Kary Prezesa Urzędu Ochrony Danych Osobowych

Data wydania decyzji **20 grudnia 2023 r.**

Podmiot kontrolowany **Minister Zdrowia**

Wysokość kary **100 000 PLN**

FORSAFE
BEZPIECZEŃSTWO PONAD WSZYSTKO

Rodzaj naruszenia

Art. 25 (1), Art. 32 (1), (2), Art. 34 (2) RODO.
Niewystarczające środki techniczne i organizacyjne zapewniające bezpieczeństwo informacji.

Przedmiot decyzji

Źródło postępowania:

W sierpniu 2023 r. do Prezesa Urzędu Ochrony Danych Osobowych (UODO) wpłynęło zgłoszenie naruszenia ochrony danych osobowych od Ministra Zdrowia (Minister) polegające nauzyskaniu przy wykorzystaniu Elektronicznej Platformy danych lekarza oraz pozostałych informacji znajdujących się na recepcie.

Opis wydarzeń:

1. Prezes UODO zwrócił się do Ministra o złożenie dodatkowych wyjaśnień w przedmiotowej sprawie oraz ponowne, prawidłowe zawiadomienie osoby, której dane dotyczą o naruszeniu bezpieczeństwa danych osobowych.

2. W trakcie przeprowadzonych czynności kontrolnych ustalono, iż Minister:

.

a) poprosił o odszyfrowanie i udostępnienie danych z recepty wystawionej przez lekarza,

b) uzyskał powyższe dane za pośrednictwem komunikatora Whatsapp,

c) opublikował otrzymane informacje na platformie społecznościowej,

d) nie wdrożył polityki bezpieczeństwa danych osobowych zgodnej z RODO.

3. Na podstawie zebranego materiału dowodowego Prezes UODO uznał, że:

a) naruszono zasady bezpieczeństwa związanego z pozyskaniem tych danych z Elektronicznej Platformy oraz przekazaniem danych za pośrednictwem komunikatora Whatsapp,

b) Minister nie miał podstaw do publikacji danych osobowych lekarza na profilu społecznościowym,

c) nie dokonano prawidłowego zawiadomienia lekarza o naruszeniu ochrony jego danych osobowych.

4. Ostatecznie Minister usunął wpis z platformy społecznościowej, ale Prezes UODO nie odstąpił od nałożenia kary.

Przyczyna naruszenia:

Minister opublikował w serwisie społecznościowym wpis zawierający dane osobowe lekarza, który wystawił na siebie receptę na lek z grupy psychotropowych i przeciwbólowych.

Decyzja PUODO:

1. Kara pieniężna w wysokości 100 000 PLN.

2. Nakaz wdrożeniaodpowiednich środków technicznych i organizacyjnych w celu zminimalizowania ryzyka wiążącego się z przetwarzaniem danych osobowych przy wykorzystaniu Elektronicznej Platformy w szczególności wynikającego z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych, po uprzednim przeprowadzeniu analizy ryzyka, uwzględniającej stan wiedzy technicznej, koszt wdrożenia, charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych – w terminie 30 dni od doręczenia niniejszej decyzji.

3. Nakaz zawiadomienia osoby, której dane zostały ujawnione na platformie społecznościowej o naruszeniu ochrony danych osobowych – w terminie 3 dni od doręczenia niniejszej decyzji.

Źródło:

https://uodo.gov.pl/decyzje/DKN.5131.32.2023

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. Wykonuj udokumentowaną analizę ryzyka uwzględniającą stan faktyczny, charakterystykę zachodzących procesów, aktywa, podatności, zagrożenia oraz istniejące zabezpieczenia, w ramach zachodzących procesów przetwarzania danych osobowych.

Materiał edukacyjny przygotowany przez FORSAFE

Opracowanie merytoryczne
Katarzyna Kawczyńska