OBOWIĄZKI ZWIĄZANE Z NARUSZENIEM OCHRONY DANYCH OSOBOWYCH

Co to jest naruszenie danych osobowych?
Przez pojęcie „naruszenia ochrony danych" należy rozumieć „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" (art. 4 pkt 12 RODO).
Aby zaistniało naruszenie muszą być spełnione łącznie trzy przesłanki:

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

Jednocześnie jak wskazuje Grupa Robocza Art. 29 można wyróżnić trzy typy naruszenia ochrony danych osobowych:

- naruszenie poufności – polega na ujawnieniu danych osobowych nieuprawnionej osobie;

Przykład: „Przypadkowe wysłanie danych osobowych klienta do niewłaściwego działu firmy lub osoby postronnej."

- naruszenie dostępności – polega na trwałej utracie lub zniszczeniu danych osobowych;

Przykład I: „Zgubienie lub kradzież nośnika zawierającego kopię bazy danych klientów administratora."
Przykład II: „Pracownik przypadkowo lub osoba nieupoważniona celowo usuwa dane ze zbioru. Administrator próbuje odzyskać dane z kopii zapasowej, jednak jego działania nie przynoszą rezultatu."

- naruszenie integralności – polega na zmianie treści danych osobowych w sposób nieautoryzowany.

Przykład: „Pracownik dla żartu zmienia nazwiska klientów poprzez dopisanie litery „s" na końcu każdego z nich."

Jakie informacje musi zawierać zgłoszenie o naruszeniu kierowane do Prezesa UODO?
Zgodnie z art. 33 ust. 3 RODO, administrator powinien wskazać w zgłoszeniu naruszenia następujące informacje:

- opis charakteru naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazanie kategorii i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
- wskazanie imienia i nazwiska oraz danych kontaktowych inspektora ochrony danych lub oznaczenia innego punktu kontaktowego, od którego można uzyskać więcej informacji;
- opis możliwych konsekwencji naruszenia ochrony danych osobowych;
- wskazanie środków, jakie zostały 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.
-

Jakie obowiązki w związku z naruszeniami danych osobowych przewiduje RODO?
RODO przewiduje następujące obowiązki związane z naruszeniem danych osobowych:

- wprowadzenie procedur umożliwiających stwierdzanie i ocenę naruszeń pod kątem wystąpienia ryzyka naruszenia praw i wolności osób fizycznych;
- prowadzenie wewnętrznej ewidencji naruszeń;
- zgłaszanie naruszeń organowi nadzorczemu;
- powiadamianie osoby, której dane dotyczą o naruszeniu;
- podejmowanie działań mających na celu przeciwdziałanie skutkom naruszenia i zapobieganie im w przyszłości.

Ważnym, jeśli nie najważniejszym, elementem całego procesu związanego ze zgłaszaniem naruszenia ochrony danych, jest szybkość podjęcia niezbędnych działań, zarówno wobec organu nadzorczego, jak i osób, których dane dotyczą. Czas ma tu bardzo duże znaczenie.

Aby zapewnić działania bez zbędnej zwłoki administratorzy powinni więc opracować i wdrożyć procedury postępowania na wypadek wystąpienia naruszenia ochrony danych. Taka procedura pomoże ujednolicić, usprawnić oraz przyśpieszyć działania w przypadku wykrycia naruszenia ochrony danych. W tej procedurze powinno się zawrzeć m.in.:

- cel, w jakim procedura została opracowana;
- zakres jej stosowania;
- katalog ewentualnych zagrożeń i naruszeń, jakie mogą wystąpić w związku z przetwarzaniem danych u konkretnego administratora;
- opis etapów zarządzania naruszeniem, począwszy od jego wykrycia, a kończąc na usunięciu;
- opis postępowania personelu administratora w przypadku wystąpienia naruszenia ochrony danych.

Dobrze zaprojektowana i wdrożona procedura postępowania na wypadek wystąpienia naruszenia ochrony danych pozwoli administratorowi przeprowadzić, w przypadku wykrycia przez niego naruszenia ochrony danych, szybką i prawidłową ocenę naruszeń, pod kątem wystąpienia ryzyka naruszenia praw i wolności osób fizycznych.
Procedura pozwala dokonać klasyfikacji zidentyfikowanych naruszeń ochrony danych, czyli określić poziom wystąpienia ryzyka naruszenia praw i wolności osób fizycznych, tj. niski, średni lub wysoki. W zależności, z jakim poziomem ryzyka naruszenia praw i wolności osób fizycznych administrator ma do czynienia, inaczej kształtują się jego obowiązki w stosunku do organu nadzorczego, a także osób, których dane dotyczą. Jeżeli w wyniku analizy administrator stwierdził, że ma do czynienia z niskim ryzykiem naruszenia praw i wolności osób fizycznych, nie jest on zobligowany do zgłoszenia naruszenia Prezesowi Urzędu Ochrony Danych Osobowych. Wskazane naruszenie musi jedynie wpisać do wewnętrznej ewidencji naruszeń. W przypadku stwierdzenia średniego ryzyka naruszenia praw i wolności osób fizycznych, obowiązkiem administratora jest zgłoszenie naruszenia ochrony danych Prezesowi UODO, jak również umieszczenie wpisu w wewnętrznej ewidencji naruszeń. Wystąpienie wysokiego ryzyka naruszenia praw i wolności osób fizycznych, oprócz wpisu w ewidencji naruszeń, wymaga od administratora powzięcia odpowiednich działań, zarówno wobec organu nadzorczego (zgłoszenie naruszenia ochrony danych), ale także w niektórych przypadkach również wobec osób, których dane dotyczą. W przypadku naruszeń, które mogą powodować wysokie ryzyko naruszenia praw lub wolności osoby, której dane dotyczą, RODO wprowadza bowiem dodatkowy obowiązek niezwłocznego zawiadomienia podmiotu danych przez administratora, chyba, że ten podjął działania prewencyjne przed zaistnieniem naruszenia albo działania zaradcze po wystąpieniu naruszenia (art. 34 ust. 3 RODO).
Niezależnie od poziomu ryzyka, administrator zobowiązany jest do wprowadzenia środków zaradczych mających na celu zminimalizowanie ryzyka i zabezpieczenia danych osobowych.

Przykłady naruszeń

Przykład: „W wyniku przerwy w dostawie prądu lub ataku typu blokada usług, administrator tymczasowo lub trwale traci dostęp do danych osobowych."

W powyższym przykładzie mamy do czynienia ze zdarzeniem skutkującym utratą dostępności danych osobowych przez pewien odcinek czasu. Jest to naruszenie, ponieważ brak dostępu do danych może mieć znaczący wpływ na prawa i wolności osób fizycznych. Pamiętać należy jednak, że nie każda czasowa niedostępność do danych jest naruszeniem. Jest nią tylko taka niedostępność danych, która może stanowić ryzyko dla praw i wolności osób fizycznych, np. w przypadku szpitala brak dostępu danych pacjentów może prowadzić do uniemożliwienia przeprowadzenia operacji medycznej, a zatem narażenia życia, co należy zaklasyfikować jako wysokie ryzyko dla praw i wolności osób fizycznych. W przypadku kilkugodzinnego braku dostępu spółki medialnej do swoich systemów i niemożliwości wysyłania newslettera do abonentów, istnieje natomiast niskie prawdopodobieństwo naruszenia praw i wolności osób fizycznych. Podobnie w przypadku planowanej konserwacji systemu, dane osobowe mogą być niedostępne przez pewien czas i nie należy traktować tego jako naruszenia bezpieczeństwa (ryzyko niskie).
Chociaż utrata dostępu do systemów administratora może być tylko tymczasowa i w początkowej fazie naruszenia nie wywołuje skutków dla praw i wolności osób fizycznych, ważne jest, aby administrator po przeprowadzeniu pełnej analizy ryzyka, rozważył wszystkie możliwe konsekwencje naruszenia, zarówno te które już zaistniały jak i te, które mogą zaistnieć w przyszłości.

Przykład: System informatyczny administratora został zainfekowany złośliwym oprogramowaniem. Po przeprowadzeniu wstępnej analizy administrator stwierdził, że nastąpiła tymczasowa utrata dostępu do danych jednak z uwagi na fakt, że administrator posiadał elektroniczny system zabezpieczeń chroniący przed wyciekiem danych, ryzyko naruszenia praw i wolności osób fizycznych było małe, a samo naruszenie nie wymagało zgłoszenia do Prezesa UODO. Po paru godzinach okazało się jednak, że w wyniku ww. włamania do systemu, haker po obejściu zabezpieczeń, uzyskał dostęp do danych osobowych, w związku z czym ryzyko naruszenia praw i wolności osób fizycznych stało się wysokie i wymagało zgłoszenia do organy nadzorczego.

Naruszenie danych może mieć miejsce również w następujących przypadkach:

- zmiana danych bez zgody osoby, której dane dotyczą;
- wysłanie danych do niewłaściwej osoby (np. poprzez niewłaściwie zaadresowanie poczty elektronicznej);
- utrata nośników danych (telefon, laptop, USB, teczki zawierające dane w wersji papierowej);
- nieuprawnione udostępnienie danych (np. elektronicznie – przekazywanie danych przez zdalny dostęp np. VPN, często przydzielane bezterminowo - ale też np. telefonicznie (rozmówca podaje się za pracownika policji czy urzędu, próbując wyciągnąć informacje);
- nieodpowiednie usuwanie danych (np. administrator postanawia pozbyć się starych komputerów. Przed sprzedażą usuwa jedynie pliki na pulpicie i opróżnia kosz ze starych plików. Nie usuwa jednak danych z dysku komputera).

Kiedy nie ma obowiązku zgłoszenia naruszenia Prezesowi UODO?

- Art. 33 ust. 1 RODO wskazuje, że w przypadku, gdy „jest mało prawdopodobne, by naruszenie to skutkowało naruszeniem praw lub wolności osób fizycznych", administrator nie ma obowiązku zawiadomienia organu nadzorczego o naruszeniu ochrony danych.
- W świetle art. 33 RODO, nie każde naruszenie ochrony danych osobowych wiąże się z naruszeniem bezpieczeństwa danych. Obowiązek zgłoszenia, o którym mowa w ww. artykule, dotyczy tylko tych naruszeń, które stanowią naruszenie bezpieczeństwa danych.
- *Przykład I: Pracownik kancelarii przez pomyłkę wynosi poza jej obszar teczkę z niezabezpieczonymi danymi osobowymi, wśród których znajdują się również szczególne kategorie danych osobowych. Po chwili orientuje się, że nastąpiła pomyłka i wraca do kancelarii zwracając teczkę. Działanie takie naruszyło zasady ochrony danych, ale nie wpłynęło na bezpieczeństwo danych, które nie zostały udostępnione.*
- *Przykład II: Administrator traci bezpiecznie zaszyfrowany pendrive. Klucz szyfrowania pozostaje w posiadaniu administratora i nie jest to jedyna kopia danych osobowych. W takiej sytuacji dane pozostają niedostępne dla złodzieja. Oznacza to małe prawdopodobieństwo, by naruszenie stanowiło zagrożenie dla praw lub wolności osób, których dane dotyczą.*
- Do każdej sytuacji należy jednak podchodzić z dużą rozwagą i ostrożnością. Zmiana choćby jednego z kluczowych elementów zdarzenia może bowiem doprowadzić do odmiennych wniosków, np. jeżeli w przypadku opisanym w przykładzie II po czasie okaże się, że naruszono bezpieczeństwo klucza lub, że oprogramowanie narażone jest na ataki, wówczas zmieni się ryzyko naruszenia praw i wolności osób, a w związku z tym może powstać obowiązek zgłoszenia naruszenia Prezesowi UODO. Podobna sytuacja może się zdarzyć, gdy w sytuacji zaistnienia naruszenia, administrator nie będzie dysponował kopią zapasową danych osobowych. W takim przypadku będziemy mieli do czynienia z naruszeniem dostępności, stanowiącym ryzyko dla praw i wolności osób fizycznych i w związku z tym, sytuacja ta będzie wymagała zgłoszenia naruszenia organowi nadzorczemu.

Sposoby informowania osób, których dane dotyczą o naruszeniu.

Forma, w jakiej podmioty danych powinny być zawiadomione o naruszeniu, nie została wprost wskazana w RODO. Ostateczny jej dobór będzie zależał od danych kontaktowych podmiotów danych, którymi dysponuje administrator. Mając na względzie znaczenie zawiadomienia, powinno być ono sporządzone w formie, która umożliwi podmiotowi danych na wielokrotne zapoznanie się z jego treścią. Bardzo ważne jest, aby zawiadomienie zostało dostarczone do adresata w możliwie

najkrótszym czasie. Wybierając mniej efektywny środek komunikacji, administrator może spowodować nieuzasadnioną zwłokę w przekazaniu informacji. W tym kontekście wadą przesyłki nadanej drogą tradycyjną jest czas niezbędny na jej doręczenie podmiotowi danych. Dla porównania zasadniczą zaletą elektronicznej formy komunikacji jest jej szybkość, co jest pożądane z uwagi na obowiązek powiadomienia podmiotu danych bez zbędnej zwłoki (art. 34 ust. 1 RODO). Forma ta umożliwia adresatowi wielokrotne zapoznanie się z komunikatem oraz jego wydruk w razie potrzeby. Co do zasady administrator bezpośrednio powiadamia osoby, których dane naruszono, chyba że wymagałoby to niewspółmiernie dużego wysiłku. W takim przypadku administrator wydaje publiczny komunikat lub stosuje podobny środek, aby w równie skuteczny sposób poinformować osoby, których dane dotyczą, (art. 34 ust. 3 lit. c RODO). Do powiadamiania osób, których dane naruszono, administrator powinien stosować komunikaty dedykowane, które nie powinny być przesyłane razem z innymi informacjami, na przykład newsletterem, czy standardową wiadomością. Pomoże to przekazać informacje o naruszeniu w jasny i przejrzysty sposób. Powiadomienia ograniczającego się do komunikatu prasowego, czy firmowego bloga nie uznaje się za skuteczne poinformowanie osoby fizycznej o naruszeniu.

Jak szybko należy zgłosić naruszenie Prezesowi UODO?

Zgodnie z art. 33 ust. 1 RODO, w przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości nie później niż w terminie 72 godzin po stwierdzeniu 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.

Jak wynika z ww. artykułu, zgłoszenie naruszenia powinno być przesłane do właściwego organu nadzorczego, bez zbędnej zwłoki. To czy zawiadomienia dokonano bez zbędnej zwłoki, należy ustalić z uwzględnieniem w szczególności charakteru i wagi naruszenia, jego konsekwencji oraz niekorzystnych skutków dla osoby, której dane dotyczą.

Ponadto administrator musi zgłosić naruszenie nie później niż w terminie 72 godzin po stwierdzeniu naruszenia. Według Grupy Roboczej Art. 29 administrator „stwierdza" naruszenie, kiedy ma on wystarczający stopień pewności co do tego, że miało miejsce zdarzenie zagrażające bezpieczeństwu, które doprowadziło do naruszenia ochrony danych.

Termin wskazany w art. 33 ust. 1 RODO nie powinien być przekraczany przez administratorów, jednakże RODO przewiduje pewne okoliczności, gdy zgłoszenie naruszenia organowi nadzorczemu może nastąpić po 72 godzinach od stwierdzeniu naruszenia. W takim przypadku, administrator jest zobligowany do podania przyczyn opóźnienia (więcej w pkt. „Czy dopuszczalne jest przekazywanie informacji o naruszeniu po upływie 72 godzin od stwierdzenia naruszenia?").

Jakie informacje należy przekazać osobom, których dane dotyczą w związku z naruszeniem?

Zgodnie z art. 34 ust. 2 RODO zawiadomienie skierowane do osób, których dane dotyczą powinno jasnym i prostym językiem opisywać charakter naruszenia ochrony danych osobowych oraz zawierać przynajmniej informacje i środki, o których mowa w art. 33 ust. 3 lit. b), c) i d). Zgodnie z tym przepisem, administrator powinien podać przynajmniej następujące informacje:

- imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub innego punktu kontaktowego, od którego można uzyskać więcej informacji;
- opis możliwych konsekwencji naruszenia ochrony danych osobowych;
- opis środków zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu - w tym w stosownych przypadkach - środków w celu zminimalizowania jego ewentualnych negatywnych skutków.

Zawiadomienie powinno być sformułowane jasnym i prostym językiem. Aby wymóg ten został spełniony, administrator powinien mieć na względzie grupę odbiorców, do której zawiadomienie będzie skierowane i dostosować do niej jego treść. Tytułem przykładu: jeżeli określony podmiot posiada klientów w zbliżonym wieku i poziomie wykształcenia, język komunikatu powinien uwzględniać te okoliczności. Jeżeli natomiast adresaci są zróżnicowani lub administrator nie posiada wystarczających danych dla dokładniejszego określenia grupy odbiorców zawiadomienia, to w takim przypadku punktem odniesienia powinien być przeciętny adresat takiej wiadomości. Celem jest

przekazanie odbiorcy komunikatu łatwego do zrozumienia. Ponadto komunikat nie powinien być nadmiernie rozbudowany, gdyż długa informacja z reguły utrudnia zrozumienie istoty przekazu.

Kiedy i w jakim celu trzeba zawiadomić o naruszeniu osoby, których dane dotyczą?
Zgodnie z art. 34 pkt. 1 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". Z powołanego przepisu wynika, że administrator będzie zobowiązany do zawiadomienia podmiotu danych wówczas, gdy spełnione zostaną łącznie dwie przesłanki. Po pierwsze, musi dojść do naruszenia ochrony danych osobowych. Po drugie, może ono powodować wysokie ryzyko naruszenia praw lub wolności osoby, której dane dotyczą. Do takich przypadków należą sytuacje, w których naruszenie prowadzi do dyskryminacji, kradzieży tożsamości, oszustwa, straty finansowej lub uszczerbku na reputacji. Jeżeli naruszenie dotyczy danych wrażliwych, można założyć, że jest prawdopodobne, iż takie naruszenie może prowadzić do wskazanych wyżej szkód. Nie jest konieczne, aby wysokie ryzyko zmaterializowało się i by faktycznie doszło do naruszenia praw lub wolności. Dlatego nie ma znaczenia, czy ostatecznie ich naruszenie nastąpi. Wystarczający jest fakt samego pojawienia się wysokiego ryzyka naruszenia praw lub wolności.
RODO wymaga, aby osoby fizyczne zostały zawiadomione o naruszeniu ich danych „bez zbędnej zwłoki". Oznacza to, że administrator powinien zrealizować przedmiotowy obowiązek tak szybko, jak pozwalają na to okoliczności danej sprawy. Należy przyjąć, że im poważniejsze jest ryzyko naruszenia praw lub wolności podmiotu danych, tym szybciej powinno nastąpić zawiadomienie, jak wskazuje motyw 86 RODO. Poinformowanie na czas osób fizycznych o zaistniałym naruszeniu ma na celu umożliwienie podmiotom danych podjęcie niezbędnych działań zapobiegawczych dla ochrony przed negatywnymi skutkami naruszenia. Jako przykład można wskazać wyciek haseł bankowych, w przypadku którego reakcja banku powinna być natychmiastowa.

Czy RODO wymaga podjęcia innych kroków w związku z naruszeniem?
Podobnie jak w przypadku każdego incydentu związanego z bezpieczeństwem, administrator powinien ustalić, czy naruszenie było wynikiem błędu ludzkiego lub problemu systemowego i zobaczyć w jaki sposób można zapobiec powtórce incydentu - czy to poprzez lepsze procesy, dalsze szkolenia lub inne kroki naprawcze. W celu sprawnej realizacji przez administratorów i podmioty przetwarzające obowiązków w zakresie naruszeń ochrony danych zalecane jest wdrożenie procedur. Ponadto procedura zgłaszania organowi nadzorczemu naruszeń ochrony danych osobowych oraz zawiadamiania o naruszeniach podmiotów danych, powinna być elementem kodeksu postępowania, zgodnie z art. 40 ust. 2 lit. i RODO.

Jakie naruszenia należy wpisywać do wewnętrznej ewidencji?
Art. 33 ust. 5 RODO nakłada na administratorów obowiązek dokumentowania wszelkich naruszeń ochrony danych osobowych, czyli prowadzenia wewnętrznej ewidencji naruszeń. Użyte w ww. artykule sformułowanie „wszelkich naruszeń" oznacza, że ewidencja powinna obejmować wszystkie naruszenia spełniające kryteria określone w definicji zawartej w art. art. 4 pkt 12 RODO. W ewidencji powinny zatem się znaleźć zarówno naruszenia ochrony danych osobowych podlegające obowiązkowi notyfikacyjnemu Prezesowi UODO, jak i te, które nie podlegają zgłoszeniu organowi nadzorczemu ze względu na okoliczność, że jest mało prawdopodobne, że skutkowałyby one ryzykiem naruszenia praw lub wolności osób fizycznych.
Zgodnie z wymaganiami art. 33 ust. 5 RODO administrator musi rejestrować informacje o naruszeniu obejmujące okoliczności naruszenia ochrony danych osobowych, przebieg i naruszone dane osobowe. Ewidencja powinna obejmować ponadto skutki i konsekwencje naruszenia oraz działania naprawcze podjęte przez administratora.
Prowadzenie ewidencji łączy się z zasadą rozliczalności przewidzianą w art. 5 ust. 2 RODO oraz obowiązkami administratora wynikającymi z art. 24 RODO. Jak wskazuje art. 33 ust. 5 (zdanie 2) RODO organ nadzorczy może zażądać dostępu do dokumentacji (ewidencji) naruszeń i dokumentacja ta powinna pozwolić organowi na weryfikowanie przestrzegania RODO w zakresie tych obowiązków.
Grupa Robocza Art. 29 podkreśla również, że w przypadku podjęcia decyzji o niezgłoszeniu naruszenia, wskazane jest udokumentowanie takiego faktu w ewidencji wraz z podaniem przyczyny,

dla której administrator uznaje ryzyko naruszenia praw i wolności osób fizycznych za mało prawdopodobne.
Jeżeli chodzi o sposób prowadzenia ewidencji, Grupa Robocza Art. 29 podkreśla, że administrator może zdecydować o dokumentowaniu naruszeń w rejestrze czynności przetwarzania prowadzonym zgodnie z art. 30 RODO. Nie ma wymogu prowadzenia osobnego rejestru naruszeń, jeżeli informacje dotyczące naruszenia można łatwo zidentyfikować i przedłożyć na żądanie.
Brak udokumentowania naruszenia we właściwy sposób może prowadzić do wykonania przez organ nadzorczy uprawnień na mocy art. 58 RODO lub nałożenia administracyjnej kary pieniężnej zgodnie z art. 83 RODO.

O jakich naruszeniach trzeba powiadomić Prezesa UODO?
W przypadku wykrycia przez administratora naruszenia ochrony danych osobowych konieczne jest, aby w pierwszej kolejności dokonana została analiza pod kątem wystąpienia ryzyka naruszenia praw i wolności osób fizycznych. Jeżeli w wyniku przeprowadzonego badania okaże się, że nie ma prawdopodobieństwa wystąpienia ryzyka naruszenia praw i wolności osób fizycznych, administrator zwolniony jest z obowiązku powiadamiania organu nadzorczego o naruszeniu. Jednakże pamiętać trzeba, że organ nadzorczy będzie mógł zwrócić się do administratora o uzasadnienie decyzji o niezgłaszaniu naruszenia, w związku z tym, wnioski z przeprowadzonej analizy należy udokumentować w wewnętrznej ewidencji naruszeń.
Ryzyko naruszenia praw i wolności osób fizycznych jest obecne, kiedy naruszenie może skutkować fizyczną, materialną lub niematerialną szkodą dla osób fizycznych, których dane naruszono. Szkodami takimi są np. dyskryminacja, kradzież tożsamości lub oszustwo dotyczące tożsamości, nadużycia finansowe, straty finansowe, nieuprawnione cofnięcie pseudonimizacji, utrata poufności danych osobowych chronionych tajemnicą zawodową, naruszenie dobrego imienia lub inne znaczące skutki gospodarcze lub społeczne dla danej osoby fizycznej. Jeżeli naruszenie dotyczy danych osobowych ujawniających pochodzenie etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych lub danych genetycznych, dotyczących zdrowia lub życia seksualnego, należy uznać, że występuje duże prawdopodobieństwo takiej szkody.

Czy dopuszczalne jest przekazywanie informacji o naruszeniu po upływie 72 godzin od stwierdzenia naruszenia?
Administratorzy nie zawsze będą dysponować wszystkimi wymaganymi informacjami dotyczącymi naruszenia w ciągu 72 godzin od jego stwierdzenia. W związku z tym, zgodnie z art. 33 ust. 4 RODO, administrator może udzielać informacji sukcesywnie. W takim przypadku administrator powinien przekazać brakujące informacje, jak tylko wejdzie w ich posiadanie. Zawiadamianie „sukcesywne" jest dopuszczalne pod warunkiem, że administrator poda organowi nadzorczemu przyczyny opóźnienia.