Kary Prezesa Urzędu Ochrony Danych Osobowych

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

Podmiot kontrolowany **Wójt Gminy Nowiny**

Wysokość kary **50 000 PLN**

FORSAFE
BEZPIECZEŃSTWO PONAD WSZYSTKO

Rodzaj naruszenia

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

Przedmiot decyzji

Źródło postępowania:

W grudniu 2021 r. Wójt Gminy Nowiny (Wójt) zgłosił do Prezesa Urzędu Ochrony Danych Osobowych (UODO) naruszenie ochrony danych osobowych, które polegało na zaszyfrowaniu serwera zawierającego bazę danych programu kadrowo-płacowego urzędu.

Opis wydarzeń:

1. Początek sprawy: Incydent miał miejsce po otworzeniu przez pracownika urzędu zainfekowanego linku.

2. Ustalenia powłamaniowe: CERT Polska poinformowało Wójta o wycieku danych z urzędu, które następnie zostały upublicznione.

3. Zakres danych: Naruszenie dotyczyło danych osobowych około 1 000 obecnych i byłych pracowników, zleceniobiorców i wykonawców, w tym imion i nazwisk, imion rodziców, dat urodzenia, numerów rachunków bankowych, adresów zamieszkania lub pobytu, numerów PESEL, nazwisk rodowych matek, adresów e-mail, serii i numerów dowodów osobistych oraz numerów telefonów.

4. Odzyskanie danych: Dział IT urzędu przywrócił dane tylko do września 2019 r. Dane zgromadzone po tej dacie zostały utracone, ponieważ ich kopie znajdowały się na zaszyfrowanym serwerze.

5. Stanowisko Prezesa UODO: Prezes UODO na podstawie zgromadzonych materiałów stwierdził, że Wójt był świadomy ryzyka utraty poufności danych i dostępu do nich z powodu ataku ransomware. Mimo to:

a) nie zainstalował odpowiedniego systemu antywirusowego na serwerach,

b) nie aktywował usługi firewall,

c) nie prowadził efektywnej polityki ochrony danych osobowych w zakresie tworzenia kopii zapasowych,

d) nie przeprowadzał testów odtwarzania danych z kopii zapasowych,

e) używał systemu, który nie był już wspierany przez producenta.

Przyczyna naruszenia:

Wójt nie wprowadził odpowiednich środków technicznych i organizacyjnych gwarantujących bezpieczeństwo przetwarzania danych na serwerach..

Decyzja PUODO:

1. Kara pieniężna w wysokości 50 000 PLN.

Źródło:

https://uodo.gov.pl/decyzje/DKN.5131.34.2022

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

3. Wykonuj kopie zapasowe na potrzeby zachowania ciągłości działania systemów informatycznych i utrzymania integralności danych.

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

5. Przeprowadzaj cykliczne szkolenia dla pracowników obejmujące przypomnienie stosowania się do wdrożonych procedur.

Materiał edukacyjny przygotowany przez FORSAFE

Opracowanie merytoryczne
Katarzyna Kawczyńska