Kary organów nadzorczych w Unii Europejskiej

Kraj oraz organ nadzorczy
Włochy
Italian Data Protection Authority (Garante)

Data wydania decyzji
15 grudzień 2022 r.

Podmiot kontrolowany
Eurosanità S.P.A.

Wysokość kary
120 000 EUR

FORSAFE
BEZPIECZEŃSTWO PONAD WSZYSTKO

Rodzaj naruszenia

Art. 5 RODO, Art. 9 RODO, Art. 32 RODO.
Niewystarczające środki techniczne i organizacyjne zapewniające bezpieczeństwo informacji.

Przedmiot decyzji

Źródło postępowania:

Włoski organ nadzorczy otrzymał skargę na Eurosanità S.P.A. (Eurosanità), odnoszącą się do omyłkowego otrzymania dokumentu zawierającego dokumentację medyczną innej osoby.

Opis wydarzeń:

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

2) Eurosanità po powzięciu informacji o omyłkowo wysłanej dokumentacji medycznej, dokonała zgłoszenia naruszenia ochrony danych osobowych, w którym poinformowano, iż naruszenie:

a) było następstwem błędu personelu medycznego,

b) wystąpiło na skutek wpisania danych z wizyty przyjętego pacjenta na oddział SOR do karty medycznej innego pacjenta o tym samym imieniu i nazwisku,

c) dotyczyło jednego pacjenta,
d) obejmowało dane osobowe zawarte w dokumentacji medycznej SOR, m.in. szczegółowe raporty, badania i konsultacje kardiologiczne.

3) Eurosanità po zaistniałej sytuacji podjęła decyzję o wdrożeniu dodatkowych środków technicznych i organizacyjnych mających na celu zmniejszenie ryzyka popełnienia podobnego błędu w przyszłości.

4) Na podstawie zebranego materiału dowodowego włoski organ nadzorczy uznał, że Eurosanità nie wdrożyła adekwatnych środków technicznych i organizacyjnych.

Przyczyna naruszenia:

Błędne sporządzenie dokumentacji medycznej SOR a następnie wysłanie jej do osoby o takim samym imieniu i nazwisku jak przyjęty pacjent.

Decyzja:

Kara pieniężna w wysokości 120 000 EUR.

Źródło:

https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9870788

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.

Materiał edukacyjny przygotowany przez FORSAFE

Opracowanie merytoryczne
Katarzyna Kawczyńska