KOMPAS FORSAFE 2022/50

Kary organów nadzorczych w Unii Europejskiej

Kraj oraz organ nadzorczy **Holandia**
Dutch Supervisory Authority for Data Protection

Data wydania decyzji **11 lutego 2021 r.**

Podmiot kontrolowany **OLVG**

Wysokość kary **440 000 EUR**

FORSAFE
BEZPIECZEŃSTWO PONAD WSZYSTKO

Rodzaj naruszenia

Naruszenie art. 32 RODO.
Niewystarczające środki techniczne i organizacyjne zapewniające bezpieczeństwo informacji.

Przedmiot decyzji

Źródło postępowania:

OLVG (szpital kliniczny w Amsterdamie) dokonał zgłoszenia do holenderskiego organu nadzorczego 2 naruszeń ochrony danych osobowych, które polegały na dostępie pracowników i pracujących studentów do elektronicznych teczek pacjentów.

Opis wydarzeń:

1) W związku z otrzymanymi zgłoszeniami holenderski organ nadzorczy zdecydował o dokonaniu czynności kontrolnych w OLVG.

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

a) nie podjął wystarczających środków w latach 2018-2020, aby uniemożliwić dostęp nieuprawnionych pracowników do dokumentacji medycznej,

b) nie wprowadził dwuskładnikowego uwierzytelniania do systemu informatycznego zawierającego dokumentację medyczną,

c) nie sprawdził należycie, kto miał dostęp do jakiego pliku,

d) nie zapewnił, aby system komputerowy posiadał wystarczające zabezpieczenia.

3) Ostatecznie holenderski organ nadzorczy uznał, iż OLVG nie zastosował odpowiedniego poziomu bezpieczeństwa przetwarzania danych osobowych w szpitalnym systemie informatycznym.

Przyczyna naruszenia:

OLVG nie spełniło wymogu uwierzytelniania dwuskładnikowego i regularnej oceny plików dziennika.

Decyzja Dutch Supervisory Authority for Data Protection (AP):

1) Kara pieniężna w wysokości 440 000 EU.

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) Wykonaj wdrożenie procedur i systemu powiadamiania o zdarzeniach niepożądanych, w tym monitorowanie ruchu sieciowego.

3) Stosuj wieloskładnikowe uwierzytelnianie.

Materiał edukacyjny przygotowany przez FORSAFE

Opracowanie merytoryczne
Katarzyna Cieślak