

Kary i decyzje Prezesa Urzędu Ochrony Danych Osobowych



Data wydania decyzji

19 stycznia 2022 r.

Podmiot kontrolowany

**Santander Bank Polska
S.A.**

Wysokość kary

545 748 PLN**FÖRSÄFE**
BEZPIECZEŃSTWO PONAD WSZYSTKO**Rodzaj naruszenia**

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

**Przedmiot decyzji****Źródło postępowania:**

W lutym 2021 r. do Prezesa Urzędu Ochrony Danych Osobowych (UODO) wpłynęło zgłoszenie naruszenia ochrony danych osobowych od Santander Bank Polska S.A. (Bank) polegające na posiadaniu przez byłego pracownika Banku nieuprawnionego dostępu do Platformy Usług Elektronicznych ZUS (PUE ZUS).

Opis wydarzeń:

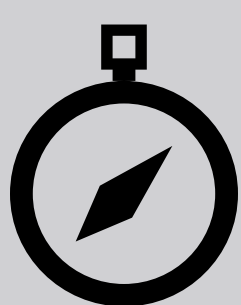
- 1) W lutym 2021 r. były pracownik Banku w wiadomości elektronicznej poinformował, iż nadal posiada dostęp do PUE ZUS z ramienia Banku jako Płatnika.
- 2) W związku z powyższym były pracownik Banku mógł przeglądać znajdujące się w profilu Banku dane pracowników w zakresie: imię i nazwisko, numer PESEL, adres zamieszkania lub pobytu, informacja o zwolnieniu lekarskim.
- 3) Bank na prośbę Prezesa UODO ustalił, iż były pracownik Banku pięciokrotnie logował się do platformy PUE ZUS po zakończeniu stosunku pracy.
- 4) Naruszenie ochrony danych osobowych dotyczyło 10 500 osób.
- 5) Zaistniała sytuacja miała miejsce ze względu na to, że byłemu pracownikowi Banku nie odebrano po zakończeniu stosunku pracy dostępu do PUE ZUS.
- 6) Bank nie dokonał zawiadomienia osób, których dane dotyczą o naruszeniu ochrony danych osobowych uznając, iż były pracownik Banku w trakcie zatrudnienia na swoim stanowisku pracy miał dostęp do szerszego katalogu danych pracowniczych.
- 7) Prezes UODO uznał jednak, że w wyniku zaistniałej sytuacji doszło do naruszenia poufności danych, które wiąże się z wysokim ryzykiem naruszenia praw lub wolności osób fizycznych, co powoduje konieczność zawiadomienia osób, których dane dotyczą, o naruszeniu ochrony ich danych osobowych.

Przyczyna naruszenia:

Bank nie dokonał bez zbędnej zwłoki zawiadomienia o naruszeniu ochrony danych osobowych osób, których dane dotyczą.

Decyzja PUODO:

- 1) Kara pieniężna w wysokości 545 748 PLN.
- 2) Nakaz zawiadomienia osób, których dane dotyczą o naruszeniu ochrony ich danych osobowych – w terminie 3 dni od dnia doręczenia decyzji.

**Kompas FÖRSÄFE****JAK UNIKAĆ TAKICH NARUSZEŃ?**

- 1) Odbieraj uprawnienia w systemie informatycznym osobom, którym wygasło upoważnienie.
- 2) Wykonuj cykliczne przeglądy nadanych uprawnień dostępu do danych osobowych w systemach informatycznych.
- 3) 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.
- 4) 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.

