Kary organów nadzorczych w Unii Europejskiej

Kraj oraz organ nadzorczy — **Holandia**
Dutch Supervisory Authority for Data Protection (AP)

Data wydania decyzji — **31 maj 2021 r.**

Podmiot kontrolowany — **UWV**

Wysokość kary — **450 000 EUR**

FORSAFE
BEZPIECZEŃSTWO PONAD WSZYSTKO

Rodzaj naruszenia

Art. 32 RODO
Niewystarczające środki techniczne i organizacyjne zapewniające bezpieczeństwo informacji

Przedmiot decyzji

Źródło postępowania:
Holenderski organ nadzorczy dokonał czynności kontrolnych w UWV.

Opis wydarzeń:

1) UWV będąc Agencją Ubezpieczeń Pracowniczych, zarządza stroną werk.nl, która służy do obsługi i komunikacji z osobami poszukującymi pracy.

2) Od 2016 r. w UWV miało miejsce dziewięć naruszeń ochrony danych osobowych, które polegały na wysłaniu wiadomości grupowych poprzez powyższą aplikację do grupy osób poszukujących pracy. Wiadomości te zawierały plik z danymi osobowymi różnej liczby osób poszukujących pracy.

3) W pliku najczęściej znajdowały się takie dane osobowe jak: imię i nazwisko, adres, wykształcenie, narodowość, numer BSN, informacje o stanie zdrowia, informacje o zdolności do pracy.

4) Ilość osób, których dotyczyło pojedyncze naruszenie waha się między 10 000 do 11 062 osób.

5) W związku z powyższym holenderski organ nadzorczy uznał, iż UWV nie zagwarantował poziomu bezpieczeństwa dostosowanego do ryzyka w kontekście wysyłania wiadomości grupowych za pośrednictwem aplikacji.

Przyczyna naruszenia:

UWV nie wdrożył odpowiednich środków technicznych i organizacyjnych zapewniających bezpieczeństwo danych osobowych.

Decyzja:

Kara pieniężna w wysokości 450 000 EUR.

Źródło:

https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boete_uwv_beveiliging_groepsberichten.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.

Materiał edukacyjny przygotowany przez FORSAFE

Opracowanie merytoryczne
Katarzyna Cieślak