



Czym jest naruszenie ochrony danych osobowych?

#RODOFAQ

Naruszenia ochrony danych osobowych, to temat, który spędza sen z powiek niejednemu administratorowi danych, procesorowi czy Inspektorowi ochrony danych. Wystąpienia naruszeń obawiają się również pracownicy mający węższy bądź szerszy dostęp do danych.

W tym miejscu odpowiemy sobie krótko na podstawowe pytanie w tym zakresie, czyli czym to naruszenie ochrony danych osobowych jest.

RODO definicja

Termin zdefiniowano w art. 4 ust. 12 Ogólnego rozporządzenia o ochronie danych:

„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

RODO praktyka

Formuła definicji wskazanej w RODO jest bardzo szeroka. Oczywiście gdzieś tutaj trzeba postawić zdroworozsądkową granicę. Jeżeli obejrzymy sobie raport z oprogramowania antywirusowego, to znajdziemy dziennie co najmniej kilkadziesiąt prób ataku na nasze zasoby IT (dot. komputerów, serwerów, stron internetowych).

Czy każde z tych zdarzeń z osobna powinniśmy potraktować jako naruszenia ochrony danych osobowych? Jeśli pójdziemy tą drogą, to nasza praca będzie sprowadzała się głównie do analizowania incydentów RODO.

Spójrzmy jeszcze raz na przytoczoną w poprzednim akapicie definicję. Jasno wskazuje nam ona, że abyśmy mogli mówić o naruszeniu ochrony danych osobowych **spełnione muszą zostać wszystkie z trzech opisanych warunków**, tj.:

- 1) naruszenie musi dotyczyć danych osobowych,
- 2) skutkiem naruszenia jest zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych,
- 3) naruszenie jest skutkiem złamania zasad bezpieczeństwa danych.





Nieudany atak hakerski nie będzie zatem naruszeniem ochrony danych osobowych – nie doszło do przełamania zabezpieczeń. Podobnie będzie z kradzieżą sformatowanego laptopa. Skradziony sprzęt nie zawierał bowiem żadnych danych osobowych.

Jeżeli jednak haker pokona nasze zabezpieczenia i uzyska nieuprawniony dostęp do danych osobowych, to wszczęta powinna zostać [procedura reagowania na incydenty RODO](#).



Postępowanie z naruszeniami ochrony danych osobowych – praktyczny pakiet procedur, szablonów i instrukcji

Przygotowaliśmy dla Ciebie kompleksowy pakiet wytycznych w zakresie zarządzania naruszeniami ochrony danych osobowych w organizacji.

Nasze dokumenty zostały opracowane w taki sposób, aby ich dostosowanie do działalności Twojej organizacji było jak najbardziej intuicyjne i proste.

[SPRAWDŹ](#)

Mamy naruszenie – co dalej?

Jeśli już stwierdzimy naruszenie ochrony danych osobowych, to konieczna będzie m.in. ocena ryzyka naruszenia praw i wolności osób, których danych to zdarzenie dotyczy. Jeśli ocenimy, że incydent skutkuje takim ryzykiem to o jego wystąpieniu musimy poinformować UODO. Jeśli ryzyko takie jest na poziomie wysokim, to dodatkowo powinniśmy poinformować o nim także te osoby.

Każdorazowe wszczęcie procedury reagowania na incydent, będzie wymagało od nas przeprowadzenia wielu różnych czynności.

Temu jak radzić sobie z naruszeniami RODO poświęciliśmy cały cykl artykułów na naszym blogu:

1. [Ups... mamy naruszenie ochrony danych osobowych,](#)
2. [Zgłoszenie naruszenia RODO do Urzędu Ochrony Danych Osobowych,](#)
3. [Zgłaszanie naruszenia ochrony danych osobowych osobom poszkodowanym.](#)

Autor artykułu:

Przemysław Zegarek, Prezes Zarządu Lex Artist sp. z o.o.

Źródła:



-
- [Rozporządzenie Parlamentu Europejskiego i Rady \(UE\) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE \(Ogólne rozporządzenie o ochronie danych\)](#)

