Kary organów nadzorczych w Unii Europejskiej

Kraj oraz organ nadzorczy
Litwa
Lithuanian Data Protection Authority (VDAI)

Data wydania decyzji
20 kwietnia 2023

Podmiot kontrolowany
Przedsiębiorstwo

Wysokość kary
20 000 EUR

FORSAFE
BEZPIECZEŃSTWO PONAD WSZYSTKO

Rodzaj naruszenia

Art. 5 (1) e), f), art. 32 (1) b), d) RODO.
Nieprzestrzeganie ogólnych zasad przetwarzania danych.

Przedmiot decyzji

Źródło postępowania:

Do litewskiego organu nadzorczego wpłynęło zgłoszenie naruszenia bezpieczeństwa danych osobowych polegające na nieautoryzowanym dostępie do bazy danych.

Opis wydarzeń:

1. Przedsiębiorstwo w wysłanym zgłoszeniu poinformowało, iż naruszenie:

a) dotyczyło około 50 000 osób (klienci),

b) obejmowało następujące dane osobowe – imię i nazwisko, adres e-mail, adres zamieszkania, numer telefonu, numer rejestracyjny samochodu.

2. Na podstawie zebranego materiału dowodowego litewski organ nadzorczy ustalił, że:

a) nie wdrożono środków zapewniających właściwą kontrolę dostępu i uwierzytelniania administratorów systemów informatycznych oraz innych uprzywilejowanych użytkowników:

- podczas łączenia się z panelem administracyjnym bazy danych systemu informatycznego nie zastosowano ograniczenia dostępu tylko dla osób uprawnionych,

- nie stosowano uwierzytelniania wieloskładnikowego podczas wprowadzania danych logowania użytkownika w panelu administracyjnym bazy danych systemu,

- nie zapewniono dostatecznego poziomu ochrony przed zbieraniem haseł lub innymi podobnymi cyberatakami,

- nie zainstalowano zabezpieczeń przed zgadywaniem hasła,

- nie prowadzono monitoringu działań użytkowników systemu i zapisów dziennika,

b) nie zapewniono właściwego gromadzenia i przechowywania zapisów logów systemów informatycznych,

c) nie przestrzegano terminów przechowywania zapisów logów oraz zaleceń dotyczących monitoringu,

d) naruszano zasadę ograniczenia przechowywania, gdyż dane osobowe klientów były przechowywane przez 5 lat.

Przyczyna naruszenia:

Przedsiębiorstwo nie dokonało adekwatnego doboru zabezpieczeń systemu informatycznego wykorzystywanego do przetwarzania danych osobowych.

Decyzja:

Kara pieniężna w wysokości 20 000 EUR.

Źródło:

https://vdai.lrv.lt/uploads/vdai/documents/files/Apibendrinimas%20dėl%20saugumo%20priemoniu%20neuztikrinimo%20ir%20terminu%202023-04-20.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. Dokonuj regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania danych osobowych w systemach teleinformatycznych.

3. Wdróż procedury retencji danych oraz regularnie weryfikuj czas przetwarzania danych osobowych.

Materiał edukacyjny przygotowany przez FORSAFE

Opracowanie merytoryczne
Katarzyna Kawczyńska