

Kary organów nadzorczych w Unii Europejskiej



Kraj oraz organ nadzorczy

Finlandia

Deputy Data Protection Ombudsman



Data wydania decyzji

7 grudnia 2021 r.



Podmiot kontrolowany

Psykiaterikeskus Vastaamo



Wysokość kary

608 000 EUR








Rodzaj naruszenia

Naruszenie art.5 (1) f), art. 33 (1), art. 34 (1) RODO.
Nieprzestrzeganie ogólnych zasad przetwarzania danych.



Przedmiot decyzji

Źródło postępowania:

Psykiaterikeskus Vastaamo (Vastaamo) dokonał zgłoszenia do fińskiego organu nadzorczego naruszenia ochrony danych osobowych, które polegało na pozyskaniu przez hakera bazy danych pacjentów.

Opis wydarzeń:

1)

Fiński organ nadzorczy zdecydował o dokonaniu czynności kontrolnych w Vastaamo celem rozpatrzenia przedmiotowej sprawy.

2)

W trakcie czynności kontrolnych fiński organ nadzorczy ustalił, iż nieuprawniona osoba uzyskała dostęp do bazy danych pacjentów co najmniej 2 razy – w grudniu 2018 r. i marcu 2019 r.

3)

Po tym zdarzeniu haker umieścił na serwerze informację o skopiowaniu danych oraz żądanie okupu za odzyskanie utraconych danych.

4)

Najprawdopodobniej przyczyną wycieku danych był niezabezpieczony port MySQL w bazie danych, który nie posiadał uwierzytelnienia administratora. Ponadto identyfikator głównej bazy danych pacjentów nie był chroniony hasłem, a nazwie użytkownika przyznano prawo do logowania się do bazy danych pacjentów z dowolnego adresu IP. Co więcej w okresie od 26 listopada 2017 r. do 13 marca 2019 r. serwer bazy danych pacjentów był otwarty na Internet bez ochrony firewall.

5)

Analiza powłamaniami wykazała również brak oddzielnego środowiska deweloperskiego, testowego i produkcyjnego do tworzenia aplikacji, brak aktualizacji systemu, brak zainstalowanego oprogramowania antywirusowego, brak wykonywania testów podatności oraz brak zewnętrznych audytów bezpieczeństwa.

6)

W wyniku ataku hakerskiego wykradziono dane osobowe najprawdopodobniej ok 69 tys. osób.

7)

Wykradzione dane obejmowały informacje o dzieciach, osobach starszych oraz osobach z problemami zdrowia psychicznego, w tym dane osobowe szczególnej kategorii.

8)

W wyniku tego zdarzenia w sieci TOR został umieszczony plik zawierający bazę danych pacjentów Vastaamo a co najmniej 15 tys. osób otrzymało groźbę ujawnienia informacji o nich w przypadku braku zapłaty od 200 do 500 EUR.

9)

Na podstawie zebranego materiału dowodowego fiński organ nadzorczy dopatrył się następujących naruszeń:

a)

Vastaamo przeprowadził ocenę skutków, która nie spełniała wymogów art. 35 ust. 7 RODO,

b)

Vastaamo nie wdrożył podstawowych środków bezpiecznego przetwarzania danych osobowych,

c)

Vastaamo nie zabezpieczył danych osobowych przed nieuprawnionym i niezgodnym z prawem przetwarzaniem lub przypadkową utratą, zniszczeniem lub uszkodzeniem,

d)

Vastaamo nie dokonał zgłoszenia naruszenia ochrony danych oraz nie poinformował pacjentów o tym zdarzeniu w marcu 2019 r. uznając, że istnieje małe prawdopodobieństwo naruszenia praw i wolności osób fizycznych.

Przyczyna naruszenia:

Vastaamo nie wdrożył adekwatnych środków technicznych i organizacyjnych w wyniku czego doszło do ataku hakerskiego i kradzieży bazy danych.

Decyzja Deputy Data Protection Ombudsman:

1)

Kara pieniężna w wysokości 608 000 EUR, w tym:

a)

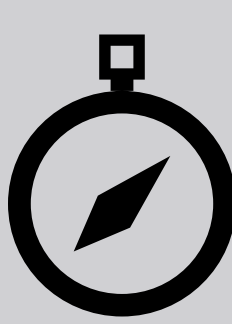
145 600 EUR za naruszenie art. 33 ust. 1 RODO,

b)

145 600 EUR za naruszenie art. 34 ust. 1 RODO,

c)

316 800 EUR za naruszenie art. 5 ust. 1 lit. f) RODO.



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)

Dokonuj weryfikacji doboru, jak i poziomu skuteczności stosowanych środków technicznych na każdym etapie przetwarzania oraz oceniaj weryfikację przez pryzmat adekwatności do ryzyka oraz proporcjonalności w stosunku do stanu wiedzy technicznej, kosztów wdrażania oraz charakteru, zakresu, kontekstu i celów przetwarzania.

3)

Wykonuj regularne testowanie, mierzenie i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania danych osobowych.

4)

Wykonuj testy podatności systemów informatycznych i aplikacji.

5)

Zweryfikuj, czy posiadasz wdrożone środki bezpieczeństwa, jakie zostały wskazane w decyzji fińskiego organu nadzorczego:

a)

stosowanie zapory ogniowej,

b)

stosowanie dla administratorów osobistych identyfikatorów z silnymi hasłami,

c)

stosowanie VPN,

d)

przechowywanie logów serwera na oddzielnym serwerze przez co najmniej rok,

e)

regularne aktualizowanie oprogramowania,

f)

monitorowanie zdarzeń związanych z bezpieczeństwem danych.

Materiał edukacyjny
przygotowany przez FORSAFE





Opracowanie merytoryczne
Katarzyna Cieślak

