Kary i decyzje Prezesa Urzędu Ochrony Danych Osobowych

Data wydania decyzji: **19 stycznia 2022 r.**

Podmiot kontrolowany: **Fortum Marketing and Sales Polska S.A.**

Wysokość kary: **4 911 732 PLN**

FORSAFE BEZPIECZEŃSTWO PONAD WSZYSTKO

Rodzaj naruszenia

Naruszenie art. 5 ust. 1 lit. f), art. 25 ust. 1, art. 28 ust. 1, art. 32 ust. 1 i 2 RODO.
Niewystarczające środki techniczne i organizacyjne zapewniające bezpieczeństwo informacji.

Przedmiot decyzji

Źródło postępowania:

W kwietniu 2020 r. do Prezesa Urzędu Ochrony Danych Osobowych (UODO) wpłynęło zgłoszenie naruszenia ochrony danych osobowych od Fortum Marketing and Sales Polska S.A. (Spółka) polegające na skopiowaniu danych klientów przez nieuprawnione podmioty z programu, którego dostawcą była PIKA Sp. z o.o. (PIKA).

Opis wydarzeń:

1) O fakcie nieuprawnionego skopiowania bazy danych Spółka dowiedziała się od dwóch niezależnych internautów, którzy poinformowali ją, iż posiadają dostęp do bazy jej klientów.

2) Źródłem naruszenia było zlecenie przez Spółkę firmie PIKA wprowadzenia zmian w środowisku teleinformatycznym do obsługi archiwum cyfrowego w celu zwiększenia wydajności działania repozytorium.

3) Zmiana polegała na utworzeniu nowego serwera dla bazy danych.

4) Wdrożone przez PIKA rozwiązanie nie zostało skonsultowane ze Spółką, która nie miała możliwości przetestowania go w środowisku testowym.

5) Jednocześnie Spółka nie zażądała od PIKA przedstawienia projektów zmian oraz nie zweryfikowała, czy zapewniają one bezpieczeństwo przetwarzania danych osobowych swoich klientów.

6) Nowoutworzona baza danych zawierała następujące dane o klientach: imię i nazwisko, adres zamieszkania lub pobytu, numer PESEL, rodzaj, seria i numer dokumentu tożsamości, adres e-mail, numer telefonu, numer i adres punktu poboru oraz dane dotyczące umowy (np. data i numer umowy, rodzaj paliwa, numer licznika).

7) Naruszenie ochrony danych osobowych dotyczyło 120 428 osób.

8) Spółka nie dokonała zawiadomienia osób, których dane dotyczą o naruszeniu ochrony danych osobowych uznając, iż nie wystąpiło wysokie ryzyko naruszenia praw lub wolności osób fizycznych.

9) W związku z powyższym Prezes UODO zwrócił się do Spółki o niezwłoczne zawiadomienie osób, których dane dotyczą, o naruszeniu ich danych osobowych.

10) W odpowiedzi na powyższe pismo Spółka poinformowała Prezesa UODO o realizacji jego zaleceń.

Przyczyna naruszenia:

Spółka nie wdrożyła odpowiednich środków technicznych i organizacyjnych zapewniających bezpieczeństwo danych osobowych oraz nie dokonała weryfikacji podmiotu przetwarzającego.

Decyzja PUODO:

1) Kara pieniężna w wysokości 4 911 732 PLN.

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 przetwarzanych danych osobowych w systemach teleinformatycznych.

3) Nadzoruj i monitoruj prace rozwojowe nad systemami informatycznymi.

4) Kontroluj podmioty przetwarzające m.in. w zakresie wdrożonych środków organizacyjnych i technicznych zapewniających bezpieczeństwo danych, notyfikacji naruszeń ochrony danych osobowych.

Pamiętaj!
Podpisanie umowy powierzenia przetwarzania danych osobowych bez audytu podmiotu przetwarzającego nie może być uznane jako spełnienie obowiązku przeprowadzenia postępowania weryfikującego podmiot przetwarzający pod kątem spełnienia przez niego wymogów RODO.

Materiał edukacyjny przygotowany przez FORSAFE

Opracowanie merytoryczne
Katarzyna Cieślak