Kary i decyzje Prezesa Urzędu Ochrony Danych Osobowych

Data wydania decyzji	14 października 2021 r.
Podmiot kontrolowany	Bank Millennium S.A.
Rodzaj kary	363 832 PLN

FORSAFE
BEZPIECZEŃSTWO PONAD WSZYSTKO

Rodzaj naruszenia

Naruszenie art. 33 (1), art. 34 (1) RODO.
Niewystarczające wypełnienie obowiązku powiadomienia o naruszeniu danych.

Przedmiot decyzji

Źródło postępowania:

Do Prezesa Urzędu Ochrony Danych Osobowych (UODO) wpłynęła skarga na Bank Millennium S.A. (Bank), której przedmiotem były nieprawidłowości w procesie przetwarzania danych osobowych Skarżących polegające na zagubieniu dokumentacji zawierającej dane osobowe Skarżących, przekazanej Bankowi w związku z procedurą założenia konta bankowego. Zaistniała sytuacja miała miejsce w jednym z oddziałów Banku.

Opis wydarzeń:

1) Skarżący w maju 2019 r. zostali powiadomieni o zagubieniu dokumentacji zawierającej ich dane osobowe. W związku z powyższym udali się do Banu celem uzyskania szczegółowych informacji w przedmiotowej sprawie.

2) Skarżący nie uzyskali dodatkowych wyjaśnień, więc dokonali zgłoszenia reklamacyjnego, które zostało złożone w placówce Banku.

3) Biorąc pod uwagę powyższe, Prezes UODO zwrócił się do Banku o wyjaśnienie, czy w związku z zaistniałym zdarzeniem zostało dokonane zgłoszenie naruszenia ochrony danych osobowych i czy dopełniono obowiązku zawiadomienia osób, których dane dotyczą, o naruszeniu ich danych osobowych. Prezes UODO poprosił również o złożenie dodatkowych wyjaśnień w przedmiotowej sprawie.

4) Bank w odpowiedzi na otrzymane pismo udzielił następujących wyjaśnień:

a) oddział Banku nadał do Centrali Banku przesyłkę, w której znajdowały się dokumenty takie jak: pełnomocnictwo, umowy na określone produkty Banku a także ankieta i jej wyniki,

b) na dokumentach znajdowały się w następujące dane: imię, nazwisko, PESEL, adres zameldowania, numery rachunków bankowych, numer CIF (numer identyfikacyjny nadawany klientom Banku) Skarżącej oraz imię, nazwisko i PESEL Skarżącego,

c) podmiotem odpowiedzialnym za dostarczenie dokumentów była firma kurierska, która ostatecznie poinformowała Bank, że nie zdołała zlokalizować przesyłki i zakończyła próby jej poszukiwania,

d) Bank wykorzystując metodologię ENISA ocenił zdarzenie jako mogące powodować średnie ryzyko naruszenia praw i wolności Skarżących, więc Bank nie zgłosił naruszenia do Prezesa Urzędu Ochrony Danych Osobowych oraz nie zawiadomił osób o naruszeniu ochrony ich danych osobowych,

e) Bank przesłał Skarżącym ogólne informacje dotyczące charakteru naruszenia oraz informacje o środkach pozwalających na zminimalizowanie jego ewentualnych negatywnych skutków, w tym umożliwienie skorzystania z bezpłatnej usługi Alert.

5) W związku z zaistniałą sytuacją, Prezes UODO wszczął z urzędu postępowanie administracyjne w przedmiocie nałożenia na Bank administracyjnej kary pieniężnej.

6) W odpowiedzi na zawiadomienie o wszczęciu postępowania administracyjnego Bank przesłał dodatkowe wyjaśnienia i załączył dokonaną ocenę pod kątem ryzyka naruszenia praw i wolności osób fizycznych.

7) Ostatecznie Prezes UODO zdecydował o nałożeniu na Bank kary pieniężnej.

Przyczyna naruszenia:

Bank nie dokonał zgłoszenia Prezesowi UODO naruszenia ochrony danych osobowych oraz nie zawiadomił o naruszeniu ochrony danych osobowych osób, których dane dotyczą.

Decyzja PUODO:

1) Kara pieniężna w wysokości 363 832 PLN.

2) Zawiadomienie osób o naruszeniu ochrony ich danych osobowych – w terminie 3 dni od dnia doręczenia niniejszej 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) Ocenę ryzyka naruszenia praw lub wolności osoby fizycznej dokonaj przez pryzmat osoby dotkniętej naruszeniem, a nie interesów Administratora.

3) 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 UODO. Na zgłoszenie masz 72 godziny od momentu stwierdzenia naruszenia.

4) 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.

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.

6) Pamiętaj, że obowiązek zawiadomienia osoby fizycznej o naruszeniu nie jest uzależniony od materializacji negatywnych konsekwencji dla takiej osoby, ale od samej możliwości wystąpienia takiego ryzyka.

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

8) Wpisz naruszenie ochrony danych osobowych do wewnętrznej ewidencji naruszeń

Materiał edukacyjny przygotowany przez FORSAFE

Opracowanie merytoryczne
Katarzyna Cieślak