

Szanowni Państwo,

z przykrością informujemy, że 28 września 2026 r. stwierdziliśmy naruszenie ochrony danych osobowych w serwisie Faktuownia.pl („Faktuownia”). Osoba nieuprawniona włamała się do naszych systemów i skopiowała dużą część bazy danych, w tym danych z Państwa konta.

Naruszenie obejmuje:

- (a) Państwa dane osobowe, których administratorem jest Faktuownia - dane konta i jego użytkowników;
- (b) dane osobowe Państwa kontrahentów i innych osób, które powierzyli Państwo Faktuowni do przetwarzania jako ich administrator - m.in. dane z faktur, kontrahentów i płatności.

Stosownie do Polityki Prywatności oraz Regulaminu powierzenia przetwarzania danych osobowych („Regulamin”) dane z lit. (a) są administrowane przez Faktuownię. Dane z lit. (b), wprowadzone przez Państwa do konta, są administrowane przez Państwa, a Faktuownia przetwarza je na Państwa polecenie.

W zakresie danych z lit. (a) ta wiadomość jest zawiadomieniem, o którym mowa w art. 34 RODO. W zakresie danych z lit. (b) jest zgłoszeniem naruszenia administratorowi na podstawie art. 33 ust. 2 RODO i §4 ust. 8 Regulaminu.

Informacje przekazujemy etapami (art. 33 ust. 4 RODO). W najbliższych dniach, w uzupełnieniu do niniejszego zawiadomienia oraz z uwagi na poufność danych Państwa klientów, uruchomimy na Państwa koncie w Faktuowni panel ze szczegółowymi informacjami dla Państwa konta: kategorie danych, zakresy dat i liczby rekordów. Panel udostępni też imienną listę osób objętych naruszeniem z proponowaną kategorią ryzyka oraz szkic zgłoszenia do Prezesa UODO; decyzja o zawiadomieniu kontrahentów i jej wykonanie należą do Państwa jako administratora.

Co się stało?

Osoba nieuprawniona uzyskała dostęp do naszych systemów i skopiowała dane z bazy danych na własne serwery.

- Nieuprawniony dostęp trwał od 27.09.2026, ok. godz. 3:20, do 28.09.2026, ok. godz. 17:45.
- Lukę usunęliśmy 28.09.2026 o godz. 18:01.
- Rodzaj naruszenia: naruszenie poufności danych (dane zostały skopiowane).

Jakie dane zostały pobrane?

Przy każdej kategorii wskazujemy, kto jest administratorem danych, i jakiego okresu dotyczy pobranie. **(a) Fakturownia** - dane konta i jego użytkowników, których administratorem jest Fakturownia. **(b) Właściciel konta** - dane kontrahentów i innych osób, które klient wprowadził do konta i powierzył Fakturowni do przetwarzania jako ich administrator.

Kategoria danych	Administrator	Co pobrano
Dane firmy i użytkowników: nazwa firmy, NIP, adres, imiona i nazwiska, adresy e-mail i telefony użytkowników, identyfikator konta	(a) Fakturownia	w całości, jeśli zostały wprowadzone
Dane działów: adres, NIP, nazwa banku, numer rachunku, IBAN, SWIFT	(a) Fakturownia	w całości, jeśli zostały wprowadzone
Zaszyfrowane hasła użytkowników ze skrótem (hasła nie były zapisane jawnie)	(a) Fakturownia	w całości
Tokeny API, klucze integracji zapisane bezpośrednio w ustawieniach konta	(a) Fakturownia	w całości - zależnie od używanych integracji
Identyfikatory sesji	(a) Fakturownia	w całości
Kwoty z faktur: netto, VAT i brutto według stawek, waluta, kwota zapłacona i pozostała do zapłaty	(a) Fakturownia (b) Właściciel konta	faktury z całego okresu
Salda rachunków bankowych pobrane przez usługę "Połączenie z kontem bankowym"	(a) Fakturownia	w całości - tylko jeśli integracja była aktywna
Kontrahenci: nazwa lub imię i nazwisko, NIP, adres, adres dostawy, e-mail, telefon, numer rachunku, notatka, pola własne	(b) Właściciel konta	tylko kontrahenci dodani przed 16.10.2024

Panel kontrahenta: link dostępowy i - jeśli kontrahent ustawił hasło - skrót hasła	(b) Właściciel konta	tylko kontrahenci dodani przed 16.10.2024
Dodatkowe strony faktury (np. odbiorca, płatnik): nazwa lub imię i nazwisko, NIP, adres, e-mail, telefon, notatka; treść dodatkowych pól opisowych (np. „Uwagi”, „Odbiorca”, własne etykiety)	(b) Właściciel konta	faktury z całego okresu - w zakresie, w jakim pola były uzupełnione
Pełna treść faktur: sprzedawca, nabywca, numer, daty, kwoty, sposób i termin płatności, uwagi	(b) Właściciel konta	tylko faktury wystawione przed 22.03.2021
Pozycje faktur: nazwy towarów, ilości, ceny	(b) Właściciel konta	tylko faktury sprzed 6.06.2019
Płatności: daty, kwoty, tytuły przelewów, nazwy i numery rachunków nadawców	(b) Właściciel konta	w zakresie, w jakim zostały wprowadzone
Produkty i cennik: nazwy, kody, opisy, ceny	(b) Właściciel konta	w całości
Dane zaimportowane z plików (faktury, kontrahenci, produkty)	(b) Właściciel konta	w zakresie, w jakim zostały wprowadzone
Zawartość eksportów i importów zlecanych w systemie	(b) Właściciel konta	zlecone do 6.03.2026 - w większości
Dokumenty magazynowe	(b) Właściciel konta	tylko sprzed 14.07.2023
Akcje magazynowe	(b) Właściciel konta	tylko sprzed 16.05.2022
Historia aktywności na koncie	(a) Fakturownia	tylko sprzed 24.11.2021

Informacje o załącznikach: nazwa, typ,
rozmiar, data

(b) Właściciel
konta

tylko pliki dodane
przed 6.11.2025

Daty graniczne ustaliliśmy z dzienników zapytań bazy danych; mogą się różnić o kilkanaście dni. Pobieranie największych zbiorów szło od najstarszych rekordów i zostało przerwane, zanim dotarło do nowszych. Dla faktur wystawionych od 22.03.2021 nie pobrano nazwy nabywcy ani numeru faktury.

Czego nie pobrano i co jeszcze ustalamy?

Nie zostały pobrane:

- certyfikaty KSeF;
- dane logowania do banków - Fakturownia ich nie przechowuje;
- dane kart płatniczych - Fakturownia ich nie przechowuje;
- dane przechowywane w ramach integracji konfigurowanych w zakładce Integracje i dodatki;
- treść faktur wystawionych od 22.03.2021 - poza kwotami, dodatkowymi polami opisowymi i danymi dodatkowych stron;
- dane kontrahentów dodane od 16.10.2024.

Według naszej wiedzy dane objęte naruszeniem nie zostały dotychczas upublicznione; monitorujemy to wspólnie z CERT Polska.

Możliwe konsekwencje i co mogą Państwo zrobić - Państwa dane (lit. a)

Opisujemy możliwe następstwa. Nie oznacza to, że już wystąpiły.

Co może się zdarzyć	Co zalecamy
Wiadomości i telefony od oszustów podszywających się pod Fakturownię, bank, urząd lub kontrahenta. Mogą wyglądać wiarygodnie, bo zawierają prawdziwe dane Państwa firmy, faktur i płatności. Ich celem może być wyłudzenie pieniędzy, haseł, kodów autoryzacyjnych lub innych danych.	Nie otwierać linków i załączników w nieoczekiwanych wiadomościach. Nie podawać haseł, kodów weryfikacyjnych, kodów BLIK ani danych kart - ani nam, ani nikomu innemu. Przy telefonie „z banku” lub „z urzędu” rozłączyć się i oddzwonić na numer z oficjalnej strony. Podejrzane SMS-y przesyłać do CERT Polska na numer 8080.

Próby przejęcia konta w Fakturowni, a przy używaniu tego samego hasła - także kont w innych serwisach.	Ustawić nowe hasło do Fakturowni. Zmienić hasło w innych serwisach, jeśli było takie samo. Sprawdzić listę użytkowników i ustawienia konta.
Użycie skradzionych kluczy do integracji z Państwa kontem.	Wpisać nowe klucze API w integracjach. Dla dotychczasowych kluczy API prowadzona jest whitelista na podstawie historycznych adresów IP użytkowników.
Fałszywe faktury, wezwania do zapłaty i prośby o przelew na zmieniony rachunek - wysyłane w Państwa imieniu albo do Państwa „od dostawcy”. Oszuści znają kwoty i wiedzą, które faktury są nieopłacone.	Każdą prośbę o zmianę numeru rachunku lub wykonanie nietypowego przelewu prosimy potwierdzić z kontrahentem, korzystając ze znanego wcześniej numeru telefonu. Nie należy korzystać z numeru podanego wyłącznie w podejrzanej wiadomości. Rachunki kontrahentów warto sprawdzać na białej liście podatników VAT. Prosimy też sprawdzić numery rachunków na Państwa fakturach w Fakturowni.

Jeżeli podejrzewają Państwo oszustwo lub nieuprawniony przelew, prosimy niezwłocznie skontaktować się z bankiem. W przypadku podejrzenia popełnienia przestępstwa należy zawiadomić Policję i zachować wiadomości oraz inne dowody. Prosimy także poinformować nas o próbie wykorzystania danych objętych naruszeniem.

Możliwe konsekwencje dla osób trzecich - dane powierzone (lit. b)

Jako administrator tych danych oceniają Państwo ryzyko i decydują, czy i jak zawiadomić osoby, których dane dotyczą. Poniżej wskazujemy zagrożenia, które widzimy, i działania, które mogą Państwo rozważyć.

Co może się zdarzyć	Co mogą Państwo rozważyć
Wiadomości i telefony podszywające się pod Państwa firmę, kierowane do kontrahentów, ich osób kontaktowych i dodatkowych stron faktur.	Poinformować kontrahentów, że mogą otrzymywać wiadomości podszywające się pod Państwa firmę, i wskazać, jak mogą je zweryfikować.

Fałszywe wezwania do zapłaty
nieopłaconych faktur na inny rachunek.

Poinformować kontrahentów, aby każdą zmianę numeru rachunku potwierdzali niezależnym kanałem - np. telefonicznie pod znanym wcześniej numerem, a nie numerem z wiadomości.

Użycie skopiowanego linku do panelu kontrahenta albo hasła kontrahenta w innych serwisach.

Linki unieważniamy i generujemy nowe. Kontrahentom, którzy ustawili hasło do panelu, warto zalecić zmianę tego hasła w innych serwisach, jeśli było takie samo.

Dla danych, których administratorem jest Fakturownia, oceniliśmy ryzyko jako wysokie: zakres danych jest szeroki, a liczba osób bardzo duża. Może to być dla Państwa punkt odniesienia przy ocenie ryzyka dla danych z lit. (b).

Termin 72 godzin na zgłoszenie do Prezesa UODO biegnie od stwierdzenia naruszenia. Według wytycznych EROD 9/2022 (pkt 44) administrator co do zasady stwierdza naruszenie, gdy poinformuje go podmiot przetwarzający. Jeżeli jednak już wcześniej uzyskali Państwo dostateczną pewność co do incydentu (np. z naszego komunikatu z 29.09.2026), termin mógł zacząć biec wcześniej. Zalecamy odnotowanie daty i godziny otrzymania tej wiadomości w Państwa dokumentacji naruszenia.

Nie muszą Państwo czekać na udostępnienie panelu ze szczegółowymi informacjami na koncie w Fakturowni: zgłoszenie wstępne można złożyć na podstawie tej wiadomości i uzupełnić później (art. 33 ust. 4 RODO).

Działania podjęte przez nas

- 28.09.2026, 13:35 - pierwsza blokada adresu atakującego;
- 28.09.2026, 18:01 - usunięcie luki w aplikacji;
- 28.09.2026, 18:56-20:14 - zmiana kluczy aplikacji i haseł usług;
- 28.09.2026, 20:44-21:51 - przeniesienie ruchu na nowe serwery zbudowane od zera, wyłączenie starych, dezaktywacja wykradzionych kluczy;
- 28.09.2026, 23:10 - czasowa blokada panelu klienta;
- 28.09.2026, 23:50 - 29.09.2026, 4:03 - wymiana tokenów API klientów;
- 29.09.2026, 2:35 - dodatkowe zabezpieczenia generatora plików PDF;

- 29.09.2026 - zgłoszenie naruszenia Prezesowi Urzędu Ochrony Danych Osobowych oraz zgłoszenie incydentu CERT Polska i Policji (CBZC);
- 29.09.2026 - poinformowanie Inspektora Ochrony Danych i ocena ryzyka dla osób fizycznych;
- 01.10.2026 - rozpoczęcie wysyłki indywidualnych zawiadomień e-mail do właścicieli kont i użytkowników.

Co dalej?

- W najbliższych dniach udostępniemy na Państwa koncie w Fakturowni informację o zakresie danych pobranych z Państwa konta.
- Bieżące ustalenia publikujemy na stronie fakturownia.pl/incydent (prosimy wpisać adres samodzielnie w przeglądarce).

Jak rozpoznać naszą wiadomość?

Ta wiadomość nie zawiera załączników i nie wymaga logowania. Nie prosimy o hasła, kody weryfikacyjne, kody BLIK ani dane kart. Wiadomości w tej sprawie wysyłamy wyłącznie z domeny fakturownia.pl.

Więcej informacji

W sprawie incydentu prosimy o kontakt:

- Inspektor Ochrony Danych: iod@fakturownia.pl
- Fakturownia sp. z o.o.: telefon +48 22 398 7771; adres korespondencyjny: [ul. Juliana Smulikowskiego 6/8](#), 00-389 Warszawa
- Zapytania administratorów danych: <https://app.fakturownia.pl/goto/helpdesk>

Przepraszamy za tę sytuację.

Z poważaniem

Fakturownia sp. z o.o.