KOMPAS FORSAFE 2021/72

Kary organów nadzorczych w Unii Europejskiej

Kraj oraz organ nadzorczy

Włochy

Italian Data Protection Authority (Garante)

Data wydania decyzji

13.07.2020

Podmiot kontrolowany

Iliad Italia S.p.A.

Wysokość kary

800 000 EUR

FORSAFE
BEZPIECZEŃSTWO PONAD WSZYSTKO

Rodzaj naruszenia

Naruszenie art. 5, art. 25 RODO.
Nieprzestrzeganie ogólnych zasad przetwarzania danych.

Przedmiot decyzji

Źródło postępowania:

Włoski organ nadzorczy otrzymał skargi na Iliad Italia S.p.A. (Iliad) dotyczące przetwarzania danych klientów w celu aktywacji kart SIM i związanego z tym sposobu pozyskiwania danych płatniczych, przetwarzania danych do celów promocyjnych oraz środków przyjętych do przechowywania danych w obszarze obsługi klientów.

Opis wydarzeń:

1) Włoski organ nadzorczy zdecydował o dokonaniu czynności kontrolnych w Iliad celem rozpatrzenia przedmiotowej sprawy.

2) Na podstawie zebranego materiału dowodowego włoski organ nadzorczy ustalił, iż:

a) Iliad pobierał zgodę na przetwarzanie danych w celach promocyjnych, ale de facto nie prowadził działań w zakresie marketingu bezpośredniego,
b) klienci Iliad aktywujący kartę SIM za pomocą Simboxa narażeni byli na utratę poufności swoich danych osobowych,
c) pracownik obsługi klienta o profilu administratora miał dostęp do danych około 3 milionów użytkowników w zakresie ich ruchu telefonicznego, generowanego z okresu ponad sześciu miesięcy,
d) Iliad nie dopełniła wymogu przechowywania różnych rodzajów danych w odrębnych systemach informatycznych.

Przyczyna naruszenia:

Administrator nie dopełnił obowiązku realizacji podstawowych zasad ochrony danych osobowych.

Decyzja Italian Data Protection Authority (Garante):

Kara pieniężna w wysokości 800 000 EUR.

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) Dokonaj wdrożenia mechanizmu dwuetapowego uwierzytelniania do aplikacji i programów dostępnych z poziomu Internetu, w których przetwarzane są dane osobowe.

3) Nadając uprawnienia dostępu do danych osobowych w systemie informatycznym pamiętaj, aby były one skorelowane z zakresem obowiązków przypisanym do danego stanowiska.

Materiał edukacyjny przygotowany przez FORSAFE

Opracowanie merytoryczne
Katarzyna Cieślak