Kary i decyzje Prezesa Urzędu Ochrony Danych Osobowych

Data wydania decyzji

21 czerwca 2021 r.

Podmiot kontrolowany

Sopockie Towarzystwo Ubezpieczeń ERGO Hestia S.A.

Wysokość kary

159 176 PLN

FORSAFE BEZPIECZEŃSTWO PONAD WSZYSTKO

Rodzaj naruszenia

Naruszenie art. 33 ust. 1 RODO, art. 34 ust. 1 RODO
Niewystarczające wypełnienie obowiązków powiadamiania o naruszeniu danych

Przedmiot decyzji

Źródło postępowania:

We wrześniu 2020 roku Spółka z branży ubezpieczeniowej zgłosiła do Prezesa Urzędu Ochrony Danych Osobowych (UODO) naruszenie ochrony danych osobowych, które polegało na wysłaniu pocztą elektroniczną do niewłaściwego odbiorcy analizy potrzeb ubezpieczeniowych oraz oferty ubezpieczenia.

Opis wydarzeń:

1) Przyczyną naruszenia ochrony danych osobowych była pomyłka pracownika Spółki, który wysyłając wiadomości e-mail, wpisał błędny adres, wobec czego korespondencja została przekazana do osoby nieuprawnionej.

2) W związku z powyższym doszło do ujawnienia następujących danych klienta Spółki:
a) imię i nazwisko – dla których Administratorem jest Spółka,
b) imię, nazwisko, numer PESEL, miejscowość, kod pocztowy, informacja o przedmiocie ubezpieczenia, informacja o produkcie ubezpieczeniowym, suma ubezpieczenia/suma gwarancyjna oraz wysokość składki – dla których Administratorem są Towarzystwa Ubezpieczeniowe.

3) Spółka będąc jednocześnie Administratorem jak i podmiotem przetwarzającym dla Towarzystw Ubezpieczeniowych, dopełniając swoich obowiązków poinformowała je o naruszeniu.

4) Z ustaleń Prezesa UODO wynika, że wszystkie Towarzystwa Ubezpieczeniowe dokonały zgłoszenia naruszenia ochrony danych osobowych z wyjątkiem Sopockiego Towarzystwa Ubezpieczeń ERGO Hestia S.A. (ERGO Hestia).

5) Aby we właściwy sposób ocenić zaistniałą sytuację Prezes UODO zwrócił się do ERGO Hestia o złożenie wyjaśnień.

6) W odpowiedzi na pismo ERGO Hestia potwierdziła, że doszło do naruszenia ochrony danych osobowych, ale zdarzenie to nie skutkowało koniecznością zawiadomienia Prezesa UODO oraz osoby, której danych osobowych naruszenie dotyczy. Swoją decyzję argumentowała wykonaną oceną pod kątem ryzyka naruszenia praw i wolności osób fizycznych w formularzu oceny naruszenia ochrony danych osobowych. Dodatkowo ERGO Hestia wskazała, że osoba nieuprawniona złożyła pisemne oświadczenie o niezapoznaniu się z treścią załącznika do e-maila, w którym były dane, i o trwałym jego usunięciu.

7) Pomimo złożonych wyjaśnień, Prezes UODO wszczął z urzędu postępowanie administracyjne w przedmiocie nałożenia na ERGO Hestia administracyjnej kary pieniężnej w związku z brakiem zgłoszenia naruszenia ochrony danych osobowych Prezesowi UODO oraz brakiem zawiadomienia o naruszeniu ochrony danych osobowych osoby, której dotyczyło naruszenie.

8) W odpowiedzi na pismo ERGO Hestia złożyła dodatkowe wyjaśnienia, ale Prezes UODO uznał jednak, że dokonana przez ERGO Hestia ocena została przeprowadzona niewłaściwie oraz wskazał kilka nieprawidłowości:
a) zaniżanie wyników w poszczególnych kryteriach,
b) brak uwzględnienia istotnych czynników dla poszczególnych kryteriów,
c) uwzględnienie czynników, które nie powinny mieć zastosowania.

Przyczyna naruszenia:

Brak zgłoszenia naruszenia ochrony danych osobowych Prezesowi UODO oraz brak zawiadomienia o naruszeniu ochrony danych osobowych osoby, której dotyczyło naruszenie.

Decyzja PUODO:

1) Kara pieniężna w wysokości 159 176 PLN.

2) Zawiadomienie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych w terminie 3 dni od dnia doręczenia decyzji.

Kompas FORSAFE

JAK UNIKAĆ TAKICH NARUSZEŃ?

1) Wykonaj ocenę naruszenia ochrony danych osobowych pod kątem wystąpienia ryzyka dla praw i wolności osób fizycznych. Dokonując oceny weź pod uwagę:
a) konkretne okoliczności naruszenia, w tym wagę potencjalnego wpływu i prawdopodobieństwo jego wystąpienia,
b) czy naruszenie może prowadzić do uszczerbku fizycznego lub szkód majątkowych lub niemajątkowych dla osób, których dane zostały naruszone. Przykładami takich szkód są: utrata kontroli nad własnymi danymi osobowymi, nieuprawnione odwrócenie pseudonimizacji, dyskryminacja, kradzież lub sfałszowanie tożsamości, straty finansowe, naruszenie dobrego imienia, naruszenie poufności danych osobowych chronionych tajemnicą zawodową lub wszelkie inne znaczne szkody gospodarcze lub społeczne,
c) liczbę osób fizycznych, na które naruszenie wywiera wpływ.

2) 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.

3) Jeśli masz wątpliwości co do oceny ryzyka dla naruszenia praw lub wolności osób fizycznych, dokonaj zgłoszenia naruszenia bezpieczeństwa danych osobowych, nawet jeśli taka ostrożność mogłaby się okazać nadmierna.

4) 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.

5) Nie wykonuj oceny naruszenia ochrony danych osobowych w sposób schematyczny, gdyż każda ocena jest inna i należy do niej podchodzić indywidualnie.

Materiał edukacyjny przygotowany przez FORSAFE

Opracowanie merytoryczne
Katarzyna Cieślak