Kary i decyzje Prezesa Urzędu Ochrony Danych Osobowych

Data wydania decyzji: **14 czerwca 2022 r.**

Podmiot kontrolowany: **Pani K.Z. prowadząca działalność gospodarczą**

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 marcu 2021 r. do Prezesa Urzędu Ochrony Danych Osobowych (UODO) wpłynęło zgłoszenie naruszenia ochrony danych osobowych od Pani K.Z. prowadzącej działalność gospodarczą (Przedsiębiorca). Naruszenie polegało na zaszyfrowaniu danych osobowych pracowników oraz pacjentów za pomocą złośliwego oprogramowania.

Opis wydarzeń:

1) Spółka w wysłanym zgłoszeniu poinformowała, iż:

a) skala naruszenia obejmowała 7000 osób,

b) zakres naruszenia obejmował następujące dane osobowe:

- HR – zawieranie umów z pracownikami, realizacja wynagrodzenia, umowy z pracownikami, oświadczenia – imię, nazwisko, numer PESEL, adres, dane przedsiębiorstwa: nazwa, adres, REGON, NIP, numer konta bankowego;
- księgowość – realizacja umów, zakupy, płatność faktury VAT, kontrahenci, faktury, umowy – dane przedsiębiorstwa: nazwa, REGON, NIP, numer konta bankowego, adres, numer telefonu, adres e-mail;
- świadczenie usług medycznych – pacjenci, karty pacjentów, deklaracje, oświadczenia – imię, nazwisko, numer PESEL, adres, NIP płatnika składek ZUS, adres e-mail, numer telefonu, historia choroby, wyniki badań

2) Prezes UODO zwrócił się do Przedsiębiorcy 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:

a) faktyczna liczba osób objętych naruszeniem to 6591,

b) przyczyną naruszenia było przełamanie zabezpieczeń serwera.

Przyczyna naruszenia:

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

Decyzja PUODO:

1) Upomnienie.

2) Nakaz dostosowania operacji przetwarzania poprzez:

a) przeprowadzenie analizy ryzyka w celu oszacowania właściwego poziomu ryzyka wiążącego się z przetwarzaniem danych osobowych,

b) wdrożenie odpowiednich środków technicznych i organizacyjnych w celu zapewnienia zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego,

c) wdrożenie odpowiednich środków technicznych i organizacyjnych w celu zapewnienia regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

Źródło:

https://www.uodo.gov.pl/decyzje/DKN.5131.56.2021

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.

Materiał edukacyjny przygotowany przez FORSAFE

Opracowanie merytoryczne
Katarzyna Cieślak