Kary organów nadzorczych w Unii Europejskiej

Kraj oraz organ nadzorczy

Irlandia

Data Protection Authority of Ireland

Data wydania decyzji

22 grudzień 2022 r.

Podmiot kontrolowany

VIEC Limited

Wysokość kary

100 000 EUR

FORSAFE
BEZPIECZEŃSTWO PONAD WSZYSTKO

Rodzaj naruszenia

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

Przedmiot decyzji

Źródło postępowania:

VIEC Limited (VIEC) dokonał zgłoszenia do irlandzkiego organu nadzorczego odnośnie naruszenia ochrony danych osobowych, które polegało na nieautoryzowanym dostępie do poczty elektronicznej jednego z menadżerów.

Opis wydarzeń:

1) W związku z otrzymanym zgłoszeniem, irlandzki organ nadzorczy zdecydował o dokonaniu czynności kontrolnych w VIEC.

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

a) naruszenie było wynikiem ataku phishingowego na adres e-mail jednego z menadżerów domu opieki zdrowotnej VIEC,

b) najbardziej prawdopodobną przyczyną naruszenia było przechwycenie danych uwierzytelniających do konta użytkownika na fałszywej stronie internetowej,

c) w związku z tym zdarzeniem wiadomości e-mail zostały przekierowane na inne konto,

d) naruszeniem zostały objęte następujące dane osobowe – imię i nazwisko, adres zamieszkania, adres e-mail, numer telefonu, PPSN, dane dotyczące zdrowia, dane biometryczne, grafiki pracowników,

e) naruszenie dotyczyło 213 osób. W tym w przypadku 117 podopiecznych dotyczyło to danych o zdrowiu, a w przypadku 12 podopiecznych dotyczyło to danych biometrycznych,

f) VIEC poinformował pracowników oraz podopiecznych o naruszeniu ich danych osobowych.

3) Na podstawie zebranego materiału dowodowego irlandzki organ nadzorczy dopatrzył się następujących uchybień:

a) wysyłanie wiadomości e-mail zawierających dane osobowe bez szyfrowania,

b) pracownicy nie byli szkoleni pod kątem potencjalnego phishingu,

c) brak wdrożenia uwierzytelniania wieloskładnikowego dla użytkowników logujących się na konta e-mail,

d) brak ustawienia daty wygaśnięcia haseł do kont e-mail użytkowników,

e) brak regularnego testowania skuteczności środków technicznych i organizacyjnych.

Przyczyna naruszenia:

VIEC nie dopełnił obowiązku wdrożenia odpowiednich środków technicznych i organizacyjnych w celu zapewnienia poziomu ochrony odpowiedniego do ryzyka.

Decyzja:

1) Kara pieniężna w wysokości 100 000 EUR.

2) Nakaz zapewnienia zgodności przetwarzania w terminie 90 dni od dnia doręczenia decyzji poprzez wdrożenie monitorowania pracowników pod kątem wykorzystywania szyfrowania podczas wysyłania e-mailem dokumentów zawierających dane osobowe.

Źródło:

https://www.dataprotection.ie/sites/default/files/uploads/2023-01/Final%20Decision%20VIEC%20IN-21-2-5%20121222_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) Monitoruj pracowników pod kątem wykorzystywania szyfrowania podczas wysyłania e-mailem dokumentów zawierających dane osobowe.

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

Materiał edukacyjny przygotowany przez FORSAFE

Opracowanie merytoryczne
Katarzyna Kawczyńska