Jak postępować z naruszeniami ochrony danych osobowych? – podsumowanie EROD

Posted on 2025-05-30

W marcu tego roku Europejska Rada Ochrony Danych (EROD) opublikowała podsumowanie dotychczasowych wytycznych dotyczących naruszeń ochrony danych osobowych. Dokument stanowi kompleksowy przewodnik po najważniejszych zagadnieniach.

Naruszenia ochrony danych osobowych i ich konsekwencje

Zgodnie z RODO, naruszeniem ochrony danych osobowych jest naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do przetwarzanych danych osobowych[1]. Takie zdarzenie może skutkować poważnymi

konsekwencjami, takimi jak:

- • utrata kontroli nad danymi osobowymi,
- • ograniczenie praw,
- • dyskryminacja,
- • kradzież lub sfałszowanie tożsamości,
- • straty finansowe,
- • nieuprawnione odwrócenie pseudonimizacji (czyli ponowne ustalenie tożsamości osoby na podstawie danych, które wcześniej zostały w ten sposób zabezpieczone),
- • naruszenie dobrego imienia,
- • naruszenie poufności danych osobowych chronionych tajemnicą zawodową.

Rodzaje naruszeń ochrony danych osobowych

EROD wyróżnia trzy podstawowe rodzaje naruszeń ochrony danych osobowych:

- • naruszenia poufności – przypadkowe lub bezprawne ujawnienie lub dostęp do danych osobowych;
- • naruszenia integralności – przypadkowa lub bezprawna modyfikacja danych osobowych;
- • naruszenia dostępności – przypadkowe lub bezprawne utracenie lub zniszczenie danych osobowych[2].

Lepiej zapobiegać, niż leczyć

Zarządzanie bezpieczeństwem przetwarzania zaczyna się od wdrożenia odpowiednich środków technicznych i organizacyjnych. EROD podkreśla, że nawet mimo stosowania zabezpieczeń, w organizacjach nadal może dochodzić do naruszeń ochrony danych

osobowych. Ryzyko ich występowania można jednak znacznie ograniczyć, stosując skuteczne działania zapobiegawcze, np.:

- • regularne szkolenia personelu z zakresu ochrony danych osobowych,
- • korzystanie z aktualnego oprogramowania antywirusowego,
- • wdrażanie polityk kontroli dostępu i regularny przegląd przyznawanych dostępów,
- • stosowanie uwierzytelniania wieloskładnikowego przy dostępie do wrażliwych[3] danych,
- • szyfrowanie dysków,
- • regularne tworzenie i testowanie kopii zapasowych,
- • automatyczne blokowanie komputerów przy braku aktywności.

Jak reagować na naruszenia ochrony danych osobowych?

Wykrywanie

W przypadku naruszenia ochrony danych osobowych kluczowa jest szybka i skuteczna reakcja. EROD wskazuje, że organizacje powinny dysponować wewnętrznymi mechanizmami wykrywania i reagowania na incydenty, w tym ich właściwej oceny w świetle obowiązków wynikających z RODO. Ważne jest również prawidłowe uregulowanie współpracy z podmiotami przetwarzającymi[4].

Dokumentowanie

EROD zaznacza, że każde „stwierdzone” naruszenie ochrony danych osobowych powinno zostać udokumentowane w wewnętrznym rejestrze[5] .

Zgłaszanie organowi nadzorczemu

Jeżeli naruszenie ochrony danych osobowych prawdopodobnie wiąże się z ryzykiem dla praw lub wolności osób fizycznych, administrator powinien zgłosić je organowi nadzorczemu w ciągu 72 godzin od jego „stwierdzenia”. Zgłoszenie powinno zawierać:

- • opis charakteru naruszenia ochrony danych osobowych,
- • imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie 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 ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków[6].

Jeżeli zgłoszenie następuje po upływie 72 godzin, konieczne jest wyjaśnienie przyczyn opóźnienia.

Zawiadamianie osób, których dane dotyczą

Osoby, których dane dotyczą, muszą zostać zawiadomione o naruszeniu ochrony danych osobowych, jeśli prawdopodobnie wiąże się ono z wysokim ryzykiem dla ich praw lub wolności. Zawiadomienie powinno nastąpić jak najszybciej i zostać dokonane przez bezpieczne kanały komunikacji.

Przykłady EROD

Dokument przedstawia przykładowe scenariusze naruszeń ochrony danych osobowych, a także działań, jakie należy podjąć w ich następstwie. EROD podkreśla jednak, że są to przykłady uproszczone, zachęcając do zapoznania się z pełną wersją wytycznych przed podjęciem decyzji w podobnej sytuacji.

Przykład 1

Kontekst i cele przetwarzania: Organizacja przechowuje zaszyfrowaną kopię archiwum danych osobowych na pendrive. Nośnik zostaje skradziony podczas włamania.

Jak reagować: Jeśli dane są zaszyfrowane nowoczesnym algorytmem, istnieją kopie zapasowe, a klucz deszyfrujący nie został skompromitowany, zgłoszenie naruszenia ochrony danych osobowych może nie być wymagane. Jeżeli jednak w przyszłości okaże się, że klucz został skompromitowany, zgłoszenie stanie się konieczne. W każdym przypadku naruszenie

należy udokumentować.

Przykład 2

Kontekst i cele przetwarzania: Agent ubezpieczeniowy otrzymuje plik Excel, w którym przez błąd konfiguracyjny może zobaczyć dane około dwudziestu osób spoza swojej grupy klientów. Agent, objęty tajemnicą zawodową, jest jedynym odbiorcą wiadomości. Zgodnie z umową, niezwłocznie informuje administratora, który koryguje błąd, przesyła poprawną wersję pliku i prosi o usunięcie pierwotnej wiadomości oraz pisemne potwierdzenie usunięcia, co zostaje wykonane.

Jak reagować: Naruszenie ochrony danych osobowych dotyczy wyłącznie poufności, obejmuje ograniczoną liczbę osób i nie obejmuje danych wrażliwych. Dzięki odpowiedniej reakcji zdarzenie prawdopodobnie nie spowoduje ryzyka dla praw lub wolności osób fizycznych. Zgłoszenie do organu nadzorczego i zawiadomienie osób, których dane dotyczą, nie jest wymagane, ale incydent musi zostać udokumentowany.

Przykład 3

Kontekst i cele przetwarzania: System informatyczny szpitala zostaje zaatakowany przez ransomware, który szyfruje dużą część danych. Zewnętrzna firma specjalizująca się w cyberbezpieczeństwie monitoruje sieć i analizuje logi. Dochodzenie potwierdza brak wycieku danych.

Jak reagować: Pomimo istnienia kopii zapasowych, naruszenie ochrony danych osobowych powoduje znaczące zakłócenia, w tym odwołanie lub opóźnienie zabiegów medycznych i obniżenie jakości usług. Wysokie ryzyko dla praw lub wolności osób fizycznych wymaga zgłoszenia do organu nadzorczego oraz zawiadomienia osób, których dane dotyczą.

Dokumentacja incydentu jest obowiązkowa.

Przykład 4

Kontekst i cele przetwarzania: Administrator świadczy usługę online, która staje się celem cyberataku. Dochodzi do wycieku danych osobowych użytkowników.

Jak reagować: Zgłoszenie do organu nadzorczego jest wymagane, jeżeli naruszenie ochrony danych osobowych prawdopodobnie wywoła ryzyko dla praw lub wolności osób fizycznych. Obowiązek zawiadomienia użytkowników zależy od kategorii danych i potencjalnej wagi skutków incydentu. Dokumentacja jest obowiązkowa.

Gdzie znaleźć więcej informacji?

Dokument w języku angielskim można pobrać ze strony internetowej EROD. Zachęcamy także do lektury poradnika Prezesa UODO dotyczącego naruszeń ochrony danych osobowych, dostępnego na stronie internetowej UODO.

Jak postępować z naruszeniami ochrony danych osobowych? – podsumowanie EROD

1. Więcej na temat definicji „naruszenia ochrony danych osobowych” w Biuletynie UODO nr 1/03/23, str. 27 ↩
2. Więcej na temat rodzajów naruszeń ochrony danych osobowych w Biuletynie UODO nr 3/05/23, str. 25. ↩
3. „Wrażliwość” to ogólna, opisowa cecha danych osobowych – może być stopniowalna i zależy od kontekstu. EROD posługuje się tym pojęciem (np. w obszarze analizy ryzyka) niezależnie od terminu „szczególnych kategorii danych”, odnoszącego się do konkretnego, zamkniętego katalogu określonego w art. 9 RODO. ↩
4. Więcej na temat roli podmiotu przetwarzającego w przypadku naruszenia ochrony danych osobowych
   w Biuletynie UODO nr 01/01/24, str. 19. ↩
5. Więcej na temat dokumentowania naruszeń ochrony danych osobowych w Biuletynie UODO nr 12_01/12_01/24_25, str. 27. ↩
6. Więcej na temat informacji, jakie należy zawrzeć w zgłoszeniu, w Biuletynie UODO nr 10/10/23, str. 18 ↩