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 Sjukvård AB**

Wysokość kary **1 463 000 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 8 kwietnia 2019 r. dokonał czynności kontrolnych w Aleris Sjukvård AB (Aleris).

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 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 potrzebne tylko, aby użytkownik mógł wykonywać swoje zadania w opiece zdrowotnej zgodnie z obowiązującymi przepisami prawa w sektorze medycznym.

3) Na powyższej podstawie oceniono, że Aleris nie podjął odpowiednich środków technicznych i organizacyjnych, aby móc zapewnić i wykazać, że przetwarzanie danych osobowych jest zabezpieczone odpowiednio do zagrożeń.

4) Na dzień kontroli w systemie TakeCare było 1058 aktywnych użytkowników, 807 aktywnych kont i 63 jednostki.

Przyczyna naruszenia:

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

Decyzja Data Protection Authority of Sweden (Datainspektionen):

1) Kara pieniężna w wysokości 15 000 000 SEK (ok. 1 463 000 EUR).

2) Wykonanie analizy potrzeb i ryzyka dla systemów dokumentacji medycznej TakeCare.

3) Przypisanie każdemu użytkownikowi indywidualnych uprawnień w zakresie dostępu do danych osobowych, które są ograniczone tylko do tego, co jest niezbędne, aby osoba mogła wypełniać swoje obowiązki w opiece zdrowotnej.

Kompas FORSAFE

JAK UNIKAĆ TAKICH 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.

Materiał edukacyjny przygotowany przez FORSAFE

Opracowanie merytoryczne
Katarzyna Cieślak