Warszawa, 11.01.2023 r.

## Naruszenie ochrony danych – czym jest i jak sobie z nim poradzić?

Naruszenia ochrony danych osobowych to temat budzący niepokój wśród administratorów danych, inspektorów ochrony danych czy pracowników organizacji. Jak sobie z nimi poradzić, jakie kroki podjąć, czy formalności związane z naruszeniami są skomplikowane? Na te pytania odpowiem krótko w poniższym artykule.
Zgodnie z RODO „naruszenie ochrony danych osobowych" oznacza 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.
W sposób bardziej przystępny można powiedzieć, że z naruszeniem ochrony danych osobowych mamy do czynienia, kiedy spełnione są trzy przesłanki:

- 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.

Zgodnie z Wytycznymi Grupy Roboczej Art. 29 możemy wymienić trzy typy naruszeń ochrony danych osobowych:

1. naruszenie poufności - polega na ujawnieniu danych osobowych nieuprawnionej osobie, np. przypadkowe wysłanie danych osobowych klienta do niewłaściwego działu firmy lub osoby postronnej.
2. naruszenie dostępności - polega na czasowej bądź trwałej utracie lub zniszczeniu danych osobowych, np. zgubienie lub kradzież nośnika zawierającego bazy danych klientów administratora przy braku kopii zapasowej,
3. naruszenie integralności - polega na zmianie treści danych osobowych w sposób nieautoryzowany, np. pracownik dla żartu zmienia nazwiska klientów poprzez dopisanie litery „a" na końcu każdego z nich.

## Jakie obowiązki w związku z naruszeniami ochrony danych ciążą na administratorze?

Administrator w celu realizacji przepisów RODO powinien:

- wprowadzić procedury umożliwiające stwierdzanie i ocenę naruszeń pod kątem wystąpienia ryzyka naruszenia praw i wolności osób fizycznych;
- prowadzić wewnętrzną ewidencji naruszeń;
- zgłaszać naruszeń organowi nadzorczemu;
- powiadamiać osoby, których dane dotyczą, o naruszeniu;
- podejmować działania mające na celu przeciwdziałanie skutkom naruszenia i zapobieganie im w przyszłości.

## Mamy naruszenie… Co zrobić?

Przeanalizować i ocenić. Pierwszym krokiem, gdy wystąpi podejrzenie naruszenia ochrony danych osobowych, jest dokonanie analizy i oceny - należy ustalić okoliczności incydentu, przyczyny jego wystąpienia, zbadać, na czym polegało naruszenie i jaka jest jego skala, ocenić ryzyka naruszenia praw i wolności osób, których dane są przetwarzane.

Gdy po przeanalizowaniu stanu faktycznego i zebraniu dowodów okaże się, że: naruszenie dotyczy danych osobowych; skutkiem naruszenia może być zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych oraz naruszenie jest skutkiem złamania zasad bezpieczeństwa danych, to należy przejść do etapu zgłaszania naruszenia.

## Jak zgłosić naruszenie?

Po stwierdzeniu naruszenia należy zająć się formalnościami i w pierwszej kolejności zgłosić naruszenie do organu nadzorczego. W Polsce organem właściwym do zgłaszania naruszeń ochrony danych osobowych jest Prezes Urzędu Ochrony Danych Osobowych (Prezes UODO).
Zgłoszenia można dokonać za pomocą formularza dostępnego na stronie uodo.gov.pl na 4 sposoby:

1. Elektronicznie poprzez wypełnienie dedykowanego formularza dostępnego bezpośrednio na platformie biznes.gov.pl,
2. Elektronicznie poprzez wysłanie wypełnionego formularza na elektroniczną skrzynkę podawczą ePUAP: UODO/SkrytkaESP,
3. Elektronicznie poprzez wysłanie wypełnionego formularza za pomocą pisma ogólnego dostępnego na platformie biznes.gov.pl,
4. Tradycyjną pocztą, wysyłając wypełniony formularz na adres Urzędu.

W przypadku wystąpienia transgranicznego naruszenia ochrony danych administrator musi przeprowadzić analizę, czy wiodącym organem nadzorczym w odniesieniu do tej konkretnej czynności przetwarzania, która została objęta naruszeniem, jest Prezes UODO, czy też może inny organ nadzorczy.

## Jakich innych formalności należy dopełnić?

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".
Materializacją wyżej określonych przesłanek jest naruszenie, które może doprowadzić do: dyskryminacji, kradzieży tożsamości, oszustwa, straty finansowej, uszczerbku na reputacji albo naruszenie, które dotyczy danych szczególnych kategorii i można założyć, że jest prawdopodobne, iż takie naruszenie może prowadzić do wskazanych wyżej szkód.
Więcej informacji nt. poprawnego powiadamiania osób o naruszeniu: W jaki sposób prawidłowo zawiadomić o naruszeniu podmiot danych? - iSecure

## Kto powinien dokonać zgłoszenia?

Każdy administrator, który stwierdzi, że doszło do incydentu naruszającego bezpieczeństwo danych i powodującego ryzyko naruszenia praw i wolności podmiotów danych, musi dokonać zgłoszenia do Prezesa UODO. Przed przystąpieniem do uzupełniania zgłoszenia, o którym mowa powyżej, powinien sprawdzić, czy dane będące przedmiotem naruszenia należą do niego, czy może zostały mu tylko powierzone do przetwarzania, ponieważ wyłącznie administratorzy mają obowiązek notyfikacji naruszeń Prezesowi UODO. Na podmiotach przetwarzających ciąży jedynie obowiązek zawiadomienia o zdarzeniu właściwego administratora.

## Ile mam czasu na zgłoszenie naruszenia?

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.
Istotne jest zwrócenie uwagi na to, czym jest „stwierdzenia naruszenia", które nie musi być jednoznaczne z momentem wystąpienia 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, a więc po przeprowadzeniu procesu oceny zdarzenia.

## Ewidencja naruszeń

Art. 33 ust. 5 RODO nakłada na administratorów jeszcze jeden obowiązek - prowadzenia wewnętrznej ewidencji wszelkich naruszeń. Co kryje się pod pojęciem „wszelkich naruszeń"? Sformułowanie to oznacza, że ewidencja powinna zawierać wszystkie naruszenia spełniające kryteria określone w definicji zawartej w art. 4 pkt 12 RODO - zatem znaleźć się w niej powinny naruszenia ochrony danych osobowych podlegające obowiązkowi notyfikacyjnemu Prezesowi UODO, jak i te, które nie podlegają zgłoszeniu organowi nadzorczemu ze względu na to, że mało prawdopodobne jest, by skutkowały one ryzykiem naruszenia praw lub wolności osób fizycznych.
Prowadzenie ewidencji naruszeń jest praktycznym sposobem realizacji zasady rozliczalności przewidzianej w art. 5 ust. 2 RODO a 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.
Aby spełnić wymagania wynikające z przepisów, ewidencja naruszeń powinna zawierać informacje o naruszeniu obejmujące: okoliczności naruszenia, przebieg i naruszone dane osobowe, skutki i konsekwencje naruszenia, opis działań naprawczych podjętych przez administratora, a 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.

## Jak uniknąć naruszeń?

Przez pierwszy rok stosowania RODO administratorzy zgłosili dokładnie 4539 naruszeń ochrony danych osobowych. W kolejnych latach liczba ta stale się zwiększała, a w ostatnim rocznym sprawozdaniu opublikowanym przez UODO wynosiła już 12946. Tendencja wzrostowa w liczbie zgłaszanych naruszeń może świadczyć o coraz większej świadomości administratorów w tym zakresie oraz sugerować, że w wielu organizacjach wdrożone zostały procedury dot. reagowania na naruszenia. Co jednak zrobić, aby w 2023 nie być uczestnikiem tej kilkunastotysięcznej liczby?
Każdy administrator powinien wprowadzić procedury ograniczające możliwość wystąpienia naruszeń (np. procedura odbioru uprawnień po zakończeniu pracy), przeprowadzać szkolenia, uczulić pracowników na kwestie związane z ochroną danych osobowych, tak by świadomie mogli oni identyfikować potencjalne zagrożenia oraz unikać naruszeń ochrony danych osobowych. Niezbędne są oczywiście również adekwatne środki techniczne i organizacyjne stosowane w celu minimalizacji ryzyka, jednak z naszego doświadczenia

wynika, że najczęściej słabym ogniwem w systemie ochrony danych osobowych jest człowiek.

**Nina Zacharska** - specjalista ds. ochrony danych osobowych w iSecure Sp. z o.o.