# Kary i decyzje Prezesa Urzędu Ochrony Danych Osobowych

Data wydania decyzji: **13 lipca 2021 r.**

Podmiot kontrolowany: **Prezes Sądu Rejonowego w Zgierzu**

Wysokość kary: **10 000 PLN**

FORSAFE BEZPIECZEŃSTWO PONAD WSZYSTKO

## Rodzaj naruszenia

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

## Przedmiot decyzji

**Źródło postępowania**:

W lutym 2020 roku do Prezesa Urzędu Ochrony Danych Osobowych (UODO) wpłynęło zgłoszenie naruszenia ochrony danych osobowych z Sądu Rejonowego w Zgierzu, polegające na zagubieniu nieszyfrowanej przenośnej pamięci zewnętrznej typu pendrive przez kuratora sądowego.

**Opis wydarzeń:**

**1)** Naruszenie ochrony danych osobowych dotyczyło 400 osób, które podlegały nadzorowi kuratorskiemu i objęte były wywiadem środowiskowym przez kuratora sądowego.

**2)** Na zagubionym pendrivie znajdowały się dane osobowe obejmujące: imię i nazwisko, datę urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, dane dotyczące zarobków i/lub posiadanego majątku, serię i numer dowodu osobistego, numer telefonu, dane dotyczące zdrowia oraz dane dotyczące wyroków skazujących.

**3)** W związku z powyższą sytuacją Prezes UODO podjął czynności kontrolne i ustalił następujące nieprawidłowości:

**a)** kuratorzy sądowi otrzymali do użytku służbowego niezabezpieczone przenośne pamięci,

**b)** kuratorzy sądowi zostali zobowiązani do wdrożenia we własnym zakresie zabezpieczeń otrzymanej przenośnej pamięci,

**c)** jedynym zabezpieczeniem zastosowanym przez kuratora sądowego było przechowywanie przenośnej pamięci w zamykanej torbie służbowej,

**d)** przedstawiona analiza ryzyka dotycząca możliwości zagubienia sprzętu i nośników została przeprowadzona niewłaściwie z powodu wskazania nieadekwatnych dla osób fizycznych następstw naruszenia ochrony danych osobowych oraz przyjęcia niewłaściwych środków bezpieczeństwa; analizowano wyłącznie środki organizacyjne z całkowitym pominięciem środków technicznych, np. w postaci szyfrowania pamięci przenośnych,

**e)** w przyjętych dokumentach, tj. Polityce Bezpieczeństwa oraz Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych nie wskazano przepisów, zapewniających regularne testowanie, mierzenie i ocenianie skuteczności zastosowanych środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania danych.

**Przyczyna naruszenia**:

Brak zastosowania zabezpieczenia przenośnego nośnika pamięci.

**Decyzja PUODO**:

Kara pieniężna w wysokości 10 000 PLN.

## Kompas FORSAFE

**JAK UNIKAĆ TAKICH NARUSZEŃ?**

**1)** Pamiętaj, że pracownik nie może zastępować administratora danych w realizacji jego zadań wynikających z przepisów o ochronie danych osobowych.

**2)** 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.

**3)** Dokonaj wdrożenia takich środków technicznych i organizacyjnych, które zapewnią bezpieczeństwo przetwarzania danych osobowych i szybką identyfikację naruszeń ochrony danych osobowych.

**4)** Dokonuj weryfikacji doboru, jak i poziomu skuteczności stosowanych środków technicznych na każdym etapie przetwarzania oraz oceny weryfikacji przez pryzmat adekwatności do ryzyk oraz proporcjonalności w stosunku do stanu wiedzy technicznej, kosztów wdrażania oraz charakteru, zakresu, kontekstu i celów przetwarzania.

**5)** Wykonuj udokumentowaną analizę ryzyka uwzględniającą stan faktyczny, charakterystykę zachodzących procesów, aktywa, podatności, zagrożenia oraz istniejące zabezpieczenia, w ramach zachodzących procesów przetwarzania danych osobowych.

Materiał edukacyjny przygotowany przez FORSAFE

Opracowanie merytoryczne
Katarzyna Cieślak