Kary organów nadzorczych w Unii Europejskiej

Kraj oraz organ nadzorczy

Szwecja

Data Protection Authority of Sweden

Data wydania decyzji

03 grudzień 2020 r.

Podmiot kontrolowany

Karolinska University Hospital of Solna

Wysokość kary

390 100 EUR

FORSAFE
BEZPIECZEŃSTWO PONAD WSZYSTKO

Rodzaj naruszenia

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

Przedmiot decyzji

Źródło postępowania:

Szwedzki organ nadzorczy dokonał czynności kontrolnych w Karolinska University Hospital of Solna (Szpital).

Opis wydarzeń:

1) Szwedzki organ nadzorczy podczas czynności kontrolnych ustalił, iż Szpital nie przeprowadził analizy potrzeb i ryzyka przed przydzieleniem uprawnień w systemach dokumentacji TakeCare, zgodnie z obowiązującymi przepisami prawa w sektorze medycznym. Tym samym, nie wykonał decyzji szwedzkiego organu nadzorczego, jaka była nałożona na Szpital w 2013 r.

2) Szwedzki organ nadzorczy zweryfikował również, że Szpital nie ograniczał uprawnień użytkowników w zakresie dostępu do wyżej wskazanego systemu dokumentacji medycznej, które byłyby ograniczone tylko do tego co jest niezbędne, aby użytkownik mógł wykonywać swoje zadania w opiece zdrowotnej zgodnie z obowiązującymi przepisami prawa w sektorze medycznym.

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

4) Na dzień kontroli w systemie TakeCare było 10 957 aktywnych użytkowników Szpitala oraz około 3 milionów pacjentów, w tym 1 970 000 pacjentów leczonych w Szpitalu.

Przyczyna naruszenia:

Szpital nie przeprowadził analizy potrzeb i ryzyka przed przydzieleniem uprawnień w systemie dokumentacji medycznej TakeCare.

Decyzja:

1) Kara pieniężna w wysokości 4 000 000 SEK (ok. 390 100 EUR).

2) Wykonanie analizy potrzeb i ryzyka dla systemu 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.

Źródło:

https://www.imy.se/globalassets/dokument/beslut/beslut-tillsyn-karolinska-universitetssjukhuset-di-2019-3839.pdf

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) 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