Kary organów nadzorczych w Unii Europejskiej

Kraj oraz organ nadzorczy
Szwecja
Data Protection Authority of Sweden

Data wydania decyzji
28 sierpnia 2023 r.

Podmiot kontrolowany
Trygg-Hansa

Wysokość kary
3 000 000 EUR

FORSAFE
BEZPIECZEŃSTWO PONAD WSZYSTKO

Rodzaj naruszenia

Art. 5 (1) f), art. 32 (1) RODO.
Nieprzestrzeganie ogólnych zasad przetwarzania danych.

Przedmiot decyzji

Źródło postępowania:

W grudniu 2020 r. szwedzki organ nadzorczy otrzymał informację, że Moderna Försäkringar (obecnie Trygg-Hansa) umożliwiła nieautoryzowany dostęp do danych osobowych swoich klientów.

Opis wydarzeń:

1. Szwedzki organ nadzorczy zdecydował o dokonaniu czynności kontrolnych w Trygg-Hansa celem rozpatrzenia przedmiotowej sprawy oraz poprosił o złożenie dodatkowych wyjaśnień.

2. W trakcie czynności kontrolnych szwedzki organ nadzorczy ustalił, iż:

a) Trygg-Hansa jest podmiotem świadczącym usługi ubezpieczeniowe, który udostępnił nowemu klientowi poprzez wiadomość unikalny adres internetowy prowadzący do strony z wyceną ubezpieczenia,

b) powyższa osoba odkryła, że zmiana liczby w adresie URL powoduje przekierowanie do dokumentów innego klienta,

c) w wyniku zaistniałej sytuacji osoby nieuprawnione mogły mieć dostęp do informacji o około 650 000 klientów,

d) naruszenie trwało od października 2018 r. do lutego 2021 r.,

e) naruszenie obejmowało następujące dane osobowe – imię i nazwisko, dane kontaktowe (adres e-mail, numer telefonu), informacja o stanie zdrowia, numer ubezpieczenia społecznego, informacje finansowe, informacje dotyczące własności, numer ubezpieczenia, numer szkody i informacja o szkodzie,

f) naruszenie mogło również obejmować informacje o naruszeniach prawa oraz informacje o przynależności do związku zawodowego.

3. Szwedzki organ nadzorczy uznał, że Trygg-Hansa nie wdrożył adekwatnych środków technicznych co skutkowało nałożeniem na niego kary administracyjnej.

Przyczyna naruszenia:

Trygg-Hansaudostępnił swoim klientom stronę zawierającą lukę w zabezpieczeniu skutkującą dostępem osób nieuprawnionych do danych osobowych innych osób**.**

Decyzja:

Kara pieniężna w wysokości 3 000 000 EUR.

Źródło:

https://www.imy.se/contentassets/c3ee6b30e5084c598ff5545cd4912055/beslut-efter-tillsyn-enligt-dataskyddsforordningen---trygg-hansa-forsakring-filial.pdf

Kompas FORSAFE

JAK UNIKAĆ TAKICH NARUSZEŃ?

1. Dokonując wyboru odpowiednich środków technicznych i organizacyjnych pamiętaj, że jest to proces dwuetapowy. W pierwszej kolejności ważne jest, aby określić poziom ryzyka, jaki wiąże się z przetwarzaniem danych osobowych. Dopiero po wykonaniu tej czynności możemy ustalić, jakie środki techniczne i organizacyjne będą odpowiednie, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku.

2. Dokonuj regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania danych osobowych w systemach teleinformatycznych.

3. Jeśli udostępniasz swoim klientom usługę poprzez stronę internetową pamiętaj, aby:

a) zadbać o prawidłową konfigurację serwera oraz usług wystawianych do Internetu,

b) stosować funkcje filtrujące zapytania do bazy danych oraz walidację i kodowanie adresu URL,

c) stosować szyfrowanie adresu URL,

d) stosować odpowiednie i kontrolowane uprawnienia dostępu do katalogów oraz plików na serwerze.

Materiał edukacyjny przygotowany przez FORSAFE

Opracowanie merytoryczne
Katarzyna Kawczyńska