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 **Capio St. Göran AB**

Wysokość kary **2 900 000 EUR**

FORSAFE BEZPIECZEŃSTWO PONAD WSZYSTKO

Rodzaj naruszenia

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

Przedmiot decyzji

Źródło postępowania:

Szwedzki Urząd Ochrony Danych Osobowych w kwietniu 2019 r. dokonał czynności kontrolnych w Capio St. Görans Sjukhus AB (Szpital w Sztokholmie).

Opis wydarzeń:

1) Szwedzki Urząd Ochrony Danych Osobowych podczas czynności kontrolnych ustalił, iż Capio St. Görans Sjukhus AB nie przeprowadził analizy potrzeb i ryzyka przed przydzieleniem uprawnień w systemach dokumentacji medycznej Cambio Cosmic, National Patient Overview i TakeCare, zgodnie z obowiązującymi przepisami prawa w sektorze medycznym w Szwecji.

2) Zweryfikował również, że Szpital nie ograniczał uprawnień użytkowników w zakresie dostępu do wyżej wskazanych systemów dokumentacji medycznej do tego tylko, co jest koniecznie do wykonywania obowiązków pracowniczych. Zatem dostęp do danych był znacznie szerszy.

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

4) Kontrola wykazała, że ponad 2700 pracowników miało dostęp do informacji dotyczących prawie 490 000 pacjentów, a ponad innych 600 pracowników miało dostęp do danych dotyczących około 3 milionów pacjentów znajdujących się w programie TakeCare.

Przyczyna naruszenia:

Capio St. Görans Sjukhus AB nadawał użytkownikom zbyt szerokie uprawnienia do danych w systemach dokumentacji medycznej.

Decyzja Data Protection Authority of Sweden (Datainspektionen):

1) Kara pieniężna w wysokości 30 000 000 SEK (2 900 000 euro).

2) Wykonanie analizy potrzeb i ryzyka dla systemów dokumentacji medycznej Cambio Cosmic, National Patient Overview i 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.

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

Materiał edukacyjny przygotowany przez FORSAFE

Opracowanie merytoryczne
Katarzyna Cieślak