ZAWIADOMIENIE O NARUSZENIU OCHRONY DANYCH OSOBOWYCH

Szanowna Pani, Szanowny Panie,

Zespół Poradni Specjalistycznych Nr 1 w Tychach Sp. z o.o., jako administrator Pani/Pana danych osobowych, informuje o naruszeniu ochrony danych osobowych, które dotyczy Pani/Pana danych.

Co się wydarzyło?

Nasza placówka korzysta z oprogramowania medycznego dostarczanego przez EuroSoft sp. z o.o. (dalej: „dostawca"). Dostawca udostępnia swoim klientom również system zgłoszeniowy Mantis, służący do obsługi zgłoszeń serwisowych związanych z użytkowanym oprogramowaniem.

W dniu 9 października 2026 r. dostawca stwierdził nieautoryzowany dostęp do serwera, na którym funkcjonował system zgłoszeniowy Mantis. Z przekazanych nam informacji wynika, że osoba nieuprawniona miała dostęp do serwera od 8 października 2026 r. (godz. 23:39) do 9 października 2026 r. (godz. 1:36).

W toku prowadzonej przez dostawcę analizy ustalono, że w systemie zgłoszeniowym znajdowały się Pani/Pana dane osobowe. Nie można wykluczyć, że osoba nieuprawniona zapoznała się z tymi danymi lub je skopiowała.

Naruszenie nie dotyczyło systemu medycznego ani znajdującej się w nim bazy danych pacjentów.

Pani/Pana dane znalazły się w zakresie naruszenia dlatego, że zostały umieszczone w treści zgłoszenia serwisowego lub w załączniku przekazanym za pośrednictwem systemu zgłoszeniowego.

Jakich Pani/Pana danych dotyczy naruszenie?

Na podstawie informacji otrzymanych od dostawcy oraz przeprowadzonej przez nas analizy ustaliliśmy, że naruszenie dotyczy następujących Pani/Pana danych:

- numer PESEL;
- imię i nazwisko;
- informacje dotyczące zdrowia (rozpoznanie, procedura).

Dane te znajdowały się w treści zgłoszenia serwisowego lub w załączniku do zgłoszenia przekazanego dostawcy.

Jakie mogą być konsekwencje naruszenia?

W związku z ujawnieniem danych osobowych, w szczególności numeru PESEL, istnieje ryzyko ich wykorzystania przez osoby nieuprawnione.

Może to skutkować w szczególności:

- próbami wykorzystania Pani/Pana danych do zawierania umów lub uzyskiwania usług (np. kredytów lub pożyczek),
- wykorzystaniem posiadanych informacji do uwiarygodnienia prób oszustwa, np. w wiadomościach lub rozmowach telefonicznych, w których sprawca podszywa się pod naszą placówkę, bank lub urząd,
- dane dotyczące zdrowia, naruszeniem prywatności i dobrego imienia, dyskryminacją lub inną szkodą niemajątkową związaną z ujawnieniem informacji o stanie zdrowia.

Co zalecamy?

Rekomendujemy zastrzeżenie numeru PESEL w aplikacji mObywatel, w banku, na poczcie albo w urzędzie gminy/miasta. Zastrzeżenie jest bezpłatne i można je w każdej chwili cofnąć.

Zalecamy również zachowanie szczególnej ostrożności wobec wiadomości e-mail, SMS i połączeń telefonicznych od osób powołujących się na znajomość Pani/Pana danych osobowych lub kontaktów z naszą placówką. W razie wątpliwości prosimy przerwać kontakt i samodzielnie skontaktować się z naszą placówką, korzystając z oficjalnych danych kontaktowych.

Prosimy nie otwierać linków ani załączników w nieoczekiwanych wiadomościach i nie podawać nikomu haseł, kodów weryfikacyjnych, kodów BLIK ani danych kart płatniczych. Nasza placówka nigdy nie prosi o takie informacje. Podejrzane SMS-y można bezpłatnie przesłać do CERT Polska na numer 8080, a podejrzane wiadomości i strony zgłosić na stronie incydent.cert.pl.

W przypadku podejrzenia oszustwa lub zauważenia nieuprawnionej transakcji prosimy niezwłocznie skontaktować się z bankiem, a w razie podejrzenia przestępstwa – zawiadomić Policję i zachować otrzymane wiadomości.

Co zrobiliśmy?

Po otrzymaniu informacji o naruszeniu od dostawcy przeprowadziliśmy analizę jego zakresu oraz możliwych konsekwencji dla naszych pacjentów. Naruszenie zgłosiliśmy Prezesowi Urzędu Ochrony Danych Osobowych w dniu 22.10.2026r.

Zgodnie z informacjami otrzymanymi od dostawcy, po wykryciu incydentu podjęto działania zmierzające do jego opanowania oraz ograniczenia ryzyka wystąpienia podobnego zdarzenia w przyszłości.