

Nie każde naruszenie ochrony danych wymaga zgłoszenia do Prezesa UODO

Datum 5.10.2026
Subjekt Urząd Ochrony Danych Osobowych
Autor Karol Witowski
Region Poland
Kategorie State institutions, Law, Accounting and consulting services, Security

W związku z najnowszymi naruszeniami ochrony danych dotyczącymi tysięcy podmiotów Prezes Urzędu Ochrony Danych Osobowych przypomina, że zgodnie z art. 33 ust. 1 RODO, w przypadku naruszenia ochrony danych osobowych administrator bez zbędnej zwłoki zgłasza je organowi nadzorczemu, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

W związku z ostatnimi incydentami polegającymi w szczególności na nieuprawnionym dostępie do baz kontrahentów oraz systemów fakturowych, Prezes UODO wskazuje na konieczność każdorazowego przeprowadzania przez administratora rzetelnej oceny ryzyka, której wynik decyduje o obowiązku zgłoszenia naruszenia.

Kiedy zgłoszenie może nie być wymagane

Z sytuacją, w której jest mało prawdopodobne, by naruszenie skutkowało ryzykiem naruszenia praw lub wolności, mamy do czynienia zazwyczaj w przypadku ujawnienia informacji o osobach prowadzących działalność gospodarczą, jeśli obejmują one **dane powszechnie dostępne w jawnym rejestrze (CEIDG)** – takie jak imię i nazwisko, nazwa firmy, NIP czy oficjalny adres działalności. Utrata poufności takich danych co do zasady nie daje osobom nieuprawnionym nowych możliwości działania na szkodę osoby, której dane dotyczą.

Kiedy zgłoszenie jest wymagane

Obowiązek notyfikacji do organu nadzorczego (Prezesa UODO) powstaje wtedy, gdy naruszenie może powodować ryzyko naruszenia praw lub wolności osób fizycznych. Dotyczy to w szczególności sytuacji, gdy wraz z danymi powszechnie dostępnymi publicznie **ujawniono również inne informacje**, które mogą umożliwić/ pozwolić na dokonanie oszustwa, kradzieży tożsamości, profilowanie lub wykorzystanie danych w działaniach socjotechnicznych.

Ryzyko takie zapewne wystąpi m.in. w przypadku ujawnienia:

- **numeru PESEL** (ryzyko kradzieży tożsamości, wyłudzeń lub zaciągania zobowiązań finansowych na dane osoby),
- **szczegółów zakupów lub usług wskazujących na stan zdrowia albo inne dane szczególnych kategorii** (ryzyko naruszenia prywatności, dyskryminacji lub nieuprawnionego profilowania),
- **informacji finansowych** (ryzyko oszustw finansowych oraz przygotowywania fałszywych faktur

lub płatności),

Jeżeli analiza wykaże **wysokie ryzyko** naruszenia praw lub wolności osób fizycznych, administrator powinien również zawiadomić osoby, których dane dotyczą, zgodnie z art. 34 RODO.

Należy pamiętać

Nawet jeśli administrator uzna, że dane naruszenie nie wymaga zgłoszenia Prezesowi UODO, nie zwalnia go to z obowiązku:

- przeprowadzenia i udokumentowania oceny ryzyka,
- wskazania w wewnętrznym rejestrze naruszeń przesłanek uzasadniających brak zgłoszenia.

RODO wymaga bowiem dokumentowania wszystkich naruszeń ochrony danych osobowych, niezależnie od tego, czy zostały zgłoszone organowi nadzorczemu.

<https://uodo.gov.pl/pl/138/4596>