Kary organów nadzorczych w Unii Europejskiej

Kraj oraz organ nadzorczy

Norwegia

Norwegian Supervisory Authority

Data wydania decyzji

27 listopada 2023 r.

Podmiot kontrolowany

Norwegian Labor and Welfare Administration

Wysokość kary

1 700 000 EUR

FORSAFE
BEZPIECZEŃSTWO PONAD WSZYSTKO

Rodzaj naruszenia

Art. 5 (1) f), art. 5 (2), art. 24 (1), art. 25 (1), art. 32 (1) d), art. 32 (2) RODO.
Niewystarczające środki techniczne i organizacyjne zapewniające bezpieczeństwo informacji.

Przedmiot decyzji

Źródło postępowania:

Norweski organ nadzorczy dokonał czynności kontrolnych w Norwegian Labor and Welfare Administration (Urząd).

Opis wydarzeń:

1. Przedmiotem przeprowadzonej kontroli było sprawdzenie stosowania zasad zachowania poufności danych osobowych w systemach informatycznych, uwzględniając przyjęte środki techniczne i organizacyjne.

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

a) Urząd nie wdrożył w wystarczającym stopniu systemu zarządzania zapewniającego przetwarzanie danych osobowych zgodnie z RODO,

b) dokumentacja dotycząca zarządzania dostępem nie zapewniała odpowiedniej ochrony danych osobowych oraz nie była regularnie poddawana audytowi,

c) Urząd nie przeprowadzał ocen ryzyka podczas tworzenia i rozwijania programów,

d) w jednym z programów dostępność metadanych o dokumentach była zbyt ogólna i szeroka,

e) Urząd nie realizował szkoleń dla administratorów programów,

f) procedury przyznawania dostępu były przestarzałe i nie zawierały wskazówek dotyczących ocen w zakresie nadawania dostępu dla użytkowników,

g) ujawnienie danych osobowych przetwarzanych wyłącznie w celach archiwalnych było zbyt ogólne i szerokie,

h) część pracowników Urzędu miała zbyt szeroki dostęp do danych w niektórych programach,

i) Urząd nie dostosowywał środków bezpieczeństwa do ryzyka przetwarzania danych osobowych,

j) Urząd nie ustanowił procedur corocznego audytu dostępu dla kierowników jednostek,

k) Urząd nie przeprowadzał systematycznej kontroli logów.

3. Na podstawie zebranego materiału dowodowego, norweski organ nadzorczy uznał, że Urząd nie ustanowił w wystarczającym stopniu odpowiednich środków technicznych i organizacyjnych, aby zapewnić i wykazać zgodność z RODO.

Przyczyna naruszenia:

Urząd nie dopełnił obowiązku wdrożenia adekwatnych środków technicznych i organizacyjnych w celu ochrony danych osobowych.

Decyzja:

1. Kara pieniężna w wysokości 1 700 000 EUR.

Źródło:

https://www.datatilsynet.no/contentassets/470d824962e949ccacdf776d425bc27d/endelig-tilsynsrapport.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. Nadając uprawnienia dostępu do danych osobowych w systemie informatycznym pamiętaj, aby były one skorelowane z zakresem obowiązków przypisanym do danego stanowiska.

3. Wykonuj cykliczne przeglądy nadanych uprawnień dostępu do danych osobowych w systemach informatycznych.

4. Realizuj cykliczne szkolenia dla pracowników oraz administratorów systemu w zakresie przyjętych procedur bezpieczeństwa danych osobowych

Materiał edukacyjny przygotowany przez FORSAFE

Opracowanie merytoryczne
Katarzyna Kawczyńska