

CNIL nałożyła na szpital 500 tys. euro kary za niewystarczające
zabezpieczenie danych pacjentów

CNIL nałożyła na szpital 500 tys. euro kary za niewystarczające zabezpieczenie danych pacjentów

Posted on 2026-10-01

Francuski organ ochrony danych (Commission nationale de l'informatique et des libertés) nałożył na Hôpital Privé de la Loire administracyjną karę pieniężną w wysokości ok. 0,5 mln euro. Postępowanie było związane z cyberatakiem, w wyniku którego osoba nieuprawniona uzyskała dostęp do danych 524 867 pacjentów oraz 202 246 osób wskazanych przez nich jako „osoby zaufane”. Wśród wykradzionych danych znajdowały się również informacje dotyczące zdrowia.

CNIL stwierdził, że szpital nie wdrożył odpowiednich środków bezpieczeństwa, które mogłyby utrudnić przeprowadzenie ataku i ograniczyć jego skutki. Organ uznał również, że

CNIL nałożyła na szpital 500 tys. euro kary za niewystarczające
zabezpieczenie danych pacjentów

szpital nie poinformował wszystkich osób, których dane zostały skradzione, o naruszeniu ochrony danych.

Atak na system informatyczny szpitala

Do naruszenia doszło latem 2025 r. Osoba atakująca zdołała uzyskać dostęp do elektronicznej dokumentacji pacjentów (dossier patient informatisé, DPI) Hôpital Privé de la Loire, w której centralizowane są dane dotyczące osób objętych opieką szpitala. W wyniku ataku uzyskano dostęp do danych 524 867 pacjentów. W przypadku części z nich były to dane dotyczące zdrowia. Dostęp uzyskano również do danych 202 246 osób określanych jako „osoby zaufane”, wskazanych przez pacjentów.

Po zgłoszeniu naruszenia CNIL przeprowadził kontrolę, która wykazała kilka uchybień po stronie szpitala w zakresie realizacji obowiązków wynikających z RODO. Dotyczyły one przede wszystkim bezpieczeństwa przetwarzania danych oraz obowiązku poinformowania osób, których dane zostały objęte cyberatakiem.

Niewystarczające zabezpieczenia systemu

Jednym z głównych ustaleń CNIL było stwierdzenie, że procedura uwierzytelniania stosowana przy dostępie do elektronicznej dokumentacji pacjentów przez użytkowników spoza szpitala nie była wystarczająco odporna na zagrożenia. Z systemu korzystali m.in.

CNIL nałożyła na szpital 500 tys. euro kary za niewystarczające zabezpieczenie danych pacjentów

lekarze niezwiązani bezpośrednio ze szpitalem. Przy dostępie do dokumentacji nie stosowano sieci VPN ani uwierzytelniania wieloskładnikowego. Zdaniem CNIL zastosowanie tych podstawowych środków bezpieczeństwa mogłoby utrudnić przeprowadzenie ataku. Osoba atakująca wykorzystała istniejącą podatność i uzyskała dostęp do danych.

Zbyt szeroki zakres uprawnień dostępowych

CNIL zakwestionował również sposób organizacji dostępu do danych pacjentów. Polityka nadawania uprawnień nie uwzględniała zasady dostępu odpowiadającego zespołowi sprawującemu opiekę nad konkretnym pacjentem. W praktyce oznaczało to, że dostęp do informacji objętych tajemnicą medyczną nie był odpowiednio ograniczony do osób rzeczywiście uczestniczących w udzielaniu świadczeń danemu pacjentowi.

Brak właściwego ograniczenia uprawnień miał szczególne znaczenie dla skali naruszenia. Osoba atakująca, posługując się danymi uwierzytelniającymi jednego konta użytkownika, była w stanie uzyskać dostęp do danych wszystkich pacjentów szpitala. Tym samym pojedyncze konto użytkownika stało się punktem dostępu do bardzo dużego zbioru danych, w tym danych dotyczących zdrowia.

Brak odpowiedniego

CNIL nałożyła na szpital 500 tys. euro kary za niewystarczające
zabezpieczenie danych pacjentów

monitorowania podejrzanej aktywności

Kolejnym stwierdzonym uchybieniem był brak środków pozwalających na wykrywanie podejrzanej aktywności w elektronicznej dokumentacji pacjentów w czasie rzeczywistym lub w bardzo krótkim czasie. Szpital nie posiadał mechanizmu, który pozwalałby odpowiednio szybko wykryć nietypową aktywność i, w razie potrzeby, uruchomić system ostrzegania.

W rezultacie osoba atakująca mogła przez kilka dni przeglądać elektroniczną dokumentację pacjentów i pobierać bardzo dużą ilość danych, a ta nietypowa aktywność nie została wykryta. CNIL uznał, że brak odpowiedniego monitorowania przyczynił się do zwiększenia skali naruszenia. W ocenie organu zastosowane przez szpital środki bezpieczeństwa nie były wystarczające, aby zapewnić poufność danych z uwzględnieniem ich liczby i charakteru.

Naruszenie art. 32 RODO

W związku z opisanymi nieprawidłowościami CNIL stwierdził naruszenie art. 32 RODO, dotyczącego bezpieczeństwa przetwarzania. Organ zwrócił uwagę, że w chwili naruszenia szpital nie wdrożył niektórych podstawowych środków bezpieczeństwa, które mogłyby utrudnić przeprowadzenie ataku. Dotyczyło to zarówno sposobu uwierzytelniania użytkowników zewnętrznych, jak i ograniczania dostępu do danych oraz wykrywania podejrzanej aktywności.

CNIL podkreślił jednocześnie, że nie jest możliwe całkowite wyeliminowanie ryzyka związanego z przetwarzaniem danych. Odpowiednio dobrane środki bezpieczeństwa

CNIL nałożyła na szpital 500 tys. euro kary za niewystarczające
zabezpieczenie danych pacjentów

powinny jednak pozwalać na zmniejszenie prawdopodobieństwa wystąpienia naruszenia oraz ograniczenie jego skutków. W toku postępowania Hôpital Privé de la Loire podjął szereg działań mających na celu podniesienie poziomu bezpieczeństwa. CNIL zobowiązał szpital do zakończenia ich wdrażania w terminach od trzech do piętnastu miesięcy, zależnie od rodzaju danego środka.

Nie wszyscy zostali poinformowani o naruszeniu

Drugie stwierdzone przez CNIL uchybienie dotyczyło obowiązku poinformowania osób, których dane zostały objęte naruszeniem. Szpital poinformował pacjentów, których dane zostały objęte naruszeniem. Nie przekazał jednak bezpośredniej informacji 202 246 osobom wskazanym przez pacjentów jako „osoby zaufane”, mimo że dane tych osób również zostały skradzione przez osobę atakującą.

CNIL uznał, że pominięcie tych osób pozbawiło je informacji niezbędnych do zrozumienia charakteru ataku i jego prawdopodobnych konsekwencji. Osoby te nie otrzymały również informacji o działaniach, które mogłyby podjąć w celu ograniczenia skutków naruszenia i ochrony przed ewentualnym wykorzystaniem ich danych w sposób złośliwy. Tym samym CNIL stwierdził również naruszenie art. 34 RODO, regulującego obowiązek zawiadomienia osób, których dane dotyczą, o naruszeniu ochrony danych osobowych.

CNIL nałożyła na szpital 500 tys. euro kary za niewystarczające
zabezpieczenie danych pacjentów

Kara w wysokości 500 tys. euro

3 września 2026 r. CNIL nałożył na Hôpital Privé de la Loire administracyjną karę pieniężną w wysokości 500 tys. euro.

Przy ustalaniu wysokości kary organ wziął pod uwagę m.in. brak wystarczającej świadomości podstawowych zasad bezpieczeństwa, bardzo dużą liczbę osób, których dane zostały objęte naruszeniem, charakter naruszonych danych oraz możliwości finansowe szpitala. Sprawa pokazuje szczególne znaczenie właściwego zabezpieczenia systemów wykorzystywanych do przetwarzania danych dotyczących zdrowia. Skala potencjalnych konsekwencji niewłaściwego zarządzania uprawnieniami dostępowymi, uwierzytelnianiem czy monitorowaniem aktywności użytkowników może być szczególnie duża w przypadku systemów centralizujących dane dużej liczby pacjentów.

Znaczenie ograniczania dostępu do danych

Decyzja CNIL zwraca uwagę na kilka elementów, które powinny być uwzględniane przy projektowaniu i utrzymywaniu systemów przetwarzających dane dotyczące zdrowia. Samo zapewnienie możliwości logowania do systemu nie jest wystarczające. Konieczne jest również odpowiednie zabezpieczenie procesu uwierzytelniania, właściwe ograniczenie zakresu uprawnień oraz monitorowanie aktywności w systemie.

CNIL nałożyła na szpital 500 tys. euro kary za niewystarczające
zabezpieczenie danych pacjentów

Szczególne znaczenie ma zasada, zgodnie z którą użytkownik powinien mieć dostęp wyłącznie do tych danych, które są mu rzeczywiście potrzebne w związku z wykonywanymi zadaniami. W analizowanym przypadku brak odpowiedniego ograniczenia dostępu sprawił, że wykorzystanie danych uwierzytelniających jednego konta umożliwiło dostęp do danych wszystkich pacjentów szpitala.

Sprawa Hôpital Privé de la Loire pokazuje również, że właściwe zabezpieczenia powinny służyć nie tylko zapobieganiu nieuprawnionemu dostępowi, ale także możliwie szybkiemu wykrywaniu nietypowej aktywności. W przypadku masowego dostępu do danych szybkie wykrycie anomalii może mieć istotne znaczenie dla ograniczenia skali naruszenia i jego skutków. Odpowiednie środki techniczne i organizacyjne powinny zatem obejmować cały proces ochrony danych – od uwierzytelniania i nadawania uprawnień, przez bieżące monitorowanie aktywności, aż po właściwe informowanie osób, których dane zostały objęte naruszeniem.

Źródło:

Komunikat Francuskiego Organu Nadzorczego

Violation de données en matière de santé : sanction de 500 000 euros à l'encontre de
l'HÔPITAL PRIVÉ DE LA LOIRE | CNIL