Kary organów nadzorczych w Unii Europejskiej

Kraj oraz organ nadzorczy

Irlandia

Data Protection Authority of Ireland

Data wydania decyzji

05 kwiecień 2022 r.

Podmiot kontrolowany

Bank of Ireland

Wysokość kary

463 000 EUR

FORSAFE
BEZPIECZEŃSTWO PONAD WSZYSTKO

Rodzaj naruszenia

Art. 32 RODO, Art. 33 RODO, Art. 34 RODO.
Niewystarczające środki techniczne i organizacyjne zapewniające bezpieczeństwo informacji.

Przedmiot decyzji

Źródło postępowania:

Bank of Ireland (Bank) dokonał zgłoszenia do irlandzkiego organu nadzorczego 22 naruszeń ochrony danych osobowych. Polegały one na wysłaniu do Centralnego Rejestru Kredytów niedokładnych lub niewłaściwych danych klientów, co skutkowało błędnym obrazem ich sytuacji finansowej oraz historii kredytowej.

Opis wydarzeń:

1)Irlandzki organ nadzorczy zdecydował o dokonaniu czynności kontrolnych w Banku celem rozpatrzenia otrzymanych zgłoszeń.

2) W trakcie czynności kontrolnych irlandzki organ nadzorczy ustalił, iż:

a) liczba osób objęta naruszeniem była różna i wahała się od 1 do 47 000 osób w zależności od naruszenia,

b) dane osobowe, których dotyczyły naruszenia, obejmowały wrażliwe finansowe i gospodarcze dane osobowe, z których miała wynikać zdolność kredytowa osób, których dane dotyczą.

3) Na podstawie zebranego materiału dowodowego irlandzki organ nadzorczy uznał, że Bank:

a) dokonał zgłoszenia naruszeń w terminie późniejszym niż 72 godziny od stwierdzenia naruszenia,

b) nie poinformował bez zbędnej zwłoki osób, których dane dotyczą, o naruszeniu ich danych osobowych,

c) nie dokonał wdrożenia adekwatnych środków technicznych i organizacyjnych zapewniających poziom bezpieczeństwa odpowiedni do ryzyka, jakie stwarza przetwarzanie danych klientów przy przekazywaniu informacji do Centralnego Rejestru Kredytów, takich jak:

- procedury walidacyjne w zakresie weryfikacji poprawności wysyłanych danych,
- szkolenia dla pracowników dotyczące znaczenia komunikacji z osobami, których dane dotyczą, w przypadku, gdy naruszenie danych osobowych może skutkować wysokim ryzykiem naruszenia ich praw i wolności,
- procedura zgłaszania naruszeń oraz informowania osób, które dane dotyczą, o naruszeniu ich danych osobowych.

Przyczyna naruszenia:

Bank nie dopełnił obowiązku wdrożenia odpowiednich środków technicznych i organizacyjnych w celu zapewnienia poziomu ochrony odpowiedniego do ryzyka, jakie stwarza przetwarzanie danych klientów przy przekazywaniu informacji do Centralnego Rejestru Kredytów.

Decyzja:

1) Kara pieniężna w wysokości 463 000 EUR.

2) Nakaz wdrożenia adekwatnych środków technicznych i organizacyjnych zapewniających poziom bezpieczeństwa odpowiedni do zagrożeń takich, jak:

a) aktualizacja procedur walidacyjnych w zakresie weryfikacji poprawności danych przed wysłaniem ich do Centralnego Rejestru Kredytów,

b) przeprowadzenie odpowiednich szkoleń dla pracowników dotyczących znaczenia komunikacji z osobami, których dane dotyczą, w przypadku, gdy naruszenie danych osobowych może skutkować wysokim ryzykiem naruszenia ich praw i wolności,

c) procedura zgłaszania naruszeń oraz informowania osób, które dane dotyczą, o naruszeniu ich danych osobowych.

Źródło:

https://dataprotection.ie/sites/default/files/uploads/2022-04/Final%20Decision%20in%20Inquiry%20IN-19-9-5%20%2831.03.2022%29.pdf

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) Wykonuj cyklicznie analizę ryzyka dla systemów informatycznych i aplikacji, w których przetwarzasz dane osobowe.

3) Dokonuj regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzanych danych osobowych w systemach teleinformatycznych.

4) Opracuj i wdróż procedurę zgłoszenia naruszenia ochrony danych oraz informowania osób, które dane dotyczą, o naruszeniu ich danych osobowych.

Materiał edukacyjny przygotowany przez FORSAFE

Opracowanie merytoryczne
Katarzyna Cieślak