Kary i decyzje Prezesa Urzędu Ochrony Danych Osobowych

Data wydania decyzji **11.01.2021 r.**

Podmiot kontrolowany **ENEA S.A.**

Wysokość kary **136 437 PLN**

FORSAFE
BEZPIECZEŃSTWO PONAD WSZYSTKO

Rodzaj naruszenia

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

Przedmiot decyzji

Źródło postępowania:

W czerwcu 2020 r. do Prezesa Urzędu Ochrony Danych Osobowych (UODO) wpłynęła informacja o naruszeniu ochrony danych osobowych pochodząca od osoby, która stała się nieuprawnionym adresatem przedmiotowych danych osobowych.

Opis wydarzeń:

1) Osoba związana z ENEA S.A. (Spółka) wysłała do nieuprawnionego adresata wiadomość e-mail z załącznikiem zawierającym dane osobowe adresata oraz 259 innych osób będących klientami Spółki.

2) W wyniku tego zdarzenia doszło do naruszenia poufności danych w zakresie: imion, nazwisk, adresów e-mail, numerów telefonów oraz informacji dotyczących daty rejestracji.

3) Osoba, która przesłała wiadomość wraz z niewłaściwym, niezaszyfrowanym plikiem zawierającym dane osobowe, była współpracownikiem firmy, z którą współpracuje wykonawca prowadzący dla Spółki badania jakościowe. Co więcej wspomniana osoba wysłała wiadomość z konta e-mail niebędącego jej kontem służbowym.

4) W związku z otrzymanym zgłoszeniem Prezes UODO zwrócił się do Spółki o wyjaśnienia.

5) W odpowiedzi na pismo Spółka potwierdziła, że doszło do naruszenia ochrony danych osobowych, ale zdarzenie to nie skutkowało koniecznością zawiadomienia Prezesa UODO.

6) Spółka na polecenie Prezesa UODO dokonała ponownej analizy ryzyka, która wykazała wynik analogiczny do wyniku pierwotnej analizy, czyli potwierdziła, że istnieje małe prawdopodobieństwo naruszenia praw lub wolności osób, których dane dotyczą.

7) Prezes UODO dokonując oceny kolejnych wyjaśnień ze strony Spółki stwierdził, iż nie wskazała ona żadnych dodatkowych środków zaradczych niwelujących ryzyko naruszenia praw lub wolności osób związanych z przedmiotowym zdarzeniem.

Przyczyna naruszenia:

Błąd pracownika podmiotu współpracującego z ENEA S.A.

Decyzja PUODO:

1) Kara pieniężna w wysokości 136 437 PLN

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, 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) Kontroluj podmioty przetwarzające m.in. w zakresie wdrożonych środków organizacyjnych i technicznych zapewniających bezpieczeństwo danych.

Materiał edukacyjny przygotowany przez FORSAFE

Opracowanie merytoryczne
Katarzyna Cieślak