

# Kary organów nadzorczych w Unii Europejskiej



Kraj oraz organ nadzorczy

## Niemcy

The Federal Commissioner for Data Protection and Freedom of Information (BfDI)



Data wydania decyzji

11.11.2020 r.



Podmiot kontrolowany

1&1 Telecom GmbH



Wysokość kary

900 000 EUR

FÖRSÄFE  
BEZPIECZEŃSTWO PONAD WSZYSTKO



### Rodzaj naruszenia

Naruszenie Art. 32 RODO  
Niewystarczające środki techniczne i organizacyjne zapewniające bezpieczeństwo informacji



### Przedmiot decyzji

#### Źródło postępowania:

Niemiecki organ nadzorczy otrzymał informację o nieprawidłowościach w procesie uwierzytelniania klientów 1&1 Telecom GmbH (Spółka).

#### Opis wydarzeń:

1) W toku postępowania ustalono, iż osoba dzwoniąca do działu obsługi klienta mogła uzyskać szczegółowe informacje na temat danych osobowych, uwierzytelniając się jedynie za pomocą imienia i nazwiska oraz daty urodzenia.

2) W związku z zaistniałą sytuacją, Spółka podjęła decyzję o wdrożeniu nowej, bezpieczniejszej metody uwierzytelniania.

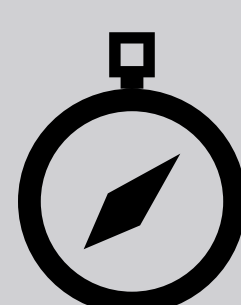
#### Przyczyna naruszenia:

Brak wystarczających środków technicznych i organizacyjnych, które uniemożliwiłyby osobom nieuprawnionym uzyskanie danych klientów z infolinii obsługi klienta.

#### Decyzja The Federal Commissioner for Data Protection and Freedom of Information (BfDI):

Kara pieniężna w wysokości 900 000 EUR.

Niemiecki organ nadzorczy pierwotnie nałożył na Spółkę karę pieniężną w wysokości 9 550 000 EUR. Spółka odwołała się od nałożonej kary do Sądu Rejonowego w Bonn, który obniżył karę do wysokości 900 000 EUR. Sąd swoją decyzję argumentował faktem, iż dotychczas nie było zarzutów co do stosowanej procedury uwierzytelniania a tym samym Spółka nie miała świadomości problemu. Ponadto Sąd uznał, iż naruszenie było niewielkie i nie mogło doprowadzić do masowego wycieku danych.



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

Materiał edukacyjny  
przygotowany przez FORSAFE



Opracowanie merytoryczne  
Katarzyna Cieślak

