Kary organów nadzorczych w Unii Europejskiej

Kraj oraz organ nadzorczy
Szwecja
Data Protection Authority of Sweden (Datainspektionen)

Data wydania decyzji
03.12.2020 r.

Podmiot kontrolowany
Aleris Närsjukvård AB

Wysokość kary
1 168 000 EUR

FORSAFE
BEZPIECZEŃSTWO PONAD WSZYSTKO

Rodzaj naruszenia

Naruszenie Art. 5 (1) f), Art. 5 (2), Art. 32 (1), Art. 32 (2) RODO
Niewystarczające środki techniczne i organizacyjne zapewniające bezpieczeństwo informacji.

Przedmiot decyzji

Źródło postępowania:

Szwedzki organ nadzorczy 24 kwietnia 2019 r. dokonał czynności kontrolnych w Aleris Närsjukvård AB.

Opis wydarzeń:

1) Szwedzki organ nadzorczy podczas czynności kontrolnych ustalił, iż Aleris nie przeprowadził analizy potrzeb i ryzyka przed przydzieleniem uprawnień w systemach dokumentacji medycznej National Patient Overview (NPÖ) i TakeCare zgodnie z obowiązującymi przepisami prawa w sektorze medycznym.

2) Zweryfikował również, że Aleris nie ograniczał uprawnień użytkowników w zakresie dostępu do wyżej wskazanych systemów dokumentacji medycznej do tego, co jest niezbędne.

3) Oceniono, że Aleris nie podjął odpowiednich środków technicznych i organizacyjnych, aby móc zapewnić i wykazać, że przetwarzanie danych osobowych jest zabezpieczone adekwatnie do zagrożeń.

4) Na dzień kontroli liczba zarejestrowanych pacjentów w TakeCare z Aleris wyniosła 55 061.

5) Liczba pracowników Aleris w momencie kontroli wynosiła 1150 pracowników miesięcznie. Liczba menedżerów, którzy mają dostęp do TakeCare wyniosła 1700.

6) Liczba pracowników mających dostęp do National Patient Overview (NPÖ) w momencie kontroli wynosiła 335 i składa się głównie z lekarzy (158 lekarzy, 87 pielęgniarek, 82 fizjoterapeutów, 4 terapeutów zajęciowych, 3 sekretarek medycznych i 1 kręgarz).

Przyczyna naruszenia:

Aleris Sjukvård AB nie przeprowadził analizy potrzeb i ryzyka przed przydzieleniem uprawnień w systemie dokumentacji medycznej TakeCare oraz National Patient Overview (NPÖ) oraz nadawał użytkownikom zbyt szerokie uprawnienia do danych w systemach dokumentacji medycznej.

Decyzja Italian Data Protection Authority (Garante):

1) Kara pieniężna w wysokości 12 000 000 SEK (ok. 1 168 000 EUR).

Kompas FORSAFE

JAK UNIKAĆ PODOBNYCH NARUSZEŃ?

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

2) 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.

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

4) Wykonuj cykliczne przeglądy nadanych uprawnień dostępu do danych osobowych w systemach informatycznych.

5) Przechowuj dane osobowe w taki sposób, aby osoby nieuprawnione nie miały do nich dostępu.

Materiał edukacyjny przygotowany przez FORSAFE

Opracowanie merytoryczne
Katarzyna Cieślak