Siedem czynników ryzyka, które należy uwzględnić po naruszeniu ochrony danych osobowych

Posted on 2025-10-30

Podejście oparte na ryzyku to fundament prawa ochrony danych osobowych. To właśnie od ryzyka dla praw lub wolności osób fizycznych zależy zakres obowiązków spoczywających na administratorach i podmiotach przetwarzających. Poniżej wyjaśniamy, jak prawidłowo ocenić ryzyko w przypadku naruszenia ochrony danych osobowych i dlaczego jest to kluczowe dla zapewnienia zgodności z RODO.

Dlaczego należy oceniać ryzyko

Przetwarzanie danych osobowych wiąże się z ryzykiem naruszenia praw lub wolności osób fizycznych. Oznacza to możliwość wystąpienia rozmaitych szkód majątkowych i niemajątkowych, a w niektórych przypadkach nawet zagrożenia dla bezpieczeństwa osobistego lub zdrowia. Administratorzy i podmioty przetwarzające muszą więc podejmować działania, aby skutecznie zapobiegać ewentualnym negatywnym konsekwencjom dla osób,

których dane dotyczą. Stanowi to podstawę regulacji dotyczących ochrony danych osobowych.

Ryzyko dla osób fizycznych powinno być analizowane w różnych kontekstach:

ØZ jednej strony niezbędne są analizy systemowe, wykonywane zarówno na etapie projektowania operacji przetwarzania, jak i w ich trakcie. Pozwalają one realizować zasady ochrony danych osobowych oraz powstrzymywać naruszenia ich bezpieczeństwa. Stopień ryzyka związanego z przetwarzaniem decyduje także o konieczności przeprowadzenia oceny skutków dla ochrony danych (art. 35 ust. 1 RODO).

ØZ drugiej strony – w przypadku wystąpienia naruszenia ochrony danych osobowych – kluczowe stają się analizy incydentalne, skoncentrowane na okolicznościach konkretnego zdarzenia. Umożliwiają one identyfikację wynikających z niego zagrożeń oraz skuteczne im zaradzenie. Co równie istotne, pomagają prawidłowo określić obowiązki prawne administratora, takie jak konieczność zgłoszenia incydentu organowi nadzorczemu oraz zawiadomienia o nim osób, których dane dotyczą (art. 33 ust. 1 i art. 34 ust. 1 RODO).

Ryzyko a obowiązki prawne Zgodnie z art. 33 ust. 1 RODO administratorzy powinni zgłaszać naruszenia ochrony danych osobowych właściwym organom nadzorczym. Zgłoszenie nie jest jednak wymagane, jeżeli wystąpienie ryzyka jest mało prawdopodobne, czyli gdy brak jest realnych przesłanek, by mogło dojść do negatywnych konsekwencji dla osób fizycznych. W sytuacjach, w których naruszenie ochrony danych osobowych może powodować wysokie ryzyko, administratorzy zobowiązani są dodatkowo do zawiadomienia o zdarzeniu osób, których dane dotyczą, stosownie do art. 34 ust. 1 RODO

Obowiązek prawny	Próg ryzyka uruchamiający obowiązek	Próg ryzyka zwalniający z obowiązku

Zgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu (art. 33 ust. 1 RODO)	Naruszenie ochrony danych osobowych może wywołać ryzyko dla praw lub wolności osób fizycznych	Jest mało prawdopodobne, że naruszenie ochrony danych osobowych wywoła ryzyko dla praw lub wolności osób fizycznych
Zawiadomienie osób, których dane dotyczą, o naruszeniu ochrony danych osobowych (art. 34 ust. 1 RODO)	Naruszenie ochrony danych osobowych może wywołać wysokie ryzyko dla praw lub wolności osób fizycznych	Jest mało prawdopodobne, że naruszenie ochrony danych osobowych wywoła wysokie ryzyko dla praw lub wolności osób fizycznych

Ocena ryzyka związanego z naruszeniem ochrony danych osobowych służy nie tylko ustaleniu, czy w konkretnej sytuacji powstaje obowiązek jego zgłoszenia lub zawiadomienia o nim osób, których dane dotyczą. Jej celem jest również określenie zakresu i rodzaju środków zaradczych, jakie należy podjąć w reakcji na zdarzenie.

Jednocześnie należy pamiętać, że zgodnie z art. 33 ust. 5 RODO administratorzy powinni dokumentować wszelkie naruszenia ochrony danych osobowych. W tym przypadku obowiązek nie zależy od ryzyka i wynika z samego faktu wystąpienia takiego zdarzenia.
Jak oceniać ryzyko w przypadku naruszenia ochrony danych osobowych

Jak widać, przepisy RODO wymagają od administratorów kompleksowego rozumienia zagrożeń wynikających z naruszeń bezpieczeństwa danych. Ograniczenie się do przypisania zdarzeniu określonego poziomu ryzyka (np. wysokiego) może nie wystarczyć. Analiza ryzyka powinna uwzględniać rzeczywisty kontekst zdarzenia, jego przyczyny i możliwe skutki dla osób fizycznych.

Aby prawidłowo ocenić ryzyko związane z naruszeniem ochrony danych osobowych, warto wziąć pod uwagę siedem podstawowych czynników:

1.Rodzaj naruszenia ochrony danych osobowych

Wśród naruszeń ochrony danych osobowych można wyróżnić naruszenia poufności,

integralności i dostępności danych. Prawidłowe ustalenie rodzaju naruszenia ma kluczowe znaczenie przy ocenie związanego z nim ryzyka. Inne konsekwencje mogą bowiem wystąpić w przypadku nieuprawnionego ujawnienia danych, a inne – gdy doszło do ich utracenia, zniszczenia lub pomyłkowej modyfikacji.

Warto pamiętać, że niektóre incydenty mogą naruszać więcej niż jeden z tych atrybutów (np. w wyniku ataku ransomware). W takich sytuacjach katalog potencjalnych skutków dla osób fizycznych może być znacznie szerszy.

2.Charakter, wrażliwość i zakres danych osobowych

Wynik analizy ryzyka zależy także od charakteru, wrażliwości i zakresu danych osobowych, które zostały naruszone. Administrator powinien zidentyfikować kategorie tych danych i ocenić ich znaczenie w określonym kontekście. Przykładowo, dane wymienione w art. 9 ust. 1 i art. 10 RODO znajdują się pod szczególną ochroną prawną, ponieważ ich naruszenie może stanowić poważną ingerencję w prywatność osoby fizycznej. Należą do nich m.in. dane biometryczne, dane dotyczące zdrowia czy dane ujawniające poglądy polityczne. W wielu sytuacjach zazwyczaj można również przyjąć, że dane o charakterze powszechnym (np. informacje o preferencjach lub zainteresowaniach) będą mniej wrażliwe niż dane finansowe.

Należy jednak pamiętać, że wrażliwość danych zależy od kontekstu – informacje pozornie neutralne, takie jak imię i nazwisko czy adres zamieszkania, również mogą negatywnie wpłynąć na sytuację jednostki.

W przypadku naruszenia poufności warto też przeanalizować, jaki zestaw informacji stał się dostępny dla osób nieuprawnionych. Znaczenie mają przy tym nie tylko dane ujawnione bezpośrednio, lecz także te, które w wyniku incydentu można łatwo połączyć z konkretną osobą (np. loginy i hasła umożliwiające dostęp do innych systemów lub kont użytkowników).
3.Łatwość identyfikacji osób, których dane dotyczą

Niektóre dane osobowe, np. numer PESEL, mogą umożliwiać jednoznaczną identyfikację

osoby fizycznej. W innych przypadkach ustalenie tożsamości wymaga dodatkowych informacji, wysiłku lub zastosowania specjalistycznych narzędzi technicznych. Łatwość identyfikacji osób, których dane dotyczą, ma istotne znaczenie przy ocenie ryzyka związanego z naruszeniem ochrony danych osobowych. Im trudniej przypisać określone informacje do konkretnej osoby, tym mniejsze ryzyko naruszenia jej praw lub wolności. Skuteczna pseudonimizacja, anonimizacja lub szyfrowanie danych może znacząco ograniczyć ryzyko negatywnych skutków incydentu.

4.Dotkliwość konsekwencji dla osób, których dane dotyczą

Ocena ryzyka związanego z naruszeniem ochrony danych osobowych powinna obejmować także wagę możliwych konsekwencji zdarzenia dla osób, których dane dotyczą. Należy rozważyć, jak poważne mogą być potencjalne szkody – zarówno materialne, mające wymiar ekonomiczny, jak i niematerialne, o charakterze osobistym lub społecznym. Do pierwszej grupy można zaliczyć np. kradzież tożsamości skutkującą wykorzystaniem danych do zawarcia niechcianych umów. Wśród szkód niematerialnych znajdują się m.in. poczucie wstydu czy dyskryminacja. Część skutków może mieć charakter złożony – np. utrata reputacji (szkoda niematerialna) może prowadzić do utraty dochodów (szkoda materialna).

Przy ocenie dotkliwości warto także uwzględnić czas trwania i nieodwracalność skutków. Im dłużej dane pozostają poza kontrolą administratora i im trudniej ograniczyć ich dalsze wykorzystanie, tym wyższa jest dotkliwość incydentu. Krótkotrwała utrata dostępu do usługi dla kilku użytkowników może mieć ograniczone konsekwencje, natomiast ujawnienie danych genetycznych lub biometrycznych w internecie może prowadzić do długotrwałych szkód, których nie da się w pełni naprawić.

5.Cechy szczególne osoby, której dane dotyczą

Przy ocenie ryzyka warto uwzględnić również cechy i sytuację osób, których dane zostały naruszone. Dotkliwość skutków incydentu zależy nie tylko od kategorii danych osobowych,

lecz także od indywidualnej podatności konkretnej osoby na ich wykorzystanie. Wyższe ryzyko może występować w przypadku osób małoletnich, osób starszych, pacjentów, osób z niepełnosprawnościami lub takich, które pozostają w zależności służbowej, ekonomicznej lub prawnej. Naruszenie danych tych osób może prowadzić do poważniejszych konsekwencji, ponieważ dysponują one mniejszymi możliwościami ochrony swoich praw lub ograniczenia skutków zdarzenia. Znaczenie mają też czynniki społeczne – np. gdy incydent dotyczy osób należących do mniejszości lub uczestniczących w działaniach związków zawodowych czy organizacji społecznych
W takich przypadkach nawet ujawnienie pozornie nieszkodliwych informacji może skutkować naruszeniem prywatności, stygmatyzacją lub narażeniem na presję ze strony innych podmiotów.

6.Cechy szczególne administratora

Ryzyko związane z naruszeniem ochrony danych osobowych zależy też od specyfiki administratora. Znaczenie mają m.in. zakres i skala przetwarzania, a także rodzaj działalności – inne konsekwencje może mieć incydent w placówce medycznej, a inne w niewielkiej organizacji społecznej.

Warto również uwzględnić pozycję zaufania społecznego lub szczególną odpowiedzialność administratora – np. w przypadku instytucji publicznych czy podmiotów przetwarzających dane osób w trudnej sytuacji życiowej. W takich przypadkach oczekiwania wobec standardów ochrony danych są wyższe, a konsekwencje incydentów – bardziej dotkliwe.

7.Liczba osób, których dane dotyczą

Przy ocenie ryzyka należy też uwzględnić skalę zdarzenia, rozumianą jako liczbę osób, których dane zostały nim objęte. Nawet jeśli skutki dla pojedynczej osoby wydają się ograniczone, wysoka liczba poszkodowanych może znacząco zwiększyć ogólny poziom ryzyka i wymagać podjęcia bardziej zaawansowanych działań zaradczych.

Warto jednak pamiętać, że liczba osób dotkniętych naruszeniem ochrony danych osobowych wpływa przede wszystkim na prawdopodobieństwo wystąpienia negatywnych konsekwencji, lecz nie zawsze na ich wagę. Poważne lub nieodwracalne skutki mogą bowiem wystąpić także w przypadku incydentu dotyczącego jednej osoby – zwłaszcza gdy naruszone dane mają charakter szczególnie wrażliwy.

Skuteczna rozliczalność

Zasada rozliczalności wymaga od administratora nie tylko przestrzegania przepisów RODO, ale także możliwości wykazania zgodności z prawem. Rzetelna analiza ryzyka po wystąpieniu naruszenia ochrony danych osobowych – oparta na uwzględnieniu przedstawionych powyżej czynników – pozwala administratorowi w sposób przejrzysty uzasadnić zarówno podjęcie, jak i zaniechanie określonych działań.

Dokumentowanie oceny ryzyka na podstawie obiektywnych kryteriów ma kluczowe znaczenie nie tylko dla bezpieczeństwa osób, których dane dotyczą, lecz i dla samego administratora. Właściwie udokumentowana analiza ryzyka to nie tylko obowiązek, ale również dowód dojrzałości organizacyjnej i świadomego podejścia do ochrony danych osobowych.