NEXPUBLICA FRANCE ukarana grzywną w wysokości 1 700 000 euro

Posted on 2026-01-30

22 grudnia 2025 r. CNIL nałożyła na NEXPUBLICA FRANCE karę w wysokości 1,7 mln euro za niewdrożenie wystarczających środków bezpieczeństwa w oprogramowaniu PCRM, narzędziu do zarządzania relacjami z użytkownikami w sektorze usług społecznych.

Informacje ogólne

NEXPUBLICA FRANCE (wcześniej INETUM SOFTWARE FRANCE), firma specjalizująca się w projektowaniu systemów informatycznych i oprogramowania, opracowuje pakiet oprogramowania o nazwie PCRM, będący narzędziem do zarządzania relacjami z użytkownikami w obszarze pomocy społecznej. Jest on wykorzystywany m.in. przez Departamentalne Domy Osób Niepełnosprawnych („Maisons départementales des personnes handicapées", MDPH) w niektórych departamentach.

Pod koniec listopada 2022 r. klienci NEXPUBLICA zgłosili do CNIL naruszenia ochrony danych osobowych, ponieważ użytkownicy portalu informowali o możliwości dostępu do dokumentów dotyczących osób trzecich. CNIL przeprowadziła następnie kontrolę w firmie,

która wykazała, że wdrożone przez nią środki techniczne i organizacyjne mające zapewnić bezpieczeństwo danych przetwarzanych za pośrednictwem oprogramowania PCRM były niewystarczające.

W konsekwencji komitet ograniczony – organ CNIL odpowiedzialny za nakładanie sankcji – nałożył na NEXPUBLICA FRANCE karę w wysokości 1,7 mln euro, biorąc pod uwagę możliwości finansowe firmy, brak znajomości podstawowych zasad bezpieczeństwa, liczbę osób dotkniętych naruszeniem oraz wrażliwość przetwarzanych danych (w szczególności ujawniających niepełnosprawność).

Naruszenie obowiązku zapewnienia bezpieczeństwa danych osobowych (art. 32 RODO)

Artykuł 32 RODO stanowi, że administrator i podmiot przetwarzający muszą wdrożyć odpowiednie środki techniczne i organizacyjne, aby zapewnić poziom bezpieczeństwa odpowiadający ryzyku, uwzględniając stan wiedzy technicznej, koszty wdrożenia, charakter, zakres, kontekst i cele przetwarzania, a także ryzyko naruszenia praw i wolności osób fizycznych.

Komitet ograniczony uznał, że firma nie spełniła tych wymogów przy wdrażaniu PCRM, biorąc pod uwagę ogólną słabość systemu informatycznego oraz zaniedbania, które doprowadziły do utrzymywania się strukturalnych problemów z bezpieczeństwem.

Stwierdzono, że zidentyfikowane w PCRM podatności:

- wynikały głównie z braku znajomości aktualnych standardów i podstawowych zasad bezpieczeństwa,
- były znane i zidentyfikowane przez firmę w kilku raportach audytowych.

Pomimo tych ustaleń luki zostały usunięte dopiero po wystąpieniu naruszeń danych.

Okoliczności te są szczególnie obciążające ze względu na profil działalności firmy, która

specjalizuje się w systemach IT i doradztwie w zakresie oprogramowania.

Komitet ograniczony nie wydał nakazu doprowadzenia do zgodności, ponieważ firma podjęła niezbędne działania naprawcze po naruszeniach danych.

Źródło:

Komunikat francuskiego organu nadzorczego

Data security: NEXPUBLICA FRANCE fined €1,700,000 | CNIL