Kary Prezesa Urzędu Ochrony Danych Osobowych

Data wydania decyzji **31 maja 2023 r.**

Podmiot kontrolowany **P. Sp. z o.o.**

Wysokość kary **47 160 PLN**

FORSAFE
BEZPIECZEŃSTWO PONAD WSZYSTKO

Rodzaj naruszenia

art. 5 ust. 1 lit. f), art. 5 ust. 2, art. 25 ust. 1, art. 32 ust. 1 i 2, art. 33 ust. 1, art. 34 ust. 1 i 2 RODO. Niewystarczające środki techniczne i organizacyjne zapewniające bezpieczeństwo informacji.

Przedmiot decyzji

Źródło postępowania:

W lipcu 2020 r. do Prezesa Urzędu Ochrony Danych Osobowych (UODO) wpłynęła informacja wskazująca na utratę dokumentacji koncesyjnej prowadzonej w formie elektronicznej przez P. Sp. z o.o. (Spółka).

Opis wydarzeń:

1. W zawiadomieniu wskazano, że dokumentacja najprawdopodobniej zawierała dane osobowe pracowników ochrony zatrudnionych na podstawie umowy o pracę oraz osób świadczących usługi w ramach zawartych umów cywilnoprawnych, a także osób fizycznych będących stronami umów cywilnoprawnych na usługę ochrony zawartych przez Spółkę.

2. Prezes UODO zwrócił się do Spółki o złożenie wyjaśnień w przedmiotowej sprawie i wyjaśnienie, czy została przeprowadzona analiza pod kątem ryzyka naruszenia praw lub wolności osób fizycznych.

3. W odpowiedzi na powyższe oraz kolejne zapytania Spółka wskazała, iż:

a) w wyniku ataku ransomware doszło do zaszyfrowania danych osobowych znajdujących się na trzech serwerach,

b) na powyższych serwerach znajdowały się dane osobowe pracowników Spółki i osób świadczących na rzecz Spółki usługi w ramach zawartych umów cywilnoprawnych,

c) utracono dostęp do następujących danych osobowych – nazwiska, imiona, daty urodzenia, numery rachunków bankowych, adresy zamieszkania lub pobytu, numery PESEL, adresy e-mail, dane dotyczące zarobków, numery telefonów oraz numery dowodów osobistych,

d) zdarzenie dotyczyło danych około 30 osób,

e) nie udało się odszyfrować danych i utracono do nich dostęp w formie elektronicznej,

f) nie odnotowano pobrania danych z serwerów, a tym samym nie doszło do naruszenia praw lub wolności osób fizycznych.

4. Biorąc pod uwagę powyższe wyjaśnienia, a także brak zgłoszenia naruszenia oraz brak zawiadomienia osób o naruszeniu ich danych osobowych, Prezes UODO wszczął z urzędu postępowanie administracyjne w przedmiocie nałożenia na Spółkę administracyjnej kary pieniężnej.

5. Na podstawie zebranego materiału dowodowego Prezes UODO uznał, że Spółka:

a) nie wdrożyła odpowiednich środków technicznych i organizacyjnych zapewniających bezpieczeństwo przetwarzania danych w systemach informatycznych oraz ochronę praw osób, których dane dotyczą,

b) nie wdrożyła odpowiednich środków technicznych i organizacyjnych w celu zapewnienia regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzanych danych osobowych w systemach informatycznych,

c) nie zgłosiła naruszenia ochrony danych osobowych bez zbędnej zwłoki,

d) nie zawiadomiła bez zbędnej zwłoki osób, których dane dotyczą, o naruszeniu ochrony ich danych osobowych.

Przyczyna naruszenia:

Spółka nie dokonała adekwatnego doboru zabezpieczeń systemu informatycznego wykorzystywanego do przetwarzania danych osobowych oraz nie realizowała odpowiedniego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzanych danych osobowych w systemach informatycznych.

Decyzja PUODO:

1. Kara pieniężna w wysokości 47 160 PLN.

Źródło:

https://www.uodo.gov.pl/decyzje/DKN.5131.8.2021

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. 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 oraz weryfikuj je pod kątem możliwości ich odtworzenia.

4. Gdy ocenisz, że naruszenie ochrony danych osobowych może powodować ryzyko dla naruszenia praw lub wolności osób fizycznych, dokonaj zgłoszenia naruszenia ochrony danych osobowych do Prezesa Urzędu Ochrony Danych Osobowych. Na zgłoszenie masz 72 godziny od momentu stwierdzenia naruszenia.

5. Gdy ocenisz, że naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, dokonaj zawiadomienia osób fizycznych, których dane dotyczą, o zaistniałym naruszeniu. Zawiadomienia należy wykonać bez zbędnej zwłoki.

Materiał edukacyjny przygotowany przez FORSAFE

Opracowanie merytoryczne
Katarzyna Kawczyńska