Kary organów nadzorczych w Unii Europejskiej

Kraj oraz organ nadzorczy

Holandia

Dutch Supervisory Authority for Data Protection (AP)

Data wydania decyzji

19 stycznia 2023 r.

Podmiot kontrolowany

Dutch Social Insurance Institution (SVB)

Wysokość kary

150 000 EUR

FORSAFE
BEZPIECZEŃSTWO PONAD WSZYSTKO

Rodzaj naruszenia

Art. 32 (1), (2) RODO.
Niewystarczające środki techniczne i organizacyjne zapewniające bezpieczeństwo informacji.

Przedmiot decyzji

Źródło postępowania:

Holenderski organ nadzorczy otrzymał skargę na Dutch Social Insurance Institution (SVB) odnoszącą się do udostępnienia członkowi rodziny danych osobowych Skarżącej bez jej zgody. Jednocześnie tego samego dnia SVB dokonało zgłoszenia naruszenia ochrony danych osobowych, które dotyczyło telefonicznego udostępnienia danych osobowych nieupoważnionemu odbiorcy.

Opis wydarzeń:

1) Holenderski organ nadzorczy zdecydował o dokonaniu czynności kontrolnych w SVB celem rozpatrzenia przedmiotowej sprawy.

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

a) w strukturze organizacyjnej SVB znajduje się dział odpowiedzialny za telefoniczny kontakt z osobami dzwoniącymi z pytaniami dotyczącymi ubezpieczeń społecznych,

b) wszyscy pracownicy powyższego działu (1500 osób) posiadają dostęp do różnych systemów, w których znajdują się następujące dane osobowe: imię i nazwisko, dane adresowe, adres e-mail, obywatelstwo, zezwolenie na pobyt, sytuacja życiowa, stan cywilny, kwota świadczenia, dane pracodawcy, numer identyfikacji podatkowej, dochód, numer rachunku bankowego, numer BSN, informacje o stanie zdrowia, informacje o wyrokach skazujących i czynach zabronionych związanych z ubezpieczeniami społecznymi,

c) zgodnie z przyjętymi instrukcjami pracownicy SVB mogli udostępniać dane osobowe po zadaniu kilku pytań weryfikujących pozwalających na ustalenie tożsamości dzwoniącego,

d) powyższe instrukcje różniły się między sobą oraz były niejasne w wielu aspektach, co powodowało niepewność pracowników co do ich stosowania a w konsekwencji do ich nieprzestrzegania,

e) SVB nie posiadał analizy ryzyka uwzględniającej nieuprawniony dostęp do danych podczas rozmowy telefonicznej.

3) SVB w związku z powyższym zdarzeniem podjął decyzję o wdrożeniu dodatkowych środków technicznych i organizacyjnych mających na celu zmniejszenie ryzyka zaistnienia identycznej sytuacji w przyszłości.

4) Na podstawie zebranego materiału dowodowego holenderski organ nadzorczy uznał, że SVB nie wdrożyło adekwatnych środków technicznych i organizacyjnych w celu zagwarantowania poziomu bezpieczeństwa dostosowanego do ryzyka w zakresie przetwarzania danych osobowych w kontekście telefonicznego kontaktu klienta z infolinią.

Przyczyna naruszenia:

Pracownicy SVB udostępnili dane osobowe nieuprawnionej osobie.

Decyzja:

Kara pieniężna w wysokości 150 000 EUR.

Źródło:

https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boetebesluit_sociale_verzekeringsbank.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 uwzględniając w niej incydenty i naruszenia, jakie miały miejsce w podmiocie.

3) Opracuj procedurę identyfikacji swoich klientów tak, aby była ona skuteczna i dawała gwarancję weryfikacji ich tożsamości.

Materiał edukacyjny przygotowany przez FORSAFE

Opracowanie merytoryczne
Katarzyna Kawczyńska