Kary Prezesa Urzędu Ochrony Danych Osobowych

Data wydania decyzji **29 kwietnia 2024 r.**

Podmiot kontrolowany **Res-Gastro M. Gaweł Sp. K.**

Wysokość kary **238 345 PLN**

FORSAFE
BEZPIECZEŃSTWO PONAD WSZYSTKO

Rodzaj naruszenia

Art. 24 (1), art. 25 (1), art. 32 (1), (2) RODO.
Niewystarczające środki techniczne i organizacyjne zapewniające bezpieczeństwo informacji.

Przedmiot decyzji

Źródło postępowania:

W lipcu 2023 r. firma Res-Gastro M. Gaweł Sp. K. (Res-Gastro) zgłosiła do Prezesa Urzędu Ochrony Danych Osobowych (UODO) naruszenie ochrony danych osobowych związane z utratą służbowego pendriva przez pracownika, który zawierał częściowo zaszyfrowane dane osobowe innego pracownika.

Opis wydarzeń:

1. Postępowanie wyjaśniające: UODO zwróciło się do Res-Gastro o złożenie wyjaśnień.

2. Zakres danych: Res-Gastro poinformowało, że na nośniku znajdowały się niezaszyfrowane dane osobowe pracownika w zakresie: imię i nazwisko, adres zamieszkania, obywatelstwo, płeć, data urodzenia, numer PESEL, seria i numer paszportu, numer telefonu, adres e-mail, zdjęcie oraz informacje o wynagrodzeniu. Na pendrivie znajdowały się również zaszyfrowane pliki z danymi finansowymi.

3. Dodatkowe wyjaśnienia: Res-Gastro podkreśliło, że posiada procedury dotyczące korzystania z zewnętrznych nośników danych oraz że pracownicy otrzymali link do instruktażowego filmu o szyfrowaniu pendrivów.

4.Stanowisko Prezesa UODO: UODO stwierdziło, że Res-Gastro nie zaimplementowało odpowiednich środków technicznych i organizacyjnych, które zapewniałyby bezpieczeństwo danych na wymaganym poziomie przy użyciu zewnętrznych nośników danych. Ponadto, firma nie przeprowadzała regularnego testowania, mierzenia i oceniania skuteczności przyjętych środków technicznych i organizacyjnych.

Przyczyna naruszenia:

Firma Res-Gastro nie zastosowała odpowiednich środków technicznych i organizacyjnych, które zapewniałyby bezpieczeństwo przetwarzania danych na zewnętrznych nośnikach danych.

Decyzja PUODO:

1. Kara pieniężna w wysokości 238 345 PLN.

2. Nakaz wdrożenia odpowiednich środków technicznych i organizacyjnych w celu zapewnienia regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania– w terminie 3 miesięcy od dnia doręczenia decyzji

Źródło:

https://uodo.gov.pl/decyzje/DKN.5131.29.2023

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. Zabezpiecz wykorzystywane pendrivy poprzez:

a) wybór urządzenia z wbudowanym mechanizmem szyfrującym,

b) zaszyfrowanie urządzenia za pomocą funcji Bitlokera,

c) zaszyfrowanie urządzenia za pomocą oprogramowania np. VeraCrypt

Materiał edukacyjny przygotowany przez FORSAFE

Opracowanie merytoryczne
Katarzyna Kawczyńska