Kary organów nadzorczych w Unii Europejskiej

Kraj oraz organ nadzorczy
Islandia
Icelandic data protection authority ('Persónuvernd')

Data wydania decyzji
3 lipca 2023 r.

Podmiot kontrolowany
Heilsuveru

Wysokość kary
81 000 EUR

FORSAFE
BEZPIECZEŃSTWO PONAD WSZYSTKO

Rodzaj naruszenia

Art. 5 (1) f), Art. 25, Art. 32 (1) b), d) RODO
Niewystarczające środki techniczne i organizacyjne zapewniające bezpieczeństwo informacji.

Przedmiot decyzji

Źródło postępowania:

W czerwcu 2020 r. do islandzkiego organu nadzorczego wpłynęło zgłoszenie naruszenia ochrony danych osobowych od Heilsuveru polegające na dostępie dwóch użytkowników serwisu do informacji o innych użytkownikach.

Opis wydarzeń:

1. Islandzki organ nadzorczy zdecydował o dokonaniu czynności kontrolnych w Heilsuveru celem rozpatrzenia przedmiotowej sprawy oraz poprosił o złożenie dodatkowych wyjaśnień.

2. W trakcie czynności kontrolnych islandzki organ nadzorczy ustalił, iż:

a) Heilsuveru jest podmiotem medycznym, który udostępnił swoim pacjentom serwis, w którym mogli się oni komunikować z lekarzem oraz uzyskać swoje wyniki badań,

b) do naruszenia doszło na skutek luki w zabezpieczeniu strony internetowej,

c) naruszenie zostało zgłoszone przez 2 osoby, które odkryły, że zmiana liczby w adresie URL powoduje przekierowanie na konto innego użytkownika,

d) w wyniku zaistniałej sytuacji można było pobrać 205 407 załączników, z których część zawierała informacje o stanie zdrowia 41 390 osób,

e) Heilsuveru niezwłocznie zareagował na zgłoszoną podatność i wyeliminował ją w ciągu kilku godzin.

3. Islandzki organ nadzorczy uznał, że Heilsuveru nie wdrożył adekwatnych środków technicznych co skutkowało nałożeniem na niego kary administracyjnej.

Przyczyna naruszenia:

Heilsuveru udostępnił swoim pacjentom stronę zawierającą lukę w zabezpieczeniu skutkującą dostępem osób nieuprawnionych do danych osobowych innych osób.

Decyzja:

1. Kara pieniężna w wysokości 81 000 EUR.

Źródło:

https://www.personuvernd.is/urlausnir/sekt-vegna-oryggisveikleika-i-heilsuveru#

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 regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania danych osobowych w systemach teleinformatycznych.

3. Jeśli udostępniasz swoim klientom usługę poprzez stronę internetową pamiętaj, aby:

a) zadbać o prawidłową konfigurację serwera oraz usług wystawianych do Internetu,

b) stosować funkcje filtrujące zapytania do bazy danych oraz walidację i kodowanie adresu URL,

c) stosować szyfrowanie adresu URL,

d) stosować odpowiednie i kontrolowane uprawnienia dostępu do katalogów oraz plików na serwerze.

Materiał edukacyjny przygotowany przez FORSAFE

Opracowanie merytoryczne
Katarzyna Kawczyńska