

# Kary organów nadzorczych w Unii Europejskiej



Kraj oraz organ nadzorczy

**Szwecja**

Data Protection Authority of Sweden



Data wydania decyzji

**7 listopada 2023 r.**



Podmiot kontrolowany

**Indcap AB**



Wysokość kary

**43 000 EUR**

**FORSAFE**  
BEZPIECZENSTWO PONAD WSZYSTKO



## Rodzaj naruszenia

Art. 32 (1) RODO.

Niewystarczające środki techniczne i organizacyjne zapewniające bezpieczeństwo informacji.



## Przedmiot decyzji

### Źródło postępowania:

Do szwedzkiego organu nadzorczego wpłynęła skarga na Indcap AB (Indcap) dotycząca wysłania klientom pliku zawierającego dane osobowe innych klientów.

### Opis wydarzeń:

1. Szwedzki organ nadzorczy w związku z otrzymaną informacją dokonał czynności kontrolnych w Indcap.
2. Kontrola ujawniła, że za zaistniałą sytuację odpowiedzialny jest pracownik Indcap, który pobrał z systemu plik, a następnie zapisał go pod podobną nazwą jak ogólny raport z wynikami środków finansowych.
3. W wyniku tego zdarzenia około 2 813 osób otrzymało plik z danymi osobowymi 53 364 klientów.
4. Powyższy plik zawierał następujące dane osobowe – imię i nazwisko, numer PESEL, nazwa banku, nazwa doradcy, adres e-mail, informacja o poziomie ryzyka, informacja o alokacji do funduszy, wartość środków finansowych, numer rachunku bankowego.
5. Po zaistniałym incydencie Indcap zdecydował o zaprzestaniu wysyłania raportów kwartalnych e-mailem, aby wyeliminować podobną sytuację w przyszłości.
6. Szwedzki organ nadzorczy uznał, że Indcap nie wdrożył barier technicznych lub organizacyjnych, które utrudniłyby nieprawidłowe przetwarzanie pliku.

### Przyczyna naruszenia:

Pracownik Indcap wysłał klientom plik zawierający dane osobowe innych klientów.

### Decyzja:

1. Kara pieniężna w wysokości 43 000 EUR.

### Źródło:

<https://www.imy.se/globalassets/dokument/beslut/2023/beslut-tillsyn-indecap.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.

