Informacja o naruszeniu ochrony danych osobowych

Data publikacji: 28.10.2026

Szanowni Państwo,

informujemy, że doszło do incydentu bezpieczeństwa u dostawcy programu do fakturowania Fakturownia.pl, z którego korzystamy przy wystawianiu faktur.

Na czym polegało zdarzenie?

W okresie od 27 września 2026 r. około godz. 3:20 do 28 września 2026 r. około godz. 17:45 osoba nieuprawniona uzyskała dostęp do systemów Fakturownia.pl i skopiowała część przechowywanej tam bazy danych, w tym dane pochodzące z naszego konta.

O zdarzeniu zostaliśmy poinformowani przez Fakturownię 1 października 2026 r. Według informacji przekazanych przez dostawcę luka w zabezpieczeniach została usunięta 28 września 2026 r., a incydent zgłoszono Policji i CERT Polska. Dostawca wdrożył również dodatkowe działania zabezpieczające.

Kogo dotyczy ta informacja?

Informacja dotyczy osób, których dane osobowe zapisane w fakturach lub związanych z nimi informacjach mogły zostać objęte incydentem.

Zakres danych zależy od informacji zapisanych w systemie i może obejmować:

- imię i nazwisko;
- adres;
- numer telefonu;
- numer PESEL, jeżeli został wpisany w uwagach do faktury;
- nazwa usług wykonanych.

Nie oznacza to, że wszystkie wymienione dane każdej osoby zostały skopiowane. Na podstawie dostępnych informacji nie możemy potwierdzić, że w każdym przypadku doszło do skopiowania konkretnych danych.

Jakie ryzyko wiąże się z incydentem?

Nieuprawnione pozyskanie danych osobowych może zwiększyć ryzyko prób oszustwa, podszywania się pod inne osoby lub wykorzystania danych do wyłudzenia zobowiązań finansowych. W szczególności połączenie numeru PESEL z innymi danymi identyfikacyjnymi może zostać wykorzystane do prób zaciągnięcia kredytu lub pożyczki, zawarcia umowy albo dokonania zakupów z odroczoną płatnością.
Istnieje ryzyko, że cyberprzestępcy będą próbowali wykorzystać te informacje do działań socjotechnicznych (tzw. phishingu). Mogą oni próbować podszywać się pod naszą firmę, wysyłając fałszywe e-maile, np. z prośbą o dopłatę, informacją o zmianie numeru konta bankowego lub przesyłając fałszywe faktury korygujące

Jak mogą Państwo się zabezpieczyć?

Zalecamy podjęcie następujących działań:

- Zastrzeżenie numeru PESEL w aplikacji mObywatel, na stronie gov.pl lub w urzędzie gminy.
- Rozważenie skorzystania z alertów BIK informujących o próbach zaciągnięcia zobowiązań.
- Zachowanie szczególnej ostrożności wobec nieoczekiwanych wiadomości SMS, e-maili i telefonów, również tych, których nadawcy podszywają się pod naszą firmę.
- Nieotwieranie podejrzanych linków i załączników oraz nieprzekazywanie haseł, kodów SMS, kodów BLIK ani danych kart płatniczych.

- Potwierdzanie telefonicznie, na znany wcześniej numer, każdej prośby o płatność na nowy rachunek bankowy.
- Weryfikacja numeru konta: nasz oficjalny numer konta bankowego do rozliczeń pozostaje bez zmian. Znajdą go Państwo na dotychczas opłacanych fakturach oraz na naszej oficjalnej stronie internetowej.
- Potwierdzenie telefoniczne: jeśli otrzymają Państwo jakąkolwiek wiadomość e-mail z informacją o zmianie naszego rachunku bankowego, prośbą o pilną dopłatę lub nietypowym załącznikiem, prosimy o bezwzględny, bezpośredni kontakt telefoniczny z nami w celu potwierdzenia autentyczności tej prośby przed wykonaniem przelewu.

Podejrzane wiadomości SMS można przesłać do CERT Polska na numer 8080.

W przypadku podejrzenia oszustwa prosimy o niezwłoczny kontakt z bankiem, a jeśli istnieje podejrzenie popełnienia przestępstwa — również z Policją. Warto zachować wszelkie wiadomości i inne dowody.

Jakie działania podjęto?

Według informacji przekazanych przez Fakturownię dostawca usunął lukę w zabezpieczeniach, zmienił klucze i hasła do swoich systemów, przeniósł system na nowe serwery oraz unieważnił dotychczasowe linki do panelu kontrahenta. Współpracuje również z CERT Polska w celu sprawdzenia, czy skopiowane dane zostały upublicznione.

W związku z incydentem podjęliśmy dodatkowe działania w celu zwiększenia bezpieczeństwa naszych danych i dostępu do systemu fakturowania. Zmieniliśmy hasła dostępowe, włączyliśmy logowanie dwuetapowe oraz wygenerowaliśmy nowy klucz API, unieważniając dotychczasowy. Działania te mają na celu ograniczenie ryzyka nieuprawnionego dostępu do naszego konta i zwiększenie poziomu jego zabezpieczenia.

Kontakt

W przypadku pytań dotyczących naruszenia lub przetwarzania danych osobowych prosimy o kontakt:

- Administrator danych: Zdrowie i Uroda “Malina-Med”
- E-mail: klinika@malinamed.pl
- Inspektor ochrony danych osobowych: Dariusz Jażdżyk, tel. 690-335-294, adres e-mail: iod.grupapozdrowie@gmail.com

Przepraszamy za zaistniałą sytuację. Publikujemy tę informację, aby umożliwić Państwu zapoznanie się z charakterem incydentu i podjęcie odpowiednich działań ochronnych.

Zdrowie i Uroda “Malina-Med” sp. z o.o.