Kary organów nadzorczych w Unii Europejskiej

Kraj oraz organ nadzorczy
Irlandia
Data Protection Authority of Ireland

Data wydania decyzji
23 styczeń 2023 r.

Podmiot kontrolowany
Centric Health Ltd.

Wysokość kary
460 000 EUR

FORSAFE
BEZPIECZEŃSTWO PONAD WSZYSTKO

Rodzaj naruszenia

Art. 5 (1) f) RODO, Art. 5 (2) RODO, Art. 32 (1) RODO, Art. 32 (2) RODO.
Nieprzestrzeganie ogólnych zasad przetwarzania danych.

Przedmiot decyzji

Źródło postępowania:

Centric Health Ltd. (Centric) dokonał zgłoszenia do irlandzkiego organu nadzorczego naruszenia ochrony danych osobowych. Naruszenie dotyczyło ataku ransomware w wyniku, którego nastąpił nieautoryzowany dostęp do danych osobowych pacjentów.

Opis wydarzeń:

1) Irlandzki organ nadzorczy zdecydował o dokonaniu czynności kontrolnych w Centric celem rozpatrzenia przedmiotowej sprawy.

2) Centric w wysłanym zgłoszeniu poinformował, iż nieuprawniona osoba uzyskała dostęp do bazy danych pacjentów, zaszyfrowała ją oraz zażądała zapłaty za kod deszyfrujący.

3) Centric poinformował pacjentów o naruszeniu ochrony ich danych osobowych oraz umieścił komunikaty w placówkach medycznych.

4) Centric zdecydował się również na zakup kodu deszyfrującego, ale nie mógł z niego skorzystać w stosunku do danych, które zostały usunięte.

5) Naruszenie obejmowało dane osobowe 70 000 pacjentów w zakresie – imię i nazwisko, data urodzenia, numer PPSN, dane kontaktowe, informacje o stanie zdrowia.

6) Ponadto w wyniku naruszenia dane osobowe 2 500 pacjentów zostały usunięte.

7) W trakcie czynności kontrolnych irlandzki organ nadzorczy ustalił, iż:

a) zapora sieciowa była źle skonfigurowana,

b) hasła administratorów nie spełniały standardów bezpieczeństwa haseł dla usług internetowych,

c) aktualizacja oprogramowania nie była systematycznie wgrywana,

d) dane osobowe pacjentów znajdujące się w bazie danych nie były szyfrowane,

e) kopie zapasowe były przechowywane niezgodnie z zasadami bezpieczeństwa,

f) kopie zapasowe nie były testowane pod kątem możliwości ich odtworzenia,

g) Centric nie posiadał funkcjonującego planu ciągłości działania.

Przyczyna naruszenia:

Centric nie wdrożył adekwatnych środków technicznych i organizacyjnych, które zapewniałyby ochronę danych osobowych pacjentów.

Decyzja:

1) Kara pieniężna w wysokości 460 000 EUR, w tym:

a) 275 000 EUR za naruszenie zasady integralności i poufności,

b) 50 000 EUR za naruszenie zasady rozliczalności,

c) 135 000 EUR za brak wdrożenia adekwatnych środków technicznych i organizacyjnych.

Źródło:

https://www.dataprotection.ie/sites/default/files/uploads/2023-02/IN-21-2-4%20Final%20Decision_Redacted.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) Dokonuj regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzanych danych osobowych w systemach teleinformatycznych.

4) Aktualizuj oprogramowanie – zarówno system operacyjny, programy i aplikacje, z których korzystasz oraz oprogramowanie antywirusowe.

5) Realizuj cykliczne szkolenia z zakresu ochrony danych osobowych oraz cyberbezpieczeństwa.

Materiał edukacyjny przygotowany przez FORSAFE

Opracowanie merytoryczne
Katarzyna Kawczyńska