# Ups... mamy naruszenie ochrony danych osobowych

Przygotowałem dla Ciebie kompendium wiedzy o radzeniu sobie z naruszeniami ochrony danych osobowych (dalej: naruszenie RODO). Komplet informacji przedstawiam w trzech częściach.

Z **pierwszej** części dowiesz się czym jest naruszenie RODO i jak mu zapobiegać. Opowiem Ci również o tym, jak powinna wyglądać skuteczna procedura raportowania o naruszeniach.

**Druga** część będzie poświęcona zgłaszaniu naruszeń organowi nadzorczemu. Dowiesz się z niej, które naruszenia powinieneś zgłaszać, a które nie. Opowiem Ci również o sposobie liczenia terminu 72h na zgłoszenie naruszenia. Dowiesz się także jak dokonać zgłoszenia naruszenia do UODO.

**Trzecia** i ostatnia część, będzie poświęcona informowaniu osób, których dotyczy naruszenie. Kiedy i w jaki sposób, powinniśmy poinformować poszkodowanych naruszeniami.

## Co to jest naruszenie ochrony danych osobowych

Zacznę od terminu naruszenia ochrony danych osobowych. Prawnicza definicja (legalna), została przedstawiona w art. 4 pkt. 12 RODO:

„***naruszenie bezpieczeństwa*** *prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych*"

Definicja jest bardzo, bardzo szeroka. Nie pozostawia zbyt dużo miejsca na wątpliwości czy interpretacje.

Dla porządku, przedstawiam jeszcze dwa oficjalne stanowiska i wytyczne w zakresie naruszeń: Urzędu Ochrony Danych Osobowych oraz Europejskiej Rady Ochrony Danych.

Urząd Ochrony Danych Osobowych:

- ✓ naruszenie musi **dotyczyć danych osobowych** przesyłanych, przechowywanych lub w inny sposób przetwarzanych przez podmiot, którego dotyczy naruszenie,
- ✓ skutkiem naruszenia może być **zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych**,
- ✓ naruszenie jest **skutkiem złamania zasad bezpieczeństwa danych.**

Więcej wytycznych polskiego organu nadzorczego znajdziesz w publikacji "Obowiązki administratorów związane z naruszeniami ochrony danych".

Europejska Rada Ochrony Danych, zwraca z kolei uwagę na to, że naruszenia możemy podzielić na trzy kategorie:

- ✓ **naruszenie dotyczące poufności danych** - dochodzi do nieuprawnionego lub przypadkowego ujawnienia lub nieuprawnionego dostępu do danych osobowych

  przykłady: *wydanie dokumentacji medycznej pacjenta innej nieuprawnionej osobie, wysłanie wiadomości mailowej zawierającej dane osobowe do innego odbiorcy niż była ona przeznaczona*,

- ✓ **naruszenie dotyczące integralności danych** - dochodzi do nieuprawnionego lub przypadkowego zmodyfikowania danych osobowych

  przykłady: *zmiana przez pracownika nazwiska wszystkich klientów poprzez dodanie do każdego na końcu litery „s"*

- ✓ **naruszenie dotyczące dostępności danych** - dochodzi do przypadkowego lub nieuprawnionego dostępu do danych osobowych lub zniszczenia danych osobowych

  przykłady: *atak hakerski, w wyniku którego Administrator danych osobowych traci dostęp do danych w systemie informatycznym, zgubienie laptopa/telefonu służbowego, na którym znajdują się dane klientów Administratora danych osobowych, przypadkowe lub zamierzone usunięcie danych osobowych klientów przez pracownika*

Uproszczę powyższe do absolutnego minimum. Jeśli coś złego wydarzy się z przetwarzanymi przez nas danymi osobowymi, to najprawdopodobniej możemy uznać, że nastąpiło naruszenie RODO.

Poniżej znajdziesz kilka praktycznych przykładów naruszeń, z którymi na co dzień mierzą się nasi eksperci.

**Małgorzata Zdunek, *ekspert ds. ochrony danych osobowych***

Wiele organizacji decyduje się na rozwiązania polegające na udostępnianiu różnego rodzaju dokumentów w obrębie swojej sieci lokalnej. Udostępniając zasób w sieci, administrator określa uprawnienia tj. kto i na jakich zasadach może korzystać z udostępnionego pliku lub folderu. I tutaj w wielu podmiotach „zaczynają się schody", a potem... naruszenia ochrony danych osobowych. Błędne określenie dostępu do folderu, czy też umieszczenie pliku z danymi w niewłaściwym miejscu, będzie prowadziło do udostępnienia danych osobowych nieuprawnionym osobom. Będziemy mieli zatem do czynienia z naruszeniem dotyczącym nie tylko poufności i dostępności danych, ale również ich integralności.

**Katarzyna Kmiecicka, *ekspert ds. ochrony danych osobowych***

Zdarzeniem, które bez żadnych wątpliwości zakwalifikujemy jako naruszenie ochrony danych osobowych, jest przekazanie dokumentacji medycznej niewłaściwemu pacjentowi. Mamy tutaj do czynienia z ujawnieniem danych osobie nieuprawnionej. Tego typu incydent wymaga podjęcia natychmiastowych i zdecydowanych działań, w szczególności z uwagi na fakt, że dokumentacja zawiera tzw. szczególne kategorie danych (informacje dotyczące staniu zdrowia).

## Co nie jest naruszeniem ochrony danych osobowych

Ponieważ definicja naruszenia RODO jest bardzo szeroka, znajdźmy sytuacje, których nie uznamy za naruszenia RODO.

Dane osobowe to nie jedyne informacje przetwarzane przez organizacje. Większość przedsiębiorców tworzy np. strategie sprzedażowe lub pracuje nad kampaniami wizerunkowymi.

Powyższe dane mogą być równie cenne i wartościowe co dane osobowe. Jednak z perspektywy RODO, zagubienie takich danych, nie będzie miało znaczenia.

Informacje o szczególnym znaczeniu dla organizacji, stanowią tzw. tajemnicę przedsiębiorstwa.

**Małgorzata Zdunek, *ekspert ds. ochrony danych osobowych***

Utratę jakiegokolwiek nośnika (np. laptopa, dysku zewnętrznego, pendrive'a) należy traktować jako potencjalne naruszenie ochrony danych osobowych. Może się jednak okazać, że na utraconym sprzęcie nie zapisano żadnych informacji, które byłyby danymi osobowymi (również w formie spseudonimizowanej). Tylko dobrze przeprowadzone postępowanie sprawdzające pozwoli na ustalenie, że w rzeczywistości na pendrive znajdowały się np. informacje o wynikach sprzedaży za ubiegły kwartał. Do naruszenia RODO zatem nie doszło.

**Krystian Dobosz, *starszy specjalista ds. ochrony danych osobowych***

Wysłanie maila na niewłaściwy adres e-mail, choć z reguły kojarzy się z naruszeniem ochrony danych osobowych, nie zawsze nim będzie. Przesłanie wiadomości z samą informacją, że „Twoja reklamacja została rozpatrzona pozytywnie, czeka na Ciebie do odbioru nowy towar. Zapraszamy do sklepu", nie powoduje ujawnienia danych osobowych i zagrożenia dla praw osoby, która powinna być właściwym adresatem korespondencji.

Dlatego tak istotne jest przeprowadzenie rzetelnej analizy danego przypadku i udokumentowanie swojej decyzji, tak by w przypadku kontroli przez Urząd Ochrony Danych Osobowych można było umotywować podjętą decyzję o stwierdzeniu lub braku stwierdzenia naruszenia.

**Tomasz Wasilczyk, *starszy specjalista ds. ochrony danych osobowych***

Dokonując oceny czy w danym stanie faktycznym doszło do naruszenia ochrony danych osobowych należy być bardzo ostrożnym oraz podchodzić z dużą rozwagą. Czasem może się okazać, że pomimo wystąpienia pewnego niepożądanego zdarzenia nie dojdzie do naruszenia przepisów RODO. Przykładem może być sytuacja, w której pracownik zgubi nośnik danych np. dysk zewnętrzny, ale w ramach postępowania sprawdzającego okaże się, że po pierwsze, zagubiony nośnik był zaszyfrowany w sposób w ogóle uniemożliwiający odczyt osobie postronnej, a ponadto na zagubionym nośniku nie znajdowały się informacje dotyczące osób fizycznych, lecz dane dotyczące osób prawnych.

## Kto będzie moim źródłem informacji o naruszeniu?

Jeśli jesteś Inspektorem Ochrony Danych lub osobą odpowiedzialną za obszar RODO, to niestety, większości naruszeń nie wykryjesz samodzielnie.

Dowiesz się o nich od innych pracowników organizacji lub bezpośrednio od osób pokrzywdzonych. Nam zdarzyły się też sytuacje, kiedy np. hakerzy sami donosili o nienależytym zabezpieczeniu serwisu internetowego.

Nie możesz jednak liczyć tylko na dobrą wolę Twoich współpracowników. Żeby przepływ informacji działał w praktyce, potrzebne są dwa elementy:

1) dobrze napisana **procedura dotycząca raportowania incydentów**,

2) **skuteczne zakomunikowanie procedury** wszystkim pracownikom organizacji.

## Procedura raportowania naruszeń w mojej organizacji

Zaczniemy od samej procedury. Na potrzebę jej wdrożenia, wskazuje motyw 87 Preambuły RODO:

*„Należy się upewnić, czy wdrożono wszelkie odpowiednie techniczne środki ochrony i wszelkie **odpowiednie środki organizacyjne**, by od razu stwierdzić naruszenie ochrony danych osobowych i szybko poinformować organ nadzorczy i osobę, której dane dotyczą."*

Rekomenduję, aby procedura raportowania o incydentach, była częścią Polityki ochrony danych osobowych w Twojej organizacji. Więcej o samej Polityce dowiesz się tutaj.

## Elementy procedury naruszeń ochrony danych osobowych

### 1. Informacje na temat tego jak pracownik, który wykrył naruszenie powinien się zachować

W pierwszej kolejności pracownik powinien wiedzieć kogo i jak szybko poinformować. Najlepiej określić, że kontakt powinien nastąpić niezwłocznie. Na przykład maksymalnie w przeciągu godziny od wystąpienia niepożądanego zdarzenia.

Poinformowane powinny zostać osoby zajmujące się ochroną danych osobowych w organizacji np. IOD, pracownik ds. ochrony danych osobowych, ale również, jeśli zdarzenie związane jest z kwestiami IT, Administrator Systemów Informatycznych, czy tez po prostu informatyk.

Warto określić w procedurze sposób komunikacji naruszenia, np. bezpośrednio wskazanym wyżej osobom lub pośrednio przez przełożonych. Dobrym pomysłem jest też wskazanie konkretnego kanału komunikacji, np. adresu email służącego do zgłaszania incydentów.

### 2. Zakres informacji jakie powinien przekazać pracownik informując o naruszeniu

Pracownicy powinni dostać jasne wytyczne, jakie informacje o naruszeniu, powinni przekazać osobom odpowiedzialnym. Jest to niezwykle ważne z perspektywy właściwego rozpoczęcia postępowania sprawdzającego. Dzięki wyczerpującemu raportowi, już na etapie przyjęcia zgłoszenia można stwierdzić z jakiego typu naruszeniem mamy do czynienia.

Powiadomienie o naruszeniu powinno zawierać przede wszystkim:

- ✓ czas i miejsce naruszenia,
- ✓ kategorie danych oraz przybliżoną liczbę osób, których dotyczy naruszenie,
- ✓ opis naruszenia,
- ✓ możliwe konsekwencje naruszenia,

- ✓ informacje o ewentualnym podjęciu środków zaradczych.

Warto określić również, jak pracownik powinien zachować się do czasu, aż na miejsce naruszenia przybędą osoby odpowiedzialne (zabezpieczenie dostępu do miejsca, wstrzymanie pracy na sprzęcie, etc.).

Opisane powyżej kroki 1 i 2, dotyczą szeregowych pracowników, którzy przetwarzają dane osobowe. Procedura powinna zawierać również informacje o tym, co dzieje się dalej.

### 3. Kto jest odpowiedzialny za koordynowanie postępowania w zakresie naruszenia

W praktyce często będzie to Inspektor Ochrony Danych lub inna osoba odpowiedzialna za RODO w organizacji. Może to być również ktoś, kto koordynuje przetwarzanie danych osobowych w ramach infrastruktury IT (np. ASI). Procedura powinna określać także formy współpracy z tymi osobami i zobowiązywać innych pracowników do udzielania im wszelkich niezbędnych wyjaśnień w zakresie stwierdzonego naruszenia.

### 4. W jaki sposób i na jakiej podstawie następuje ocena ryzyka naruszenia

Wdrażana przez Ciebie procedura powinna zawierać również wskazówki co do sposobu analizy, czy incydent może powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą.

Właściwe określenie tego ryzyka da Ci odpowiedź na pytanie, czy naruszenie kwalifikuje się do zgłoszenia Prezesowi UODO, a także czy istnieje konieczność zawiadamiania o naruszeniu osób, których danych ono dotyczy.

### 5. W jaki sposób dokumentuje się naruszenia

Wystąpienie każdego naruszenia powinno być w odpowiedni sposób udokumentowane. Z każdego postępowania sprawdzającego Inspektor Ochrony Danych (lub inna osoba odpowiedzialna) powinien sporządzić protokół.

Niezależnie od tego czy naruszenie zostanie zgłoszone do organu, fakt jego zaistnienia powinien zostać odnotowany również w rejestrze naruszeń.

### 6. Dodatkowe, indywidualne elementy

W niektórych sytuacjach w procedurę włączymy dodatkowe osoby lub instytucje. U niektórych klientów musieliśmy włączyć w procedurę ubezpieczyciela. Ubezpieczyciel chciał być poinformowany o każdym naruszeniu. Brak informacji mógł skutkować odmową wypłaty odszkodowania.

W dużych grupach kapitałowych zdarza się często, że o naruszeniu musimy poinformować globalnego Inspektora Ochrony Danych.

## Zakomunikuj procedurę zespołowi

Samo wdrożenie procedury nie zagwarantuje nam skutecznego przepływu informacji. Pierwszym krokiem ku skutecznemu zakomunikowaniu procedury jest szkolenie. Blok poświęcony naruszeniom, może być częścią większego szkolenia z zakresu RODO. Zgłaszanie naruszeń będzie jednym z kluczowych elementów szkolenia oraz ogólnie pojętej RODO świadomości. Więcej na temat RODO szkoleń i budowania świadomości, dowiesz się tutaj.

Podstawowe informacje i ścieżka postępowania podczas incydentu powinny być łatwo dostępne dla pracowników. Dzięki temu w awaryjnej sytuacji, będą mogli wrócić do zaprezentowanej w trakcie szkolenia wiedzy.

Dlatego warto zamieścić materiały informacyjne np. w intranecie, na dysku wspólnym lub wysłać w postaci materiałów informacyjnych na skrzynki mailowe pracowników.

Zdecydowanie warto omawiać zaistniałe incydenty. Zwłaszcza te o powtarzalnym charakterze. Możesz im poświęcić odrębne szkolenie w formie case-study. Możesz również informować zespół o takich sytuacjach na łamach gazetki zakładowej, w formie Newslettera czy innej komunikacji, przyjętej w Twojej organizacji.

## Zbuduj bezpieczną przestrzeń komunikacji

Jest jeszcze jeden ważny element komunikowania naruszeń. Pracownik zgłaszający naruszenie, musi czuć się bezpiecznie. Jeśli kwestie zgłaszania naruszeń przedstawisz w sposób bardzo restrykcyjny, koncentrując się na straszeniu i karach dla winnych, to o wielu naruszeniach możesz się nigdy nie dowiedzieć. Albo co gorsza, dowiesz o nich dopiero od poszkodowanych klientów.

Promuj więc zgłaszanie, a nie karanie winnych naruszeniom. Oczywiście świadome naruszenia zasad bezpieczeństwa powinny być karane. Statystyki pokazują jednak, że większość naruszeń, to nieświadome ludzkie błędy.

## Znajdź sobie sojuszników

Naruszenie zawsze jest sytuacją stresującą. Nie działaj sam! Zbuduj wokół siebie sztab kryzysowy, który pomoże Ci zminimalizować skutki naruszenia. W wielu sytuacjach, osoby dotknięte naruszeniem mogą próbować wyolbrzymiać swoje krzywdy, domagając się nieadekwatnie wysokich odszkodowań. Może nastąpić również sytuacja odwrotna. Naruszenie z Twojej perspektywy wyda Ci się niewielkie, tymczasem dla poszkodowanej osoby będzie ono obiektywnie bardzo poważne.

Pamiętaj o tym, że w sytuacji kryzysowej, nie działasz do końca racjonalnie. Niektórzy wyolbrzymiają kryzys, stresując się nadmiarowo. Inni nie dostrzegają zagrożeń, wierząc, że na pewno wszystko będzie dobrze.

Jeśli chcesz poznać obiektywne spojrzenie eksperta z zewnątrz, zapraszam na konsultacje kryzysowe. Gwarantuję, że poczujesz dużą ulgę. Usłyszysz, jakie spojrzenie na naruszenie ma osoba z zewnątrz. Dowiesz się również co można zrobić, aby zminimalizować negatywne skutki naruszenia.

### Wsparcie przy RODO naruszeniu

Jeśli właśnie mierzysz się z trudną sytuacją, jaką jest RODO naruszenie, pomożemy Ci. Być może wyzwanie z którym się mierzysz, wcale nie jest tak poważne, jak Ci się wydaje. Albo odwrotnie, sytuacja, która wydaje się być błaha, wymaga szybkich i zdecydowanych działań z Twojej strony. Daj sobie pomóc. Nasz ekspert pozwoli Ci urealnić sytuację w której się znajdujesz.

W toku naszej pracy wspieraliśmy organizacje przy ponad 50 naruszeniach RODO.

Koszt konsultacji: 300 zł netto / h.

**Wypełnij poniższy formularz i zgłoś potrzebę konsultacji przy naruszeniu (dyżurujemy również w weekendy, odpowiemy w ciągu maksymalnie 2 godzin).**

FORMULARZ

Przy naruszeniach o dużej skali, może przydać Ci się pomoc osób z doświadczeniem w zakresie PRu. Zwłaszcza jeśli chodzi o informowanie poszkodowanych o zaistniałym naruszeniu. Jeśli poinformujesz poszkodowanych w sposób nieporadny, możesz sprowokować klientów do ataku. I odwrotnie, jeśli o sytuacji kryzysowej poinformujesz poszkodowanych w odpowiedni sposób, klienci to docenią. W efekcie może się okazać, że mimo sytuacji kryzysowej, Twoja organizacja wyjdzie z niej silniejsza, obdarzona większym zaufaniem.

## Najczęstsze przyczyny naruszeń ochrony danych osobowych

Jeśli chodzi o przyczyny naruszeń, to poruszaliśmy już ten temat na naszym blogu.

Odsyłam także do raportu Związku Firm Ochrony Danych Osobowych. Raport w wyczerpujący sposób odnosi się do źródeł RODO naruszeń.

Nie wchodząc w szczegóły, o których już pisaliśmy, najczęstszą przyczyną naruszeń są niezawinione błędy ludzkie. Stąd tak istotne jest odpowiednie zakomunikowanie procedury oraz szkolenie z zakresu bezpiecznego przetwarzania danych osobowych.

## Podsumowanie

Wiesz już czym jest naruszenie i jak zbudować odpowiednie procedury aby je wykryć. Z kolejnego artykułu dowiesz się w jaki sposób postępować dalej. Czy zaistniałe naruszenie podlega obowiązkowi zgłoszenia do Urzędu Ochrony Danych Osobowych.

Nie daj się przytłoczyć sytuacją. Działaj, szukaj wsparcia, szukaj rozwiązań.

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 roku (jako IOD)
- wsparcie administratorów danych osobowych, którego udzielaliśmy jako Lex Artist w ponad 50 naruszeniach