniku wskazano także, że wysokie ryzyko, o którym mowa nie musi się urzeczywistnić.

W tych przypadkach nie musisz informować osób poszkodowanych

W treści art. 34 ust. 3 RODO, wskazano trzy wyjątkowe sytuacje, w których administrator danych osobowych jest zwolniony z obowiązku zawiadamiania osób o naruszeniu:

1) **administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony** i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym, np. dane osobowe zostały zabezpieczone za pomocą szyfrowania lub tokenizacji,

2) **administrator natychmiast po wystąpieniu naruszenia podjął środki eliminujące prawdopodobieństwo wysokiego ryzyka** naruszenia praw lub wolności osoby, np. zorientował się on, że przesyłka, w której znajdowały się dane osobowe została zaadresowana do niewłaściwego nadawcy i podjął on natychmiast kroki w celu skontaktowania się z kurierem aby nie dopuścić do dostarczenia przesyłki,

3) **kontakt z osobami wymagałby niewspółmiernie dużego wysiłku**, z zastrzeżeniem, że takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób, np. dokumenty, w których znajdowały się dane osobowe uległy zniszczeniu i administrator danych osobowych nie ma możliwości kontaktu bezpośredniego z osobami, których dane dotyczą, więc zasadnym będzie w tej sytuacji wydanie publicznego komunikatu.

Oczywiście mając na uwadze zasadę rozliczalności danych osobowych, administrator danych, powinien być w stanie wykazać się dowodami przed organem nadzorczym, że w określonej sytuacji został spełniony, któryś z powyższych warunków.

Pamiętaj też, że w przypadku naruszeń ochrony danych osobowych sytuacja może być dynamiczna. Jeśli naruszenie początkowo zostało ocenione na poziomie niskim, to po otrzymaniu dodatkowych informacji z nim związanych ocena ryzyka może się zmienić i spowodować konieczność zawiadomienia osób o naruszeniu.

Może także okazać się, że to organ nadzorczy wskaże, że istnieje konieczność zawiadomienia osób zgodnie z postanowieniem art. 34 ust. 4 RODO. Mieliśmy już do czynienia z taką sytuacją w praktyce.

Katarzyna Kmiecicka, ekspert ds. ochrony danych osobowych

U jednego z naszych klientów, podczas szacowania ryzyka naruszenia praw i wolności osób fizycznych, doszliśmy do wniosku, że naruszenie nie plasuje się na poziomie wysokim, więc dokonaliśmy jedynie jego notyfikacji w UODO. Po upływie pewnego czasu, otrzymaliśmy natomiast pismo od organu, w

którym wezwał on administratora danych do natychmiastowego poinformowania osób, o naruszeniu, które miało miejsce. Na klienta nie została nałożona żadna kara, a jedynie został on zobowiązany do podjęcie konkretnego działania w tym zakresie.

Powyższy przypadek pokazuje nam, że zawiadomienie o naruszeniu osób, których danych ono dotyczy, jest dla organu niezwykle istotne. Pamiętajmy, że głównym jego celem jest maksymalne zabezpieczenie osób, których dane dotyczą przed negatywnymi skutkami, jakie może spowodować zaistniała sytuacja.

Jak oszacować wysokie ryzyko naruszenia praw i wolności osób fizycznych

Szacowanie ryzyka naruszenia praw i wolności jest kluczowe z trzech powodów:

- **po pierwsze**, jego oszacowanie będzie potrzebne do podjęcia decyzji o zgłoszeniu naruszenia organowi nadzorczemu,
- **po drugie**, poziom ryzyka będzie odgrywał kluczową rolę przy obowiązku poinformowania osób, których danych osobowych to naruszenie dotyczy,
- **po trzecie**, dobrze wykonane szacowanie ryzyka pozwoli Ci podejść do sprawy w adekwatny sposób.

Jeśli ocena ryzyka będzie bardzo niska, to wysoki poziom stresu i angażowanie dużego zespołu kryzysowego, będzie zupełnie nieuzasadnione. I odwrotnie, jeśli sprawa jest poważna, to musisz nadać jej odpowiednią rangę i zaangażować więcej osób do jej rozpoznania.

O tym, w jaki sposób oszacujesz ryzyko naruszenia praw i wolności osób fizycznych, pisałem już w naszej wcześniejszej publikacji.

Możesz też skorzystać z kalkulatora oceny naruszenia przygotowanego przez naszych ekspertów!

Forma informowania: ustnie, mailowo, pisemnie czy w jeszcze inny sposób?

RODO nie określa w sposób bezpośredni formy w jakiej powiadomienie powinno zostać przedstawione osobom, których dane dotyczą. Ostateczny wybór metody powiadomienia, może zależeć od, tego jakimi danymi kontaktowymi dysponujesz.

W związku z tym forma powiadomienia może być:

- **ustna** (kontakt bezpośredni, telefoniczny),
- **pisemna** (korespondencja tradycyjna lub w formie elektronicznej, np. mail, sms).

Warto zaznaczyć, że zawiadomienie powinno być sporządzone w takiej formie, która pozwoli osobom, których dane dotyczą wielokrotne zapoznanie się z jego treścią.

Pamiętaj też o tym, że zawiadomienie powinno zostać dostarczone w możliwie jak najkrótszym czasie. W tym kontekście forma elektroniczna powiadomienia będzie miała dużą przewagę nad korespondencją tradycyjną.

Po pierwsze, informacje zostają przekazane bardzo szybko. Po drugie, osoba poszkodowana w każdym momencie będzie miała możliwość zapoznania się z treścią.

Co do zasady osoby powinny zostać powiadomione o naruszeniu w sposób bezpośredni, chyba że taka forma powiadomienia wymagałaby niewspółmiernie dużego wysiłku. W takim przypadku może zostać wydany publiczny komunikat lub inny podobny środek, który pozwoli w równie skuteczny sposób powiadomić osoby o naruszeniu.

Podczas formułowania treści i formy komunikatu, należy mieć także na uwadze zasadę przejrzystości. Zawiadomienie powinno być sformułowane jasnym i prostym językiem, w sposób przejrzysty dla osoby. Europejska Rada Ochrony Danych wskazuje, że **do przejrzystych metod zawiadamiania należą**:

- komunikacja bezpośrednia, np. wiadomości e-mail, SMS, wiadomości bezpośrednie,
- rzucające się w oczy bannery lub powiadomienia na stronach internetowych,
- komunikacja pocztowa,
- rzucające się w oczy reklamy w mediach drukowanych.

Powiadomienie, które jest tylko częścią komunikatu prasowego lub zostało zamieszczone na blogu przedsiębiorstwa, nie byłoby skuteczną metodą zawiadomienia osób fizycznych o naruszeniu.

Podczas formułowania zawiadomień, trzeba też mieć na uwadze język komunikacji oraz to, czy osoby zrozumiały charakter naruszenia i będą wiedziały, co muszą zrobić, aby się odpowiednio zabezpieczyć.

Na koniec warto zwrócić uwagę na motyw 88 RODO i to, że w pewnych okolicznościach, gdy jest to odpowiednio uargumentowane i zgodne z wytycznymi organów ścigania, administrator może opóźnić wysłanie zawiadomienia o naruszeniu do osób fizycznych. Opóźnienie takie powinno trwać do momentu, w którym takie zawiadomienie nie wypłynie negatywnie na prowadzone postępowanie.

Ile mam czasu na poinformowanie poszkodowanych?

W RODO wskazano jedynie, że osoby o wystąpieniu naruszenie należy zawiadomić „**bez zbędnej zwłoki**". Nie mamy żadnych dalszych wskazówek w tym zakresie. Z takim właśnie niedookreślonym precyzyjnie terminem możemy się spotkać się w wielu aktach prawnych. Co on oznacza w praktyce?

Zawiadomienie powinno zostać przedstawione osobom najszybciej jak to jest tylko możliwe, w danych okolicznościach.

Szybkość udzielenia informacji jest tutaj kluczowa. Jej dostarczenie ma na celu umożliwienie natychmiastowych działań zaradczych, osobom poszkodowanym. Przykładowo, jeśli doszło np. do wycieku z banku loginów i haseł do bankowości elektronicznej, klienci powinni zostać o tym powiadomieni, najszybciej jak to możliwe w celu natychmiastowej zmiany haseł.

Art. 34 ust. 1 RODO nie precyzuje także od kiedy należy liczyć czas („bez zbędnej zwłoki"). Według mnie zasadne jest przyjęcie, że podobnie jak w przypadku obliczania terminu 72 h na zgłoszenie naruszenia organowi nadzorczemu, kluczowy jest moment stwierdzenia tego naruszenia.

Małgorzata Zdunek, ekspert ds. ochrony danych osobowych

W praktyce, decyzja o tym, czy o danym naruszeniu informujemy osoby, których danych ono dotyczy, zostanie podjęta po stwierdzeniu tego naruszenia i dokonaniu jego kwalifikacji, jako mogące powodować wysokie ryzyko naruszenia praw lub wolności tych osób. Dopiero wtedy bowiem, jesteśmy w stanie określić, jakie negatywne skutki dla podmiotów danych niesie za sobą ten incydent. Jeżeli już na początku prowadzonego postępowania wyjaśniającego, jesteśmy w stanie oszacować przedmiotowe ryzyko jako wysokie, nie powinniśmy zwlekać z przekazaniem stosownych informacji. Przykładowo, jeżeli incydent dotyczy wycieku informacji, które mogą posłużyć do kradzieży tożsamości, osoba, której dane dotyczą powinna dowiedzieć się o nim jak najszybciej. Umożliwi jej to podjęcie stosownych działań (np. zastrzeżenie dokumentu tożsamości).

W jaki sposób i o czym informować poszkodowanych?

Wiesz już jak i kiedy należy powiadomić osoby o naruszeniu. Przyjrzyjmy się teraz temu, co powinno zawierać zawiadomienie. Zgodnie z RODO zawiadomienie powinno zawierać co najmniej:

- **imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego** – aby zapewnić osobom możliwość uzyskania dodatkowych informacji lub rozwiania wątpliwości związanych z naruszeniem,
- **opis możliwych konsekwencji naruszenia** – powinien być on możliwie jak najbardziej szczegółowy i dokładnie opisywać ryzyko jakie może spowodować naruszenie,
- **opis środków zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu**, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków – administrator danych powinien wskazać jakie działania zostały przez niego podjęte lub zostaną podjęte w związku z naruszeniem oraz powinien on przedstawić osobom, których dane dotyczą wskazówki jakie aktywności mogą one podjąć aby zminimalizować konsekwencje zaistniałej sytuacji.

W mojej ocenie, zawiadomienie warto wzbogacić jeszcze o **opis charakteru naruszenia**. Powinien on być możliwie szczegółowo i jasno opisany, aby osoby były w stanie zrozumieć co w istocie stało się z ich danymi osobowymi oraz co to dla nich oznacza.

Naruszenie ochrony danych osobowych to zdecydowanie sytuacja o potencjale kryzysowym. Jeśli naruszenie ma dużą skalę i może być bardzo dotkliwe dla poszkodowanych, to sytuacja jest bardzo poważna. Właśnie dlatego, poza spełnieniem wymogów prawnych, pamiętaj kilku ważnych zasadach.

Informuj rzetelnie – nie zatajaj informacji, nie przerzucaj odpowiedzialności na inne osoby. W praktyce często obserwuję komunikaty, w których administrator danych próbuje przerzucić odpowiedzialność np. na procesora, podwykonawcę czy jeszcze inną osobą trzecią. Takie tłumaczenia w niczym nie pomogą, a mogą jedynie drażnić Twoich klientów. Weź pełną odpowiedzialność za to co się wydarzyło. Przecież to Ty wybrałeś tych, a nie innych dostawców usług. Gwarantuję, że Twoi klienci docenią odwagę i szczerość.

Powiedz przepraszam – to słowo naprawdę ma znaczenie. Niektórzy „eksperci" od relacji doradzą Ci, aby nie przepraszać. Uzasadnią to tym, że tak otwarte przyznanie się do błędu może otworzyć poszkodowanych na poszukiwanie rozwiązań odszkodowawczych. Moje doświadczenie mówi zupełnie co innego. Ludzie doceniają słowo przepraszam. Jego użycie nie sprowokuje do masowego pisania pozwów przeciwko Tobie. Wręcz przeciwnie – klienci docenią odwagę i prostoty przekaz Twojego komunikatu.

Zaproponuj coś w zamian - Niekoniecznie musi to być wielotysięczne odszkodowanie. Mnie bardzo spodobała się reakcja jednego z organów administracji publicznej w Polsce. W komunikacie o wycieku danych, urzędnicy obiecali kupić serię wartościowych publikacji o… bezpieczeństwie informacji i prawie do prywatności do miejskiej biblioteki. Nie zawsze więc chodzi o ogromne sumy. Liczą się również gesty, które pokazują rzeczywisty szacunek do naruszonych wartości.

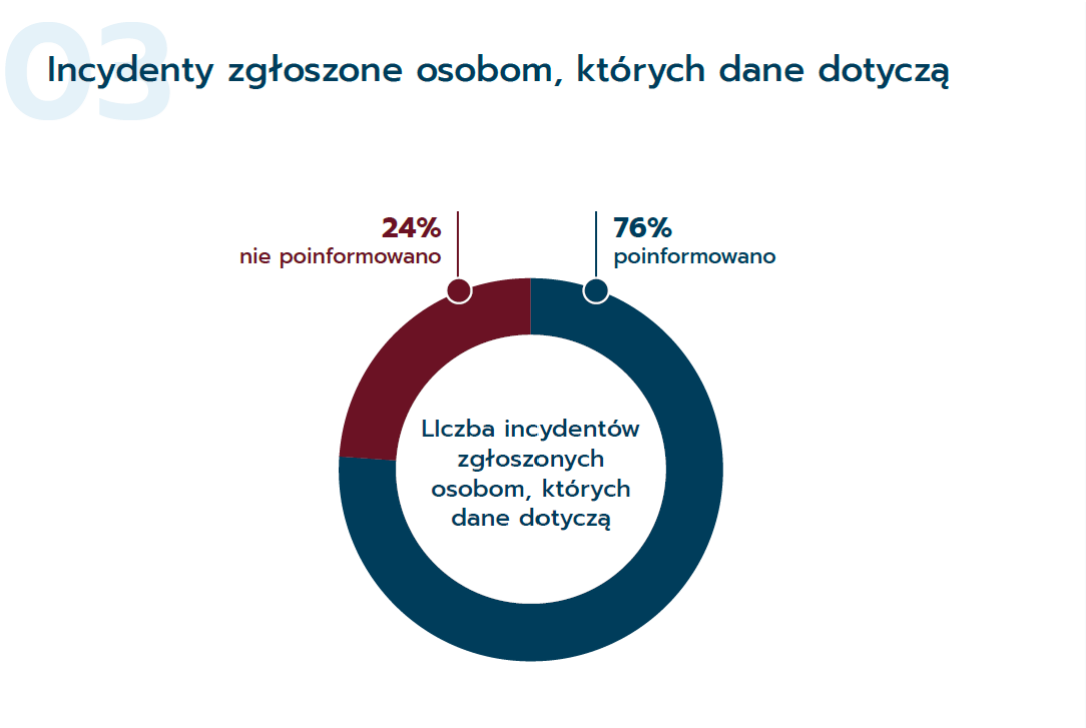
Zobacz na przykładzie opracowanym przez naszych ekspertów, jak może wyglądać zawiadomienie o naruszeniu!

Statystyka ZFODO – jak często o naruszeniach informują inni?

Interesująco wygląda statystyka, która jest elementem raportu Związku Firm Ochrony Danych Osobowych. Wynika z niej, że aż w nieco ponad ¾ przypadków, osoby poszkodowane, były informowane o incydencie. Z pełnym raportem możesz zapoznać się tutaj.

Zwraca uwagę fakt, że częściej informujemy osoby, niż Urząd Ochrony Danych Osobowych, który jest informowany „jedynie" w 59% przypadków. Mimo, że przepisy są bardziej restrykcyjne w zakresie informowania regulatora, niż osób.

Statystyka wskazuje na to, że administratorzy danych przykładają większą wagę do transparentności naruszeń.



Pamiętaj jednak, że nie zawsze informowanie osób jest najlepszym rozwiązaniem. W przypadku sytuacji błahych, nie generujących ryzyk, lepiej powstrzymać się przed niepokojeniem naszych klientów. Komunikat o naruszeniu, będzie dla nich na pewno niepokojący i angażujący. Oczywiście to zawsze trudna decyzja. Musimy wyważyć odpowiednio ryzyko i zagrożenie, w wielu przypadkach znajdziemy wiele za i przeciw informowaniu. W tym miejscu znów wracamy do fundamentu – czyli dobrze wykonanego szacowania ryzyka naruszenia!

Małgorzata Zdunek, ekspert ds. ochrony danych osobowych

Możemy wyobrazić sobie sytuację, w której pracownik administratora popełnił błąd i przesłał draft umowy nie temu kontrahentowi, któremu powinien. W dokumencie tym niewątpliwie zostały ujawnione dane osobowe (chociażby osób reprezentujących strony umowy, czy też dane osób wskazanych do kontaktu przy jej realizacji). Mamy zatem do czynienia z naruszeniem w rozumieniu RODO. Dotyczyło ono jednak danych służbowych, wskazanych na stronach internetowych, czy też w publicznie dostępnych rejestrach (CEIDG, KRS). W takim wypadku informowanie osób, których dane dotyczą nie będzie obowiązkowe.

Praktyczne przykłady naruszeń, o których powinieneś poinformować poszkodowanych

Spójrzmy jeszcze na kwestię informowania z drugiej perspektywy. Kiedy w praktyce zdecydowanie rekomendujemy informowanie osób? Oddajmy głos naszym ekspertom.

Katarzyna Kmiecicka, ekspert ds. ochrony danych osobowych

Ze swojej praktyki do takich sytuacji mogę zaliczyć te, gdzie dochodzi do naruszenie danych o szczególnym charakterze, czyli na przykład danych dotyczących stanu zdrowia, wyników badań lekarskich. Dodatkowo w sytuacjach, gdy wyciekają także dane identyfikacyjne jak PESEL, bez żadnych wątpliwości możemy stwierdzić, że naruszenie plasuje się na poziomie wysokim i zawiadomienie o nim osób jest absolutnie konieczne.

Małgorzata Zdunek, ekspert ds. ochrony danych osobowych

Zdecydowanie powinniśmy informować o naruszeniach, które dotyczą danych osobowych, z wykorzystaniem których, można dokonać kradzieży tożsamości lub wszelkiego rodzaju wyłudzeń. Jeżeli prowadzimy sklep internetowy i w wyniku ataku utraciliśmy dane naszych klientów (identyfikacyjne, adresowe, zapisanych kart płatniczych), powinniśmy nie tylko jak najszybciej poinformować te osoby o incydencie, ale także przesłać stosowne informacje do Urzędu Ochrony Danych Osobowych.

Tomasz Wasilczyk, starszy specjalista ds. ochrony danych osobowych

Co do zasady, wysokie ryzyko dla praw i wolności osób fizycznych, a więc tym samym konieczność zawiadomienia podmiotów danych, będzie występować na przykład w sytuacji, kiedy pracownik placówki medycznej wyda dokumentację medyczną innemu pacjentowi. Jeżeli naruszenie polega na omyłkowym dostarczeniu korespondencji innemu klientowi, a korespondencja ta zawiera takie dane jak imię, nazwisko i numer PESEL, to również powinniśmy poważnie rozważyć zawiadomienie o tym incydencie osób, których danych on dotyczy.

Podsumowanie

W dzisiejszych czasach incydenty i naruszenia przestają być wewnętrzną sprawą Twojej organizacji. Z uwagi na dużą skalę i zasięg, mogą stać się problemem globalnym. Obowiązki notyfikacyjne potraktuj jako sposób na stawienie czoła temu problemowi.

Praktyka pokazuje, że dobre zarządzanie kryzysowe incydentem, może w niektórych przypadkach nawet zwiększyć poziom zaufania do Twojej organizacji!

Autor artykułu:

Przemysław Zegarek, Prezes Zarządu

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)

- Wytyczne dotyczące zgłaszania naruszeń ochrony danych osobowych zgodnie z rozporządzeniem 2016/679 (przyjęte w dniu 3 października 2017 r. ostatnio zmienione i przyjęte w dniu 6 lutego 2018 r.)
- Obowiązki administratorów związane z naruszeniami ochrony danych osobowych, wersja 1.0, czerwiec 2019
- praktyczne doświadczenie budowania systemów ochrony danych osobowych od 2008 roku (jako ABI) i po 2018 roku (jako IOD)
- wsparcie administratorów danych osobowych, którego udzielaliśmy jako Lex Artist w ponad 50 naruszeniach