Kary Prezesa Urzędu Ochrony Danych Osobowych

Data wydania decyzji **19 stycznia 2023 r.**

Podmiot kontrolowany **Sąd Rejonowy Szczecin-Centrum w Szczecinie**

Wysokość kary **30 000 PLN**

FORSAFE
BEZPIECZEŃSTWO PONAD WSZYSTKO

Rodzaj naruszenia

art. 5 ust. 1 lit. f), art. 5 ust. 2, art. 25 ust. 1 i 2, art. 32 ust. 1 i 2 RODO.
Niewystarczające środki techniczne i organizacyjne zapewniające bezpieczeństwo informacji.

Przedmiot decyzji

Źródło postępowania:

We wrześniu 2020 r. do Prezesa Urzędu Ochrony Danych Osobowych (UODO) wpłynęło zgłoszenie naruszenia ochrony danych osobowych od Sądu Rejonowego Szczecin-Centrum w Szczecinie (Sąd). Polegało ono na zagubieniu przez pracownika trzech nośników danych typu pendrive, w tym jednego służbowego zaszyfrowanego oraz dwóch prywatnych nieszyfrowanych.

Opis wydarzeń:

1) Sąd w wysłanym zgłoszeniu oraz jego uzupełnieniu poinformował, iż:

a) naruszenie dotyczyło nieustalonej liczby osób,

b) na zagubionych nośnikach znajdowały się projekty orzeczeń, uzasadnień i zarządzeń w związku z prowadzonymi przez pracownika sprawami z zakresu ubezpieczeń społecznych,

c) zakres naruszenia obejmował następujące dane – imię i nazwisko, adres zamieszkania lub pobytu, dane dotyczące zakładu pracy oraz dane dotyczące zdrowia, zawarte w projektach powyższych dokumentów sporządzanych przez pracownika w okresie od grudnia 2004 r. do sierpnia 2020 r.

2) W trakcie czynności kontrolnych Prezes UODO ustalił, iż Sąd pomimo otrzymanych zaleceń pochodzących z trzech różnych audytów odnoszących się do blokowania użytkowania prywatnych/nieautoryzowanych nośników pamięci, wdrożył wyłącznie środki organizacyjne w postaci zapisów w politykach i regulaminach co bezpośrednio przyczyniło się do zaistnienia naruszenia.

3) Powyższa rekomendacja została wdrożona dopiero w październiku 2020 r., czyli po naruszeniu.

Przyczyna naruszenia:

Sąd nie wdrożył odpowiednich środków technicznych i organizacyjnych zapewniających stopień bezpieczeństwa odpowiadający ryzyku przetwarzania danych przy użyciu przenośnych pamięci.

Decyzja PUODO:

Kara pieniężna w wysokości 30 000 PLN.

Źródło:

https://www.uodo.gov.pl/decyzje/DKN.5131.12.2020

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) W przypadku stosowania przez pracowników przenośnych pamięci rozważ:

a) blokowanie portów USB pod kątem możliwości podłączenia do nich prywatnych urządzeń,

b) wprowadzenie tak zwanej białej listy urządzeń,

c) stosowane jedynie szyfrowanych nośników danych autoryzowanych przez dział IT,

d) cykliczne, przypominające szkolenia ukierunkowane na incydenty bezpieczeństwa związane z utratą nośników danych.

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 Kawczyńska