

# Kary Prezesa Urzędu Ochrony Danych Osobowych



Data wydania decyzji

**18 lipca 2023 r.**

Podmiot kontrolowany

**K.**

Wysokość kary

**15 000 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 maju 2022 r. do Prezesa Urzędu Ochrony Danych Osobowych (UODO) wpłynęło zgłoszenie naruszenia ochrony danych osobowych od K. (Administrator) polegające na kradzieży służbowego komputera przenośnego z samochodu służbowego osoby zajmującej kierownicze stanowisko.

### Opis wydarzeń:

- Administrator w wysłanym zgłoszeniu poinformował, iż naruszenie obejmowało następujące dane osobowe – imię i nazwisko, data urodzenia, adres zamieszkania lub pobytu oraz numer PESEL.
- Na podstawie zebranego materiału dowodowego Prezes UODO ustalił, że skradziony laptop nie był szyfrowany, ale dane zostały odzyskane z kopii zapasowej.
- W ocenie Prezesa UODO Administrator nie zastosował odpowiednich środków technicznych i organizacyjnych zapewniających stopień bezpieczeństwa odpowiadający ryzyku przetwarzania danych z wykorzystaniem przenośnych komputerów służbowych.

### Przyczyna naruszenia:

Administrator nie zastosował adekwatnych środków technicznych mających na celu zminimalizowanie ryzyka naruszenia bezpieczeństwa danych przetwarzanych z wykorzystaniem komputera przenośnego wynoszonego poza organizację.

### Decyzja PUODO:

- Kara pieniężna w wysokości 15 000 PLN.

### Źródło:

<https://www.uodo.gov.pl/decyzje/DKN.5131.47.2022>



## Kompas FORSAFE

### JAK UNIKAĆ TAKICH NARUSZEŃ?

- 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.
- Dokonuj regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania danych osobowych w systemach teleinformatycznych.
- Wykonuj udokumentowaną analizę ryzyka uwzględniającą stan faktyczny, charakterystykę zachodzących procesów, aktywa, podatności, zagrożenia oraz istniejące zabezpieczenia, w ramach zachodzących procesów przetwarzania danych osobowych.

