Warszawa, 20.06.2023 r.

Top 5 najpopularniejszych naruszeń na 5 lecie RODO

5 lat obowiązywania RODO minęło jak jeden dzień. Większość z nas zdążyła poznać nowe przepisy i się z nimi oswoić. Znamy podstawowe definicje, wiemy, w jaki sposób i dlaczego należy chronić dane osobowe. Niewątpliwie każdy z nas słyszał też o karach – karach, które mogą nas spotkać za zaistniałe naruszenia. O samych naruszeniach napisano dużo artykułów. Czym są naruszenia i jak sobie z nimi poradzić? Jak i kiedy należy je zgłosić? Co nam może grozić za niezgłoszenie naruszenia? Natomiast z uwagi, iż incydenty są esencją RODO i głównym celem wdrożenia przepisów o ochronie danych osobowych, informacji nigdy nie będzie wystarczająco dużo. W tym artykule skupimy się na praktycznych przykładach. Nie na ustawowych definicjach, a sytuacjach z codzienności zawodowej, w których naruszenia przydarzają się najczęściej.
Dane te pochodzą ze sprawozdań z działalności Prezesa UODO z ubiegłych lat i dotyczą najczęściej pojawiających się przypadków w zgłoszeniach kierowanych do Urzędu Ochrony Danych Osobowych. Na wstępie proponuję potraktować artykuł jako rachunek sumienia. Czy przez 5 lat obowiązywania RODO przydarzyły nam się opisywane sytuacje? Sprawdźmy więc, ile statystyka ma wspólnego z rzeczywistością.

Dokumentacja papierowa (zawierająca dane osobowe) zgubiona, skradziona lub pozostawiona w niezabezpieczonej lokalizacji.

Początkowo powyższe naruszenia nie zdarzały się zbyt często. Najczęściej były to jednostkowe, ale bardzo medialne sprawy znajdowania całych kartonów z dokumentami w lasach lub na wysypiskach. Istotnie, są bardziej skuteczne sposoby niszczenia danych osobowych. To, że zostały one wydrukowane na papierze, nie oznacza, że powinny trafić do niebieskiego kosza na makulaturę. 😊 Natomiast pandemia oraz praca zdalna zmieniły realia obrotu dokumentacją papierową – naraziły ją na większe zagrożenia niż do tej pory. Wynoszenie dokumentów poza miejsce pracy, przypadkowe pozostawianie w publicznych miejscach. Nawet z pozoru mające zagwarantować bezpieczeństwo, pandemiczne rozwiązanie, jakim było przyjmowanie korespondencji przychodzącej do „kartonów kwarantanny", rodziło ryzyko na gruncie RODO. Zazwyczaj dokumentacja oczekiwała w miejscach o swobodnym dostępie z zewnątrz (recepcja biurowca, gdzie kilka firm miało wystawione kartony obok siebie, gdyż wejście do budynku było zabronione lub znacznie ograniczone). Robiąc rachunek sumienia: czy zdarzyła nam się podobna sytuacja? Jeżeli nie to znakomicie, możemy przejść dalej. Statystycznie kolejne naruszenia przydarzały się jeszcze częściej.

Korespondencja papierowa utracona przez operatora pocztowego lub otwarta przed zwróceniem do nadawcy.

W przypadku tego typu incydentów najczęściej do naruszeń dochodziło w wyniku działań operatora pocztowego. Można się zastanowić – dlaczego tego typu zdarzenie trafiło do

zestawienia, jeżeli nie my jesteśmy za nie odpowiedzialni? Nie można przecież przypisać za to naruszenie odpowiedzialności pracownikowi, który nadaje przesyłkę. Celem wysyłki korespondencji wybieramy zaufanego operatora pocztowego. Oczywiście jest w tym dużo racji, natomiast fakt faktem, iż do naruszenia doszło. Jak każde naruszenie, należy je przeanalizować i jeżeli wiązało się przynajmniej ze średnim ryzykiem naruszenia praw, należy je zgłosić do UODO, a być może poinformować osobę, której dane dotyczą. Ten obowiązek często jest ignorowany, czego konsekwencjami było wydanie decyzji Prezesa UODO o ukaraniu administratora w podobnej sprawie.

Błędy (w tym programistyczne) w systemach informatycznych.

Błędy zdarzają się każdemu. Można nadać zbyt szerokie uprawnienia tworząc nowe konto użytkownika, przypadkowo zmienić je u całej grupy użytkowników. Błąd może dotyczyć fazy wdrożeniowej, gdzie w wyniku pośpiechu zabrakło czasu na testy, czy zaistnieć nagle i niespodziewanie, po niedawno wprowadzonej aktualizacji. Wprowadzanie nowego modułu do rozbudowanej aplikacji, integracja kilku różnych systemów lub baz danych. Na każdym z etapów prac wdrożeniowych, zaczynających się już od planowania i analizy biznesowej, powinien być zaangażowany inspektor ochrony danych. Niezwykle istotne są również działania osób niezwiązanych ze światem IT, ale korzystających na co dzień z tych systemów. Najprawdopodobniej to zwykły użytkownik jako pierwszy ma szansę dostrzec błędy, które niezauważone przedostały się na produkcję. Istotna jest świadomość, iż w takiej sytuacji każdy z pracowników powinien niezwłocznie przekazać sprawę do IOD oraz działu IT/ producenta oprogramowania. Nie bądźmy bierni, gdyż szybka reakcja pozwala znacznie zminimalizować skutki i konsekwencje naruszeń.

Udostępnienie danych niewłaściwej osobie.

Najczęściej do tego typu naruszeń dochodziło poprzez wydawanie dokumentów niewłaściwej osobie (zaświadczeń, deklaracji podatkowych) czy w przypadku omyłkowo zaksięgowanych przelewów. Na pierwszy rzut oka to naruszenie jest zbieżne z poprzednim i… następnym. Tutaj natomiast problem dotyczy w większości sytuacji, gdy dane zostały przekazane osobie nieuprawnionej. Mogli nimi być pracownicy działający na własną rękę, bez stosownego upoważnienia, czy nawet pracownicy służb lub innych organów państwowych. Ostatecznie to człowiek jest najsłabszym ogniwem każdego z zabezpieczeń i to na nas spoczywa obowiązek nierzadko podwójnego sprawdzania i weryfikacji, czy ten, kto prosi o dane osobowe, rzeczywiście może je otrzymać.

Wysłanie korespondencji do niewłaściwego odbiorcy.

Ostatni, ale nie mniej ważny – korespondencja zawierająca dane osobowe przesłana zarówno tradycyjnie, listem, jak i na elektroniczną skrzynkę pocztową e-mail do niewłaściwego odbiorcy. Jeżeli do tej pory mieliśmy czyste sumienie, to ciężko będzie uwierzyć, iż nadal pozostaliśmy bez grzechu. Chyba każda osoba miała sytuację, gdy natychmiast po kliknięciu przycisku „wyślij” myszka momentalnie jakby poraziła nas prądem.

Sprawdzając folder wysłane, po chwili niepewności okazuje się, że wysłaliśmy e-mail pod zły adres tylko dlatego, że adresat miał tak samo na imię. Dużo trudniejsze do wykrycia są naruszenia, gdzie pomylone zostało adresowanie na kopercie i do przesyłki trafiła błędna korespondencja lub np. sklejone ze sobą kilka kartek, które pierwotnie miały zostać wysłane do różnych osób. Tutaj uratuje nas już tylko dwukrotne sprawdzanie, czy aby na pewno odpowiednio zaadresowaliśmy przesyłkę. Dużo łatwiej jest się uchronić przed tym najpopularniejszym naruszeniem w formie elektronicznej. Będzie to wymagało odrobinę wiedzy technicznej, lecz zawsze z pomocą przyjdzie najpopularniejsza wyszukiwarka lub Dział IT. Jest to całkowicie zmieniający nasze życie zawodowe lifehack. Gorąco polecam w programie pocztowym ustawić regułę opóźniania dostarczenia wszystkich wiadomości wychodzących o 1 minutę. Nie jest to wymóg RODO 😊natomiast uratuje nas przed potencjalnymi naruszeniami… jak również, przed zapominaniem o dołączeniu załącznika. Dwie pieczenie na jednym ogniu.

Podsumowanie

Wdrożenie RODO nie zagwarantuje nam, iż naruszenia znikną. Jest to ciągła praca polegająca na stosowaniu, ale też sprawdzaniu i poprawianiu naszych procedur. Pamiętajmy, że o każdym podejrzeniu naruszenia powinniśmy poinformować IOD. Nie zawsze musi to wiązać się z koniecznością zgłoszenia do Urzędu Ochrony Danych Osobowych. Wiele sytuacji może nie być naruszeniem lub powodować niskie ryzyko naruszenia praw. Najistotniejsze jest wykazanie, że mamy ochronę danych pod kontrolą i panujemy nad sytuacją. Każde takie wewnętrzne zgłoszenie da możliwość zorientowania się, czy wdrożone procedury działają poprawnie, czy może jest wymagana interwencja celem ich ulepszenia.

Ostatecznie, chodzi o to, żebyśmy i my, i nasze dane były bezpieczne.

Marcin Stryszko – specjalista ds. ochrony danych w iSecure Sp. z o.o.