

Kary organów nadzorczych w Unii Europejskiej



Kraj oraz organ nadzorczy



Data wydania decyzji



Podmiot kontrolowany



Wysokość kary

Francja

French Data Protection Authority (CNIL)

13 wrzesień 2022 r.

GIE INFOGREFFE

250 000 EUR








Rodzaj naruszenia

Art. 5 (1) e) RODO, Art. 32 RODO
Niewystarczające środki techniczne i organizacyjne zapewniające bezpieczeństwo informacji



Przedmiot decyzji

Źródło postępowania:

Francuski organ nadzorczy otrzymał skargę na GIE INFOGREFFE (INFOGREFFE) odnoszącą się do strony internetowej infogreffe.fr, która przechowuje hasła użytkowników w postaci niezaszyfrowanej.

Opis wydarzeń:

- 1) Francuski organ nadzorczy zdecydował o dokonaniu czynności kontrolnych w INFOGREFFE celem rozpatrzenia przedmiotowej sprawy.
- 2) W trakcie czynności kontrolnych francuski organ nadzorczy ustalił, iż INFOGREFFE poprzez stronę internetową infogreffe.fr umożliwia przeglądanie informacji prawnych o spółkach oraz zamawianie dokumentów poświadczonych przez sądy gospodarcze.
- 3) Osoby chcąc skorzystać z płatnej części portalu muszą posiadać konto członka (jednorazowa usługa) lub abonenta (roczna subskrypcja) oraz podać następujące dane: nazwisko, imię, adres zamieszkania, adres e-mail, numer telefonu stacjonarnego lub komórkowego, wybór tajnego pytania i odpowiedź na nie oraz dane dotyczące płatności.
- 4) Na podstawie zebranego materiału dowodowego francuski organ nadzorczy dopatrył naruszenia:
 - a) zasady ograniczenia przechowywania – INFOGREFFE przechowywało dane członków i abonentów powyższej 36 miesięcy od ostatniego zamówienia usługi i/lub dokumentów, czyli dłużej niż zadeklarowano w polityce prywatności umieszczonej na stronie internetowej,
 - b) obowiązku zapewnienia adekwatnych środków technicznych i organizacyjnych:
 - hasła służące do zalogowania się do konta użytkownika były niewystarczająco silne, gdyż zostały ograniczone do 8 znaków, a ich konstrukcja nie wymagała żadnych kryteriów złożoności,
 - pierwsze tymczasowe hasła do konta użytkownika były wysyłane na maila w postaci zwykłego tekstu,
 - hasła do konta użytkownika oraz tajne pytania i odpowiedzi na nie (wykorzystywane do resetowania hasła) przechowywane są w bazie danych w postaci zwykłego tekstu (niezaszyfrowane),
 - użytkownik nie jest informowany o zmianie hasła do konta,
 - nie dokonano regularnej kontroli nad technicznymi i organizacyjnymi środkami realizowanymi przez podwykonawcę w celu zapewnienia anonimizacji i bezpieczeństwa przetwarzanych danych osobowych.

Przyczyna naruszenia:

INFOGREFFE nie dopełniło obowiązku wdrożenia odpowiednich środków technicznych i organizacyjnych w celu zapewnienia poziomu ochrony odpowiedniego do ryzyka

Decyzja:

Kara pieniężna w wysokości 250 000 EUR.

Źródło:

https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000046280956?init=true&page=1&query=san-2022-018&searchField=ALL&tab_selection=all



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) Opracuj i wdróż procedurę retencji danych oraz regularnie weryfikuj procesy przetwarzania danych osobowych w aspekcie czasu ich przechowywania.

