Kary i decyzje Prezesa Urzędu Ochrony Danych Osobowych

Data wydania decyzji: **23 czerwca 2022 r.**

Podmiot kontrolowany: **Prezydent Miasta O.**

Wysokość kary: **UPOMNIENIE**

FORSAFE BEZPIECZEŃSTWO PONAD WSZYSTKO

Rodzaj naruszenia

art. 5 ust. 1 lit. f), art. 5 ust. 2, art. 24 ust. 1, art. 25 ust. 1, art. 32 ust. 1 i 2 RODO
Niewystarczające środki techniczne i organizacyjne zapewniające bezpieczeństwo informacji.

Przedmiot decyzji

Źródło postępowania:

W październiku 2021 r. do Prezesa Urzędu Ochrony Danych Osobowych (UODO) wpłynęło zgłoszenie naruszenia ochrony danych osobowych od Prezydenta Miasta O. (Prezydent). Polegało ono na przełamaniu zabezpieczeń systemu informatycznego i zaszyfrowaniu za pomocą oprogramowania ransomware trzech serwerów wykorzystywanych do przetwarzania danych osobowych.

Opis wydarzeń:

1) Prezydent w wysłanym zgłoszeniu poinformował, iż:

a) naruszenie dotyczyło: pracowników, użytkowników, obecnych i potencjalnych klientów, klientów podmiotów publicznych Urzędu Miasta O.,

b) skala naruszenia obejmowała około 50 000 rekordów danych osobowych,

c) zakres naruszenia obejmował następujące dane osobowe: imię i nazwisko, imiona rodziców, data urodzenia, numer rachunku bankowego, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, adres e-mail, dane dotyczące zarobków lub/i posiadanego majątku, seria i numer dowodu osobistego, numer telefonu oraz nazwisko rodowe matki,

d) nie stwierdzono wystąpienia wysokiego ryzyka naruszenia praw lub wolności osób fizycznych, ale zdecydowano o wydaniu publicznego komunikatu zawiadamiającego osoby, których dane dotyczą, o naruszeniu ochrony ich danych osobowych.

2) Prezes UODO zwrócił się do Prezydenta o złożenie dodatkowych wyjaśnień dotyczących zaistniałej sytuacji.

3) Po ich otrzymaniu, Prezes UODO zdecydował o wszczęciu postępowania administracyjnego.

4) Na podstawie zebranego materiału dowodowego ustalono, że bezpośrednią przyczyną naruszenia był nieposiadający wsparcia producenta system operacyjny urządzenia służącego do wydawania kluczy (e-dozorca).

5) Ponadto Prezes UODO ustalił, iż Prezydent nie zapewnił:

a) skutecznych zabezpieczeń systemu informatycznego,

b) odpowiedniego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzanych danych osobowych w systemach informatycznych

Przyczyna naruszenia:

Prezydent nie wdrożył odpowiednich środków technicznych i organizacyjnych zapewniających bezpieczeństwo danych osobowych.

Decyzja PUODO:

Upomnienie

Źródło:

https://www.uodo.gov.pl/decyzje/DKN.5131.11.2022

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) Wykonuj cyklicznie analizę ryzyka dla systemów informatycznych i aplikacji, w których przetwarzasz dane osobowe.

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

4) Do przetwarzania danych osobowych wykorzystuj oprogramowanie posiadające aktualne wsparcie techniczne producenta.

Materiał edukacyjny przygotowany przez FORSAFE

Opracowanie merytoryczne
Katarzyna Cieślak