# Kary i decyzje Prezesa Urzędu Ochrony Danych Osobowych

**Data wydania decyzji** — **02 listopad 2022 r.**

**Podmiot kontrolowany** — **Wójt Gminy Dobrzyniewo Duże**

**Wysokość kary** — **8 000 PLN**

FORSAFE BEZPIECZEŃSTWO PONAD WSZYSTKO

## Rodzaj naruszenia

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

## Przedmiot decyzji

**Źródło postępowania**:

W lutym 2022 r. do Prezesa Urzędu Ochrony Danych Osobowych (UODO) wpłynęło zgłoszenie naruszenia ochrony danych osobowych od Wójta Gminy Dobrzyniewo Duże (Wójt), polegające na włamaniu do mieszkania pracownika i kradzieży laptopa, na którym znajdował się plik zawierający dane osobowe członków O.

**Opis wydarzeń:**

**1)** Wójt w wysłanym zgłoszeniu poinformowała, iż:

**a)** naruszenie dotyczyło 51 osób,

**b)** zakres naruszenia obejmował następujące dane – imię i nazwisko, adres zamieszkania lub pobytu oraz numer PESEL.

**2)** W dodatkowych wyjaśnieniach Wójt wskazał, iż skradziony komputer był zabezpieczony przed nieautoryzowanym dostępem jedynie za pomocą hasła, a jego dysk twardy nie był zaszyfrowany.

**3)** W związku z powyższym Prezes UODO wszczął z urzędu postępowanie administracyjne w przedmiocie nałożenia na Wójta administracyjnej kary pieniężnej w związku z naruszeniem ochrony danych osobowych członków O.

**Przyczyna naruszenia:**

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

**Decyzja PUODO**:

Kara pieniężna w wysokości 8 000 PLN.

**Źródło:**

https://www.uodo.gov.pl/decyzje/DKN.5131.8.2022

## 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 udokumentowaną analizę ryzyka uwzględniającą charakterystykę zachodzących procesów, aktywa, podatności, zagrożenia oraz istniejące zabezpieczenia, w ramach zachodzących procesów przetwarzania danych osobowych.

**3)** Wykonuj cyklicznie analizę ryzyka dla systemów informatycznych i aplikacji, w których przetwarzasz dane osobowe.

**4)** Dokonuj regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzanych danych osobowych w systemach teleinformatycznych.

Przykłady zabezpieczeń wynikających z decyzji:

**a)** Regulamin korzystania z prywatnego komputera do celów prywatnych (BYOD),

**b)** Regulamin korzystania ze służbowych laptopów,

**c)** Polityka haseł,

**d)** Polityka kopii zapasowych.

Materiał edukacyjny przygotowany przez FORSAFE

Opracowanie merytoryczne
Katarzyna Kawczyńska