**NARUSZENIE OCHRONY DANYCH OSOBOWYCH** to Incydent bezpieczeństwa prowadzący do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych

NARUSZENIE OCHRONY DANYCH OSOBOWYCH to niemożność zapewnienia zgodności z zasadami dotyczącymi przetwarzania danych osobowych ustanowionymi w RODO

INCYDENT BEZPIECZEŃSTWA to losowe zewnętrzne (np. pożar prowadzący do utraty dokumentów papierowych zawierających dane osobowe) lub wewnętrzne (np. zgubienie pendrive, na którym były zapisane dane osobowe).

O charakterze umyślnym, zarówno zewnętrzne (np. atak, którego skutkiem jest nieuprawniony dostęp do systemów informatycznych) jak i wewnętrzne (np. kradzież dokumentacji z danymi przez pracownika)

Naruszenie ochrony danych osobowych może być zatem dokonane poprzez:

1. Naruszenie poufności danych – dochodzi do nieuprawnionego lub przypadkowego ujawnienia lub nieuprawnionego dostępu do danych osobowych
2. Naruszenie integralności danych - dochodzi do nieuprawnionego lub przypadkowego zmodyfikowania danych osobowych
3. Naruszenie dostępności danych – dochodzi do przypadkowej lub nieuprawnionej utraty dostępu do danych osobowych lub zniszczenia danych osobowych

WYSTĄPIENIE NARUSZENIA danych osobowych następuje w momencie, w którym administrator uzyskuje wystarczającą dozą pewności, że doszło do wystąpienia incydentu bezpieczeństwa, który doprowadził do naruszenia ochrony danych osobowych

Przykłady incydentów bezpieczeństwa skutkujących naruszeniem danych osobowych:

1. Naruszenie poufności danych

Rodzice krytycznie chorych dzieci mogą być celem osób, które chcą czerpać korzyści z ich słabości (np. szarlatani)

1. Naruszenie integralności danych

Utracone dane mogą zakłócić leczenie co może doprowadzić do nasilenia się lub nawrotu choroby

1. Naruszenie dostępności danych

Może nastąpić nieuzasadnione opóźnienie przyznania pomocy finansowej lub jej odmowa, mająca negatywne skutki finansowe dla rodzin leczonych dzieci

W jaki sposób można dokonać naruszenia ochrony danych osobowych w postaci naruszenia dostępności?

Chodzi w tym wypadku o takie zdarzenia, jak przypadkowe usunięcie danych osobowych lub utrata możliwości odszyfrowania zaszyfrowanych danych osobowych, jeżeli stanowi ryzyko dla praw i wolności podmiotów danych. Warto mieć na uwadze, że również przejściowa utrata dostępności może być uznana za naruszenie ochrony danych osobowych.

**Obowiązek zgłaszania naruszeń**

Zgodnie z motywami RODO przy braku odpowiedniej i szybkiej reakcji naruszenie ochrony danych osobowych może skutkować powstaniem uszczerbku fizycznego, szkód majątkowych lub niemajątkowych u osób fizycznych, takich jak utrata kontroli nad własnymi danymi osobowymi lub ograniczenie praw, dyskryminacja, kradzież lub sfałszowanie tożsamości, strata finansowa, nieuprawnione odwrócenie pseudonimizacji, naruszenie dobrego imienia, naruszenie poufności danych osobowych chronionych tajemnicą zawodową lub wszelkie inne znaczne szkody gospodarcze lub społeczne.

Stąd też RODO przewiduje, że po stwierdzeniu naruszenia ochrony danych osobowych administrator powinien zgłosić je organowi nadzorczemu bez zbędnej zwłoki: jeżeli to wykonalne, nie później niż 72 godziny po zauważeniu naruszenia.

Administrator może nie dokonywać zgłoszenia, jeżeli jest w stanie wykazać zgodnie z zasadą rozliczalności, że jest mało prawdopodobne, by naruszenie to mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych.

Zgłoszenie naruszenia ochrony danych osobowych musi w szczególności:

* opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
* zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
* opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
* opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu na weryfikowanie przestrzegania przepisów RODO.

Zawiadomienie o naruszeniu osoby, której dane dotyczą

Zgodnie z motywami RODO administrator powinien bez zbędnej zwłoki poinformować osobę, której dane dotyczą, o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia jej praw lub wolności, tak aby umożliwić jej podjęcie niezbędnych działań zapobiegawczych.

Informacja taka powinna zawierać opis charakteru naruszenia ochrony danych osobowych oraz zalecenia dla danej osoby fizycznej w kwestii minimalizacji potencjalnych niekorzystnych skutków.

Informacje należy przekazywać osobom, których dane dotyczą, tak szybko, jak jest to rozsądnie możliwe, w ścisłej współpracy z organem nadzorczym, z poszanowaniem wskazówek przekazanych przez ten organ lub inne odpowiednie organy, takie jak organy ścigania.

Zawiadomienie osoby, której dane dotyczą, powinno zostać sporządzone jasnym i prostym językiem i opisywać charakter naruszenia ochrony danych osobowych.

Zawiadomienie nie jest jednak wymagane w następujących przypadkach:

* 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 do dostępu do tych danych osobowych;
* administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa wyżej;
* wymagałoby ono niewspółmiernie dużego wysiłku, przy czym w takiej sytuacji wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

Konsekwencje naruszenia ochrony danych osobowych

Administrator powinien się upewnić, że wdrożył 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.

Jeśli administrator nie zawiadomi osób, których dane dotyczą, o naruszeniu ochrony danych osobowych lub nie zgłosi tego faktu organowi nadzorczemu, organ nadzorczy może nałożyć sankcje na administratora, w tym ma prawo zastosować względem niego administracyjną karę pieniężną.

**Obowiązek zgłoszenia naruszenia danych osobowych**

W związku z wystąpieniem tzw. incydentu bezpieczeństwa administrator jest zobowiązany do zgłaszania naruszeń do organu nadzorczego.

W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin od stwierdzenia naruszenia – zgłasza je organowi nadzorczemu, właściwemu zgodnie z art. 55 RODO, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Oznacza to, że nie każde naruszenie przepisów o ochronie danych osobowych stanowi a priori naruszenie danych osobowych. Jeżeli wystąpią takie przesłanki legalizacyjne (małe prawdopodobieństwo, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych), to nie ma obowiązku zgłaszania naruszeń. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia (art. 33 ust. 1 RODO).

Ryzyko naruszenia praw i wolności może wystąpić w sytuacji takiego naruszenia ochrony danych osobowych, w wyniku którego może nastąpić:

– strata finansowa;

– kradzież lub fałszowanie tożsamości;

– dyskryminacja;

– utrata poufności danych osobowych chronionych tajemnicą zawodową, w tym szczególnych danych osobowych, jak dane dotyczące zdrowia;

- naruszenie dóbr osobistych – np. poprzez upublicznienie;

W Polsce funkcję organu nadzorczego spełnia Prezes Urzędu Ochrony Danych Osobowych (dalej – UODO).

Z wyżej wskazanego przepisu wynika, że nie każde naruszenie ochrony danych osobowych będzie nakładało na administratora obowiązek zgłoszenia faktu naruszenia do UODO. Może bowiem się zdarzyć, iż będzie mało prawdopodobne, by naruszenie skutkowało ryzykiem naruszeniem praw lub wolności osób fizycznych.

Przykładem takiej sytuacji może być zgubienie służbowego przenośnego dysku, na którym znajdowały się wrażliwe dane klientów. Pod warunkiem jednak, że był w odpowiedni sposób zabezpieczony (na przykład skomplikowanym hasłem dostępu). Istnieją wtedy bowiem małe szanse, że osoby do tego niepowołane uzyskają dostęp do wrażliwych danych.

W każdym innym przypadku, to jest wtedy gdy istnieje prawdopodobieństwo, iż naruszenie ochrony danych osobowych może skutkować ryzykiem naruszenia praw lub wolności osób fizycznych, podmiot przetwarzający – jeżeli to u niego nastąpiło naruszenie – jest zobowiązany poinformować o tym fakcie administratora, który to z kolei musi zgłosić fakt naruszenia do Urzędu Ochrony Danych Osobowych (art. 33 ust. 1 i 2 RODO).

**Jakie elementy powinno zawierać zgłoszenie z art. 33 ust. 1 RODO?**

Zgłoszenie o którym mowa w art. 33 ust. 1 RODO, czyli zgłoszenie naruszenia ochrony danych osobowych powinno co najmniej:

a) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;

b) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;

c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;

d) opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

Jeżeli administrator nie będzie w stanie wszystkich informacji udzielić w tym samym czasie, będzie mógł je dostarczać później, ale bez zbędnej zwłoki. W takim wypadku należy poinformować Urząd Ochrony Danych Osobowych o przeszkodach w tym zakresie i wskazać prawdopodobny termin, w którym informacje zostaną udzielone.

**W jaki sposób zgłosić naruszenie?**

Naruszenie ochrony danych osobowych można zgłosić na dwa sposoby – elektronicznie lub tradycyjnie – w formie formularza wysłanego na adres Urzędu Ochrony Danych Osobowych. W pierwszym kroku należy pobrać interaktywny formularz, który jest dostępny na stronie UODO. Po jego wypełnieniu można go wysłać na trzy sposoby, a mianowicie poprzez skrzynkę podawczą EPUAP, za pomocą pisma ogólnego, dostępnego na specjalnej platformie elektronicznej lub tradycyjnie pocztą.

Zawiadamianie osoby, której dane dotyczą, o naruszeniu danych osobowych

Jeżeli naruszenie danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu (art. 34 ust. 1 RODO)

Takie zawiadomienie powinno być napisane jasnym i prostym językiem, a nadto winno opisywać charakter naruszenia ochrony danych osobowych oraz powinno:

– zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;

– opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;

– opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

Istnieją jednak wyjątki od obowiązku informacyjnego względem osoby fizycznej, której dane dotyczą. Powyższe zawiadomienie nie jest wymagane, w następujących przypadkach:

a) 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 do dostępu do tych danych osobowych;

b) administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w ust. 1;

c) wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

Jeżeli administrator nie zawiadomił jeszcze osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, Urząd Ochrony Danych Osobowych – biorąc pod uwagę prawdopodobieństwo, że to naruszenie ochrony danych osobowych spowoduje wysokie ryzyko – może nałożyć na administratora obowiązek zawiadomienia osoby, której dane dotyczą lub może stwierdzić, że został spełniony jeden z warunków, o których mowa powyżej.

**Co grozi w przypadku nie zgłoszenia naruszeń, czyli nie spełnienie obowiązku notyfikacyjnego?**

Za nie zgłoszenie naruszenia danych osobowych grozi kara pieniężna.

**Jakie okoliczności będą brane pod uwagę przy wymierzaniu kary w przypadku stwierdzenia naruszenia?**

– charakter i waga naruszenia;

– czas trwania naruszenia;

– liczba poszkodowanych osób i rozmiar poniesionych przez nich szkody;

– rodzaj danych osobowych, których dotyczyło naruszenie;

– rodzaj i zakres działań podjętych w związku z naruszeniem;

– stopień odpowiedzialności administratora danych osobowych;

– stopień współpracy administratora danych osobowych z organem;

– sposób w jaki organ nadzorczy dowiedział się o naruszeniu, w szczególności czy administrator sam zgłosił naruszenie, czy też zrobiła to osoba trzecia;

– brak wdrożenia środków zapewniających bezpieczeństwo przetwarzania danych osobowych.

**Jakie okoliczności wpływają łagodząco na wysokość kary?**

Te okoliczności to:

– nieumyślność naruszenia i niezgłoszenia,

– okoliczność, że nie stwierdzono w następstwie naruszenia żadnych szkód po stronie osób, których dotyczyły objęte postępowaniem naruszenia ochrony danych osobowych

– okoliczność, że w trakcie postępowania w przedmiocie nałożenia na kary pieniężnej, podmiot dokonał w procedurze zawiadamiania Prezesa UODO o naruszeniach danych osobowych zmian mających na celu wyeliminowanie możliwości zaistnienia  w przyszłości naruszenia podlegającego ukaraniu.

**Jakie kary nakładał Prezes Urzędu Ochrony Danych Osobowych w konkretnych sprawach?**

Naruszenia przepisów podlegają administracyjnej karze pieniężnej w wysokości do 10 000 000 EUR, a w przypadku przedsiębiorstwa – w wysokości do 2 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego

**Podsumowanie**

W przypadku naruszenia ochrony danych osobowych na administratorze ciąży szereg bardzo ważnych obowiązków – poczynając od przeprowadzenia wewnętrznego postępowania, którego celem będzie ustalenie, czy rzeczone naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych, skończywszy na obowiązku poinformowania o tym fakcie Urzędu Ochrony Danych Osobowych oraz osoby, której dane te dotyczą.

Umiejętne radzenie sobie z incydentami bezpieczeństwa może Państwa uchronić przed negatywnymi skutkami prawnymi wynikającymi z naruszenia ochrony danych osobowych, dlatego tak ważne jest, żeby nie bagatelizować sprawy i postąpić zgodnie z literą prawa.

**Kiedy bezwzględnie trzeba zgłosić naruszenie**

W toku wcześniejszych rozważań zaznaczyliśmy, że administrator powinien zgłaszać organowi nadzorczemu każdy przypadek naruszenia ochrony danych osobowych, chyba że „jest mało prawdopodobne, by incydent skutkował ryzykiem naruszenia praw lub wolności osób fizycznych”. Oznacza to, że jeżeli ryzyko naruszenia praw lub wolności osób fizycznych nie występuje lub jest niewielkie, z powiadomienia można zrezygnować. W tym momencie powstaje jednak pytanie: jak stwierdzić, czy takie ryzyko istnieje, a jeżeli istnieje, to jaka jest jego skala? Pewne wskazówki w tym zakresie odnajdujemy w motywie 75 RODO. Co z nich wynika? Przede wszystkim to, że ryzyko naruszenia praw lub wolności osób jest następstwem takiego przetwarzania danych osobowych, które może prowadzić do uszczerbku fizycznego lub szkód majątkowych lub niemajątkowych. Chodzi tu zwłaszcza o sytuacje, w których:

1. osoby, których dane dotyczą, mogą zostać pozbawione przysługujących im praw lub wolności lub możliwości sprawowania kontroli nad swoimi danymi osobowymi;
2. przetwarzaniu podlegają dane szczególnie chronione, czyli dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, wyznanie, przekonania światopoglądowe lub przynależność do związków zawodowych, a także dane genetyczne, dotyczące zdrowia, seksualności, wyroków skazujących i czynów zabronionych lub związanych z tym środków bezpieczeństwa;
3. dochodzi do zautomatyzowanego przetwarzania danych, w tym profilowania;
4. przetwarzane są dane osób wymagających szczególnej opieki, zwłaszcza dzieci;
5. przetwarzanie danych odbywa się na dużą skalę i wpływa na znaczną liczbę osób, których dane dotyczą.

**Wagę naruszeń** można obliczyć z uwzględnieniem następujących czynników:

* Kontekst Przetwarzania Danych (KPD) – pozwala na określenie, jakie kategorie danych są związane z naruszeniem (np. podstawowe, szczególne, finansowe, poufne) oraz czynniki mające wpływ na ten kontekst (np. czas trwania naruszenia, zakres danych, liczba osób, których dotyczy naruszenie, publiczna dostępność danych);
* Prawdopodobieństwo Identyfikacji (PI) – umożliwia wskazanie stopnia łatwości zidentyfikowania osoby, której naruszone dane dotyczą przez osobę, która weszła w ich posiadanie;
* Okoliczności Naruszenia (ON) – ułatwia ustalenie czy wystąpiły takie okoliczności, jak naruszenie poufności, integralności, dostępności danych osobowych, a także czy sprawca działał intencjonalnie.