Kary i decyzje Prezesa Urzędu Ochrony Danych Osobowych

Data wydania decyzji **05.01.2021 r.**

Podmiot kontrolowany **Pani M. Z. prowadząca działalność gospodarczą pod firmą K.**

Wysokość kary **85 588 PLN**

FORSAFE
BEZPIECZEŃSTWO PONAD WSZYSTKO

Rodzaj naruszenia

Naruszenie Art. 58 ust. 2 lit. e) RODO.
Nieprzestrzeganie nakazu decyzji administracyjnej.

Przedmiot decyzji

Źródło postępowania:

W lipcu 2019 r. do Prezesa Urzędu Ochrony Danych Osobowych (UODO) wpłynęła informacja od Pani M. Z. prowadzącej działalność gospodarczą pod firmą K. (Przedsiębiorca) o naruszeniu ochrony danych osobowych, które polegało na nieuprawnionym skopiowaniu w kwietniu 2019 roku danych osobowych stu pacjentów z systemu informatycznego przychodni przez byłego pracownika celem wykorzystania ich do marketingu własnych usług.

Opis wydarzeń:

1) Nieuprawniony dostęp do danych obejmował następujące dane osobowe pacjentów: numer PESEL, imię i nazwisko, imiona rodziców, data urodzenia, adres zamieszkania lub pobytu oraz numer telefonu.

2) Przedsiębiorca nie poinformował osób, których dane dotyczą, o naruszeniu ochrony danych osobowych, pomimo, że ocenił ryzyko naruszenia praw i wolności osób fizycznych jako wysokie.

3) Prezes UODO w odpowiedzi na zgłoszenie, wezwał Przedsiębiorcę do niezwłocznego zawiadomienia osób, których dane dotyczą, o naruszeniu ochrony ich danych osobowych.

4) Przedsiębiorca nie zareagował na pismo Prezesa UODO i w konsekwencji zostało wszczęte postępowanie administracyjne w tej sprawie, którego efektem był nakaz zawiadomienia osób, których dotyczyło naruszenie w terminie trzech dni od dnia, w którym decyzja stanie się ostateczna.

5) Gdy decyzja administracyjna stała się prawomocna, Prezes UODO wszczął kolejne postępowanie celem sprawdzenia, czy nałożone obowiązki zostały wykonane i wezwał Przedsiębiorcę do przedłożenia dowodów.

6) W odpowiedzi na powyższe wezwanie Przedsiębiorca pismem poinformował, że nie jest w stanie ustalić, których pacjentów dotyczyło naruszenie.

7) Prezes UODO ponownie wezwał Przedsiębiorcę do zrealizowania nałożonych na niego obowiązków w terminie 7 dni oraz przedłożenia dowodów ich wykonania.

8) W odpowiedzi na wezwanie pełnomocnik Przedsiębiorcy okazał kopie zawiadomień, które okazały się niekompletne w zakresie treści, jaka powinna być wysłana do osób objętych naruszeniem.

9) Prezes PUODO dokonał ponownego wezwania Przedsiębiorcy do zrealizowania nałożonych na niego obowiązków zgodnie z wytycznymi.

10) W odpowiedzi na ponowne wezwanie do złożenia wyjaśnień pełnomocnik Przedsiębiorcy wyjaśnił, że wszystkie punkty wskazane w wezwaniu zostały spełnione i nie ma podstaw do ponownego wysyłania zawiadomień do pacjentów.

11) W ocenie PUODO, Przedsiębiorca nie zrealizował nałożonych na niego obowiązków i nałożono na niego karę pieniężną.

Przyczyna naruszenia:

Niewykonanie przez Przedsiębiorcę nakazu decyzji administracyjnej Prezesa Urzędu Ochrony Danych Osobowych z lutego 2020 roku.

Decyzja PUODO:

1) Kara pieniężna w wysokości 85 588 PLN

Kompas FORSAFE

JAK UNIKAĆ TAKICH NARUSZEŃ?

1) Dokonując zgłoszenia naruszenia danych osobowych, współpracuj z Prezesem Urzędu Ochrony Danych Osobowych oraz wykonuj jego zalecenia, wytyczne, nakazy lub decyzje.

2) 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. Przykładowe formy przekazania informacji o naruszeniu to: komunikat widoczny bezpośrednio na stronie internetowej, bez konieczności otwierania dodatkowych podstron, komunikat na portalu społecznościowym, komunikat na lokalnych witrynach internetowych, ogłoszenia w gazetach.

3) Nadając uprawnienia dostępu do danych osobowych w systemie informatycznym pamiętaj, aby były one skorelowane z zakresem obowiązków przypisanym do danego stanowiska.

4) Wykonuj cykliczne przeglądy nadanych uprawnień dostępu do danych osobowych w systemach informatycznych.

5) Odbieraj uprawnienia w systemie informatycznym osobom, którym wygasło upoważnienie.

6) Weryfikuj programy i aplikacje w zakresie rejestrowania eksportu danych.

Materiał edukacyjny przygotowany przez FORSAFE

Opracowanie merytoryczne
Katarzyna Cieślak