Kary i decyzje Prezesa Urzędu Ochrony Danych Osobowych

Data wydania decyzji 01 czerwca 2022 r.

Podmiot kontrolowany Miejski Ośrodek Pomocy Społecznej w O.

Wysokość kary UPOMNIENIE

FORSAFE
BEZPIECZEŃSTWO PONAD WSZYSTKO

Rodzaj naruszenia

art. 5 ust. 1 it. 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 czerwcu 2021 r. do Prezesa Urzędu Ochrony Danych Osobowych (UODO) wpłynęło zgłoszenie naruszenia ochrony danych osobowych od Miejskiego Ośrodka Pomocy Społecznej w O. (MOPS). Naruszenie polegało na zagubieniu nieszyfrowanej przenośnej pamięci zewnętrznej typu pendrive przez pracownika MOPS.

Opis wydarzeń:

1) MOPS w wysłanym zgłoszeniu poinformował, iż:

a) wiedzę o naruszeniu powziął od Prezesa UODO, który poinformował o przekazaniu przez anonimową osobę do UODO znalezionej przenośnej pamięci zewnętrznej typu pendrive z danymi osobowymi,

b) skala naruszenia obejmowała 50 osób – pracownicy i podopieczni, w tym dzieci,

c) zakres naruszenia obejmował następujące dane osobowe – imię i nazwisko, imiona rodziców, data urodzenia, adres zamieszkania lub pobytu, numer PESEL oraz dane dotyczące zdrowia,

d) osoby zostały poinformowane o naruszeniu ich danych osobowych.

2) Prezes UODO uznał jednak, że treść wysłanego zgłoszenia nie spełnia wymagań wskazanych w RODO. Nakazał więc o ponowne zawiadomienie osób, których dotyczyło naruszenie oraz zwrócił się do MOPS o złożenie dodatkowych wyjaśnień w przedmiotowej sprawie.

3) Biorąc pod uwagę zaistniałą sytuację Prezes UODO wszczął z urzędu postępowanie administracyjne w przedmiocie nałożenia na Spółkę administracyjnej kary pieniężnej.

Przyczyna naruszenia:

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

Decyzja PUODO:

Upomnienie.

Źródło:

https://www.uodo.gov.pl/decyzje/DKN.5131.2.2022

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) Zabezpiecz wykorzystywane pendrivy poprzez:

a) wybór urządzenia z wbudowanym mechanizmem szyfrującym,

b) zaszyfrowanie urządzenia za pomocą funkcji Bitlokera,

c) zaszyfrowanie urządzenia za pomocą oprogramowania np. VeraCrypt.

Materiał edukacyjny przygotowany przez FORSAFE

Opracowanie merytoryczne
Katarzyna Cieślak