

Jak zgłosić naruszenie ochrony danych do Prezesa UODO

Zgłoszenie wstępne – instrukcja dla klientów Fakturowni

Stan informacji: e-mail „Zawiadomienie o naruszeniu ochrony danych osobowych” z 1 października 2026 r.

W skrócie – pięć kroków

1. **Ustalić, kiedy dowiedzieli się Państwo o naruszeniu.** Od tej chwili biegnie 72 godziny na zgłoszenie.
2. **Już teraz złożyć zgłoszenie wstępne:** pobrać z konta częściowo wypełniony formularz, uzupełnić pola zaznaczone na żółto i złożyć go w UODO. Ryzyka i zawiadomień jeszcze Państwo nie oceniają.
3. **Po udostępnieniu panelu ze szczegółami Państwa konta** (w najbliższych dniach) – sprawdzić, jakie dane zostały pobrane, i porównać to z tym, co Państwo wpisywali w Fakturowni.
4. **Dopiero wtedy ocenić ryzyko dla osób z faktur** i zdecydować, czy i kogo zawiadomić.
5. **Złożyć zgłoszenie uzupełniające** z danymi z panelu i z Państwa decyzjami (część 6).

1. Dlaczego to Państwo składają zgłoszenie

Dane osobowe Państwa kontrahentów i innych osób z faktur wprowadzili Państwo do Fakturowni. Wobec tych danych są Państwo **administratorem**, a Fakturownia – **podmiotem przetwarzającym**, który przetwarza je na Państwa polecenie. W razie naruszenia podmiot przetwarzający zgłasza je administratorowi, a administrator – Prezesowi Urzędu Ochrony Danych Osobowych (art. 33 RODO).

1 października 2026 r. zgłosiliśmy Państwu naruszenie wiadomością e-mail „Zawiadomienie o naruszeniu ochrony danych osobowych”. Na Państwa koncie udostępniamy teraz **częściowo wypełniony formularz zgłoszenia do UODO** i tę instrukcję. W najbliższych dniach udostępnimy także **panel ze szczegółowymi informacjami o zakresie danych objętych wyciekiem z Państwa konta**. Zgłoszenia dokonują Państwo – my pomagamy, przekazując informacje, formularz i instrukcję.

O danych, których administratorem jest Fakturownia (dane konta i jego użytkowników), poinformowaliśmy osobno – tych danych Państwo nie zgłaszają.

2. Ile mają Państwo czasu

Zgłoszenie składa się bez zbędnej zwłoki, w miarę możliwości **w ciągu 72 godzin od chwili, w której dowiedzieli się Państwo o naruszeniu** z dostateczną pewnością. Zwykle jest to chwila otrzymania naszego e-maila z 1 października 2026 r. – godzinę odbioru można sprawdzić w skrzynce. Jeśli wiedzieli Państwo o incydencie wcześniej, np. z naszego komunikatu z 29 września 2026 r., termin mógł zacząć biec wcześniej.

Prosimy zapisać tę datę i godzinę w swojej dokumentacji. Zgłoszenie złożone po 72 godzinach nadal jest obowiązkowe – trzeba w nim wyjaśnić przyczynę opóźnienia. Brak kompletu informacji nie usprawiedliwia opóźnienia; po to jest zgłoszenie wstępne.

3. Dlaczego teraz zgłoszenie wstępne

Formularz UODO przewiduje trzy rodzaje zgłoszeń: **kompletne, wstępne** – z podstawowymi informacjami w terminie i obowiązkiem późniejszego uzupełnienia – oraz **uzupełniające**. RODO pozwala przekazywać informacje etapami, jeżeli nie da się ich podać od razu (art. 33 ust. 4 RODO).

Wciąż ustalamy dokładny zakres danych pobranych z poszczególnych kont. Termin 72 godzin biegnie jednak niezależnie od tego. Dlatego **rekomendujemy, aby już teraz złożyć zgłoszenie wstępne** na podstawie informacji z naszego e-maila z 1 października 2026 r., a po udostępnieniu panelu ze szczegółami wycieku z Państwa konta – ocenić ryzyko i złożyć **zgłoszenie uzupełniające**.

Dlaczego to bezpieczne rozwiązanie? UODO wskazuje, że opóźnienia nie usprawiedliwia czekanie na zakończenie analizy, oceny ryzyka ani zgromadzenie wszystkich informacji – w takich przypadkach należy złożyć zgłoszenie wstępne i później je uzupełnić (Poradnik UODO, pkt 9.2). Europejska Rada Ochrony

Danych zaleca, aby w pierwszym zgłoszeniu poinformować organ, że pełne informacje zostaną przekazane później (Wytyczne 9/2022, pkt 57) – to zdanie jest już w polu 4A formularza.

Jeżeli po analizie okaże się, że zgłoszenie było bezprzedmiotowe, wyjaśniają to Państwo w zgłoszeniu uzupełniającym (część 6). Za zgłoszenie incydentu, który ostatecznie okazał się nie być naruszeniem, nie przewidziano sankcji (Wytyczne 9/2022, pkt 60). Ryzykowne jest natomiast spóźnione zgłoszenie.

Co znaczy „zgłoszenie wstępne” w tej sytuacji? Bez wiedzy, jakie dane z Państwa konta zostały pobrane, nie da się rzetelnie ocenić ryzyka dla osób z faktur ani zdecydować, czy je zawiadomić. Dlatego w zgłoszeniu wstępnym **opisują Państwo zdarzenie i kategorie danych, które mogły zostać objęte, a ocenę ryzyka i decyzję o zawiadomieniu osób zapowiadają na zgłoszenie uzupełniające**. Formularz UODO przewiduje to wprost: w pkt 10 jest odpowiedź „Nie oeniłem jeszcze”.

4. Jak złożyć zgłoszenie

Elektronicznie

Przez formularz zgłoszenia naruszenia ochrony danych osobowych do Prezesa UODO w serwisie **biznes.gov.pl** – adres prosimy wpisać samodzielnie w przeglądarce. Zgłoszenie podpisuje się profilem zaufanym, podpisem kwalifikowanym albo e-dowodem. Pełnomocnik załącza pełnomocnictwo udzielone w formie elektronicznej oraz dowód uiszczenia opłaty skarbowej. Treść pól przenoszą Państwo do formularza elektronicznego z pobranego formularza – pola są w tej samej kolejności, a żółtych wskazówek się nie przenosi.

Na papierze – listownie lub osobiście

- Pobrać z konta częściowo wypełniony formularz UODO, uzupełnić go, usunąć żółte wskazówki, wydrukować, wpisać datę i miejscowość i podpisać przez osobę lub osoby uprawnione do reprezentowania Państwa firmy. Jeżeli podpisuje pełnomocnik – załączyć pełnomocnictwo.
- Wysłać na adres **Urząd Ochrony Danych Osobowych, ul. Stanisława Moniuszki 1A, 00-014 Warszawa** – najlepiej listem poleconym – albo złożyć osobiście w kancelarii UODO (godziny pracy kancelarii: 8:00–16:00).
- Zachować kopię formularza oraz dowód nadania lub potwierdzenie złożenia. Jeśli termin 72 godzin jest bliski, szybciej jest złożyć zgłoszenie elektronicznie albo osobiście.

Częściowo wypełniony formularz – jak z niego korzystać

Na Państwa koncie udostępniamy **oficjalny formularz UODO, w którym wypełniliśmy już pola dotyczące incydentu** – opis zdarzenia, czas naruszenia, rodzaj i charakter naruszenia, dane Fakturowni jako podmiotu przetwarzającego oraz działania, które podjęliśmy. Ten formularz jest jednakowy dla wszystkich klientów i opiera się na informacjach z naszego e-maila z 1 października 2026 r. Tych tekstów nie trzeba przepisywać.

- Pola oznaczone w tej instrukcji **„Wypełnione przez Fakturownię”** są już w formularzu. Prosimy je przeczytać i sprawdzić – mogą Państwo dopisać do nich własne informacje.
- Pola oznaczone **„Do decyzji i uzupełnienia przez Państwa”** wymagają Państwa wiedzy lub oceny – zależą od tego, jakie dane Państwo wpisywali i czym zajmuje się Państwa firma. W formularzu są oznaczone na żółto – wraz z krótkimi wskazówkami, co wpisać. Szersze wyjaśnienia i przykłady są w tej instrukcji.
- Miejsca w **[nawiasach kwadratowych]** uzupełniają Państwo. **Przed złożeniem prosimy usunąć wszystkie żółte wskazówki** i uwagę pod tytułem formularza – w zgłoszeniu ma zostać tylko Państwa treść.
- **Nie wpisują Państwo numerów zgłoszeń Fakturowni** (do UODO, CERT Polska, Policji) – dotyczą one zgłoszeń Fakturowni, a nie Państwa. **Nie podają Państwa danych Inspektora Ochrony Danych Fakturowni jako swoich.**

Szare ramki w części 5 pokazują, co Fakturownia wpisała w danym polu, oraz przykłady tekstów do Państwa uzupełnień.

5. Pole po polu

Część 1. Typ zgłoszenia

1 Typ zgłoszenia

WYPEŁNIONE PRZEZ FAKTUROWNIE DO DECYZJI I UZUPEŁNIENIA PRZEZ PAŃSTWA

- W formularzu zaznaczyliśmy „**Zgłoszenie wstępne**”. Przybliżoną datę uzupełnienia (pole opcjonalne) można pominąć albo wpisać datę, do której planują Państwo zakończyć analizę.
- Przy zgłoszeniu uzupełniającym – „**Zgłoszenie uzupełniające/zmieniające**”, z datą poprzedniego zgłoszenia i sygnaturą sprawy nadaną przez UODO (część 6).

1 Własna sygnatura sprawy (opcjonalnie)

DO DECYZJI I UZUPEŁNIENIA PRZEZ PAŃSTWA

Numer z Państwa rejestru naruszeń, jeśli go Państwo prowadzą; można pominąć.

1 Zgłoszenie organowi w innym państwie lub innym organom

DO DECYZJI I UZUPEŁNIENIA PRZEZ PAŃSTWA

Zaznaczyć **tylko wtedy, gdy Państwo sami** coś zgłosili – np. Policji próbę oszustwa wobec Państwa firmy – i podać własny numer. Zgłoszeń dokonanych przez Fakturownię tu nie wpisujemy.

Część 2. Podmiot zgłaszający

2A–2B Dane i adres siedziby administratora

DO DECYZJI I UZUPEŁNIENIA PRZEZ PAŃSTWA

Dane **Państwa firmy** według KRS lub CEIDG: pełna nazwa (przy jednoosobowej działalności – imię i nazwisko przedsiębiorcy i nazwa firmy), NIP, REGON, KRS (jeśli dotyczy), adres siedziby z gminą, powiatem i województwem. Sektor wybierają Państwo z listy (pole opcjonalne).

2C Osoby uprawnione do reprezentowania administratora

DO DECYZJI I UZUPEŁNIENIA PRZEZ PAŃSTWA

Osoby, które mogą działać w imieniu firmy (zarząd według KRS, wspólnicy, przedsiębiorca). Nie musi to być właściciel konta w Fakturowni.

2D Pełnomocnik

DO DECYZJI I UZUPEŁNIENIA PRZEZ PAŃSTWA

Zaznaczyć, jeśli zgłoszenie składa pełnomocnik, np. kancelaria lub biuro rachunkowe – z pełnomocnictwem.

2E Inspektor ochrony danych lub inny punkt kontaktowy

DO DECYZJI I UZUPEŁNIENIA PRZEZ PAŃSTWA

Dane **Państwa inspektora ochrony danych**. Jeśli go nie wyznaczono – zaznaczyć „Inspektor nie został wyznaczony” i podać osobę kontaktową w Państwa firmie (imię i nazwisko, telefon, e-mail). Urząd będzie się kontaktował z tą osobą.

2F Inne podmioty uczestniczące w przetwarzaniu

WYPEŁNIONE PRZEZ FAKTUROWNIE

Wpisaliśmy Fakturownię jako podmiot przetwarzający. Jeśli na Państwa koncie pracowało biuro rachunkowe, mogą je Państwo dodać jako drugi podmiot.

Nazwa i dane kontaktowe: Fakturownia sp. z o.o., ul. Juliana Smulikowskiego 6/8, 00-389 Warszawa;
Inspektor Ochrony Danych: iod@fakturownia.pl; tel. +48 22 398 7771.

Rola: Podmiot przetwarzający – dostawca internetowego programu do wystawiania faktur Fakturownia.pl, przetwarzający dane osobowe kontrahentów administratora na podstawie Regulaminu powierzenia przetwarzania danych osobowych. Naruszenie nastąpiło w systemach informatycznych tego podmiotu.

Część 3. Czas naruszenia

3A Data stwierdzenia naruszenia

DO DECYZJI I UZUPEŁNIENIA PRZEZ PAŃSTWA

Data i godzina, kiedy dowiedzieli się Państwo o naruszeniu – zwykle otrzymania naszego e-maila z 1 października 2026 r. (zob. część 2 tej instrukcji).

3A Sposób stwierdzenia naruszenia

WYPEŁNIONE PRZEZ FAKTUROWNIE DO DECYZJI I UZUPEŁNIENIA PRZEZ PAŃSTWA

Tekst jest w formularzu; prosimy uzupełnić datę i godzinę otrzymania naszego e-maila. Warianty:

Zgłoszenie naruszenia przez podmiot przetwarzający – Fakturownia sp. z o.o. – na podstawie art. 33 ust. 2 RODO: wiadomość e-mail „Zawiadomienie o naruszeniu ochrony danych osobowych” otrzymana **[data, godzina]**.

[Jeśli wiedzieli Państwo wcześniej:] Informacja o incydencie opublikowana przez podmiot przetwarzający **[data]**, a następnie zgłoszenie naruszenia przez podmiot przetwarzający e-mailem otrzymanym **[data, godzina]**.

[W zgłoszeniu uzupełniającym można dodać:] Szczegółowe informacje o danych z konta administratora podmiot przetwarzający udostępnił w panelu konta **[data]**.

3A Data powiadomienia przez podmiot przetwarzający (opcjonalnie)

DO DECYZJI I UZUPEŁNIENIA PRZEZ PAŃSTWA

Data i godzina otrzymania naszego e-maila (wysyłka rozpoczęła się 1 października 2026 r.).

3A Powody opóźnienia

DO DECYZJI I UZUPEŁNIENIA PRZEZ PAŃSTWA

Tylko jeśli od chwili stwierdzenia naruszenia minęło więcej niż 72 godziny – Państwa wyjaśnienie.

3B Data i czas rozpoczęcia i zakończenia naruszenia

WYPEŁNIONE PRZEZ FAKTUROWNIE

W formularzu:

Rozpoczęcie: 27.09.2026, ok. godz. 3:20

Zakończenie: 28.09.2026, ok. godz. 17:45

Część 4. Charakter naruszenia

4A Opis naruszenia

WYPEŁNIONE PRZEZ FAKTUROWNIE DO DECYZJI I UZUPEŁNIENIA PRZEZ PAŃSTWA

Opis zdarzenia jest w formularzu – poniżej jego treść. Na końcu mogą Państwo dopisać własne informacje, a w zgłoszeniu uzupełniającym – zakres danych z Państwa konta według panelu (przykłady w nawiasach).

Administrator korzysta z internetowego programu do wystawiania faktur Fakturownia.pl. Dane osobowe kontrahentów administratora i innych osób wskazanych na fakturach przetwarza w imieniu administratora podmiot przetwarzający – Fakturownia sp. z o.o.

Według informacji podmiotu przetwarzającego od 27.09.2026, ok. godz. 3:20, do 28.09.2026, ok. godz. 17:45 osoba nieuprawniona miała dostęp do jego systemów i skopiowała dużą część bazy danych na własne serwery, w tym dane z konta administratora. Podmiot przetwarzający stwierdził naruszenie 28.09.2026 i tego samego dnia o godz. 18:01 usunął lukę. 1 października 2026 r. zgłosił naruszenie administratorowi wiadomością e-mail (art. 33 ust. 2 RODO) i zapowiedział przekazanie szczegółowych informacji o danych z konta administratora. Podmiot przetwarzający zgłosił incydent także Prezesowi UODO, CERT Polska i Policji (CBZC).

Według informacji podmiotu przetwarzającego pobieranie największych zbiorów danych szło od rekordów najstarszych i zostało przerwane, zanim objęło nowsze, dlatego zakres pobranych danych zależy od daty ich zapisania. Z konta administratora mogły zostać pobrane: dane kontrahentów dodanych przed 16.10.2024 (nazwa lub imię i nazwisko, NIP, adres, adres dostawy, e-mail, telefon, numer rachunku, notatka, pola własne) oraz link do panelu kontrahenta i – jeśli kontrahent ustawił hasło – skrót hasła; dane dodatkowych stron faktury, np. odbiorcy lub płatnika (nazwa lub imię i nazwisko, NIP, adres, e-mail, telefon, notatka), treść dodatkowych pól opisowych oraz kwoty – z faktur z całego okresu; pełna treść faktur wystawionych przed 22.03.2021 (sprzedawca, nabywca, numer, daty, kwoty, sposób i termin płatności, uwagi); pozycje faktur sprzed 6.06.2019 (nazwy towarów, ilości, ceny); płatności (daty, kwoty, tytuły przelewów, nazwy i numery rachunków nadawców); dane zaimportowane z plików oraz zawartość eksportów i importów zleconych do 6.03.2026 (w większości); dokumenty magazynowe sprzed 14.07.2023 i akcje magazynowe sprzed 16.05.2022; informacje o załącznikach (nazwa, typ, rozmiar, data) dla plików dodanych przed 6.11.2025. Daty graniczne ustalono z dzienników zapytań bazy danych; mogą się różnić o kilkanaście dni. Dla faktur wystawionych od 22.03.2021 nie pobrano nazwy nabywcy ani numeru faktury.

Według informacji podmiotu przetwarzającego nie zostały pobrane: certyfikaty KSeF; dane logowania do banków i dane kart płatniczych (podmiot przetwarzający 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 faktury; dane kontrahentów dodanych od 16.10.2024. Według wiedzy podmiotu przetwarzającego dane nie zostały dotychczas upublicznione; podmiot przetwarzający monitoruje to wspólnie z CERT Polska.

[Zgłoszenie wstępne:] Zgłoszenie ma charakter wstępny. Administrator uzupełni je po otrzymaniu od podmiotu przetwarzającego szczegółowych informacji o danych ze swojego konta.

[Później, w zgłoszeniu uzupełniającym – według panelu:] Z konta administratora pobrano w szczególności: **[kategorie danych, okresy i liczby rekordów według panelu, sprawdzone przez Państwa]**.

[Opcjonalnie:] Administrator korzysta z programu od [rok]. Administrator nie stwierdził dotychczas prób wykorzystania danych / stwierdził [opis].

4B Na czym polegało naruszenie

WYPEŁNIONE PRZEZ FAKTUROWNIE

Zaznaczyliśmy: **e) Nieuprawnione uzyskanie dostępu do informacji poprzez złamanie zabezpieczeń.**

4C Działanie złośliwego oprogramowania

WYPEŁNIONE PRZEZ FAKTUROWNIE

Pozostawiliśmy puste – nie dotyczy (w 4B nie zaznaczono f).

4D Przyczyna naruszenia

WYPEŁNIONE PRZEZ FAKTUROWNIE

Zaznaczyliśmy: **Zewnętrzne działanie zamierzone.**

4E Charakter naruszenia

WYPEŁNIONE PRZEZ FAKTUROWNIE

Zaznaczyliśmy: **Naruszenie poufności danych** (według informacji podmiotu przetwarzającego dane zostały skopiowane).

4F Dzieci – usługi społeczeństwa informacyjnego

DO DECYZJI I UZUPEŁNIENIA PRZEZ PAŃSTWA

Zwykle nie dotyczy. Zaznaczają Państwo tylko, jeśli sprzedają Państwo usługę internetową bezpośrednio dzieciom. Jeśli na fakturach są dane dzieci w innym kontekście (np. szkoła, zajęcia, opieka), zaznacza się „Dzieci” w części 7.

Część 5. Liczba osób i wpisów

5 Przybliżona liczba osób, których dotyczy naruszenie

DO DECYZJI I UZUPEŁNIENIA PRZEZ PAŃSTWA

- Liczą się tylko **osoby fizyczne**: konsumenci, osoby prowadzące jednoosobową działalność, osoby kontaktowe firm i inne osoby wskazane na fakturach (odbiorcy, płatnicy). Spółek, fundacji czy urzędów nie liczymy.
- W zgłoszeniu wstępnym podają Państwo **szacunek na podstawie własnej wiedzy** – ile osób fizycznych **mogło zostać objętych** naruszeniem: np. ilu kontrahentów-osób fizycznych i osób kontaktowych mają Państwo w kartotece, z uwzględnieniem dat z pola 4A (np. kontrahenci dodani przed 16.10.2024). Lepiej podać liczbę z zapasem niż zaniżoną.
- Wystarczy zapis: „ok. [liczba] – szacunek, zostanie doprecyzowany w zgłoszeniu uzupełniającym”. Dokładniejsze liczby ustalą Państwo po udostępnieniu panelu – panel pokaże wstępne wyliczenie, które trzeba będzie sprawdzić, bo jest automatyczne i może się mylić.

5 Przybliżona liczba wpisów danych osobowych

DO DECYZJI I UZUPEŁNIENIA PRZEZ PAŃSTWA

Wpis to rekord, a nie osoba – jedna osoba może mieć kartę kontrahenta, kilka faktur i kilka płatności. W zgłoszeniu wstępnym wystarczy szacunek (np. liczba kart kontrahentów i faktur dla osób fizycznych); dokładniejsze liczby – w zgłoszeniu uzupełniającym, na podstawie panelu.

Część 6. Kategorie danych osobowych

6A Dane podstawowe

WYPEŁNIONE PRZEZ FAKTUROWNIE DO DECYZJI I UZUPEŁNIENIA PRZEZ PAŃSTWA

- W zgłoszeniu wstępnym zaznaczają Państwo kategorie, które **mogły zostać objęte** naruszeniem – czyli te, które były zapisane w Państwa koncie i mieszczą się w zakresie opisanym w polu 4A. Zakres potwierdzą Państwo w zgłoszeniu uzupełniającym. Najczęściej: **nazwiska i imiona, adres e-mail, numer telefonu, adres zamieszkania** (gdy kontrahentami są osoby prywatne lub jednoosobowe działalności prowadzone pod adresem domowym), **numer rachunku bankowego**.
- Numer PESEL** – jeśli wpisywali Państwo PESEL, np. w danych dodatkowych stron faktury dla osób prywatnych. **Nazwa użytkownika i/lub hasło** – jeśli kontrahenci ustawili hasło do panelu kontrahenta.
- W polu „Inne” wpisaliśmy kategorie wspólne dla wszystkich kont: NIP; dane z faktur (numery, daty, kwoty, sposób i termin płatności, informacja o nieopłaconych fakturach); nazwy towarów i usług; tytuły przelewów; treść uwag i notatek – **[opisać, co w nich wpisywano]**.
- Fakturownia nie wie, co Państwo wpisywali w uwagach, notatkach, opisach i nazwach pozycji – może tam być np. data urodzenia, numer dowodu, imiona rodziców, informacja o leczeniu czy sprawie sądowej. Takie dane także trzeba zaznaczyć.

Przykłady, kiedy trzeba zaznaczyć więcej: gabinety i placówki medyczne – często data urodzenia, PESEL, a także dane o zdrowiu (6B); szkoły, przedszkola, zajęcia dla dzieci – dane dzieci, imiona

rodziców; kancelarie – opisy spraw, czasem dane z art. 10 RODO (6C); najem i usługi wymagające potwierdzenia tożsamości – seria i numer dowodu; kursy i szkolenia – PESEL, data urodzenia.

6B Dane szczególnej kategorii

DO DECYZJI I UZUPEŁNIENIA PRZEZ PAŃSTWA

- Dane, których ujawnienie najbardziej szkodzi: o zdrowiu, pochodzeniu, poglądach, wyznaniu, przynależności do związków zawodowych, życiu seksualnym, dane genetyczne i biometryczne.
- Zaznaczają Państwo, jeśli z faktur, notatek lub nazw usług zapisanych w koncie można je wywnioskować – w zgłoszeniu wstępnym także wtedy, gdy nie wiadomo jeszcze, czy te dane zostały pobrane. **Ważne:** sam fakt, że ktoś jest klientem gabinetu, terapeuty czy apteki, jest już informacją o zdrowiu – nawet gdy na fakturze nie ma diagnozy.

6C Dane z art. 10 RODO (wyroki, czyny zabronione)

DO DECYZJI I UZUPEŁNIENIA PRZEZ PAŃSTWA

Dotyczy głównie kancelarii i firm współpracujących z sądami – np. faktura „obrona w sprawie karnej” ujawnia, że ktoś był podejrzanym.

Część 7. Kategorie osób

7 Kategorie osób i szczegółowy opis

WYPEŁNIONE PRZEZ FAKTUROWNIĘ DO DECYZJI I UZUPEŁNIENIA PRZEZ PAŃSTWA

- Zaznaczyliśmy **Klienci (obecni i potencjalni)** – prosimy sprawdzić; dodatkowo – zależnie od Państwa działalności – np. Pacjenci, Uczniowie, Dzieci, Pracownicy (gdy na fakturach są pracownicy lub osoby kontaktowe), Osoby o szczególnych potrzebach.
- Nie zaznaczają Państwo „Użytkownicy” z myślą o użytkownikach konta w Fakturowni – o ich danych informuje Fakturownia.
- Opis: część wspólna jest w formularzu; prosimy uzupełnić część dotyczącą Państwa firmy.

Kontrahenci administratora i inne osoby wskazane na jego fakturach i dokumentach (nabywcy, odbiorcy, płatnicy, nadawcy płatności), których dane były zapisane w programie Fakturownia.pl. Według informacji podmiotu przetwarzającego naruszenie obejmuje m.in. kontrahentów dodanych przed 16.10.2024 oraz osoby wskazane jako dodatkowe strony faktur z całego okresu; szczegółowy zakres dat – w pkt 4A.

[Państwa uzupełnienie, np.:] w większości przedsiębiorcy prowadzący jednoosobową działalność i osoby kontaktowe firm / konsumenci – pacjenci gabinetu; administrator korzysta z programu od **[rok]**; wśród osób **[są / nie ma]** osób szczególnie narażonych (dzieci, osoby starsze, pacjenci).

Część 8. Możliwe konsekwencje

8A Konsekwencje dla osób

WYPEŁNIONE PRZEZ FAKTUROWNIĘ DO DECYZJI I UZUPEŁNIENIA PRZEZ PAŃSTWA

- Zaznaczyliśmy – do sprawdzenia: **Utrata kontroli nad własnymi danymi osobowymi** oraz **Strata finansowa** (fałszywe faktury i wezwania do zapłaty na zmieniony numer rachunku). Pozostałe prosimy zaznaczyć, jeśli dotyczą:
- **Kradzież lub sfalszowanie tożsamości** – jeśli wśród danych są numery PESEL lub dokumentów. **Naruszenie dobrego imienia, dyskryminacja** – jeśli z danych wynikają informacje wrażliwe. **Utrata poufności danych chronionych tajemnicą zawodową** – np. kancelarie, gabinety lekarskie i psychologiczne.
- W polu „Inne” wpisaliśmy:

Wykorzystanie danych do wiadomości i telefonów podszywających się pod administratora, jego kontrahentów, bank lub urząd, w celu wyłudzenia pieniędzy lub danych; fałszywe wezwania do zapłaty nieopłaconych faktur na inny numer rachunku; użycie skopiowanego linku do panelu kontrahenta albo hasła kontrahenta w innych serwisach, jeśli było takie samo.

8B Czy wystąpiło wysokie ryzyko?

DO DECYZJI I UZUPEŁNIENIA PRZEZ PAŃSTWA

- W zgłoszeniu wstępnym **nie oceniają Państwo jeszcze ryzyka** – bez informacji, jakie dane z Państwa konta zostały pobrane, taka ocena nie byłaby rzetelna. Ocenę przedstawi Państwo w zgłoszeniu uzupełniającym (część 6).
- Na formularzu papierowym pola „Tak” / „Nie” prosimy pozostawić bez zaznaczenia i w uzasadnieniu wpisać tekst poniżej. Jeśli formularz elektroniczny nie pozwoli przejść dalej bez zaznaczenia, z ostrożności można zaznaczyć „Tak” – a w uzasadnieniu wyraźnie napisać, że to założenie ostrożnościowe do czasu ustalenia zakresu danych.

Ocena ryzyka nie jest na tym etapie możliwa: administrator nie otrzymał jeszcze od podmiotu przetwarzającego informacji o zakresie danych pobranych z jego konta. Administrator przeprowadzi ocenę po ich otrzymaniu i przedstawi ją w zgłoszeniu uzupełniającym. [Jeśli zaznaczono „Tak”:] Zaznaczenie „Tak” jest założeniem ostrożnościowym do czasu ustalenia zakresu danych.

Część 9. Środki bezpieczeństwa i środki zaradcze

9A Środki dotychczas stosowane

DO DECYZJI I UZUPEŁNIENIA PRZEZ PAŃSTWA

Państwa środki, np.: umowa powierzenia z dostawcą, indywidualne konta użytkowników, logowanie dwuetapowe, zasady haseł, nadawanie i odbieranie uprawnień, przeszkolenie pracowników. Prosimy opisać tylko to, co faktycznie stosowali Państwo. W formularzu jest już zdanie:

Dane były przetwarzane w systemie podmiotu przetwarzającego Fakturownia sp. z o.o. na podstawie Regulaminu powierzenia przetwarzania danych osobowych, który określa obowiązki podmiotu przetwarzającego w zakresie bezpieczeństwa danych.

9B Środki, aby naruszenie się nie powtórzyło

WYPEŁNIONE PRZEZ FAKTUROWNIE DO DECYZJI I UZUPEŁNIENIA PRZEZ PAŃSTWA

Działania Fakturowni są w formularzu; prosimy dopisać swoje.

Według informacji podmiotu przetwarzającego: 28.09.2026, 13:35 – pierwsza blokada adresu atakującego; 18:01 – usunięcie luki w aplikacji; 18:56–20:14 – zmiana kluczy aplikacji i haseł usług; 20:44–21:51 – przeniesienie ruchu na nowe serwery zbudowane od zera, wyłączenie starych, dezaktywacja wykradzionych kluczy; 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.

Administrator [do wyboru i uzupełnienia]: zmiana haseł użytkowników konta [data]; włączenie logowania dwuetapowego [data]; przegląd listy użytkowników konta [data]; wpisanie nowych kluczy API i kluczy integracji [data].

9C Środki ograniczające skutki dla osób

WYPEŁNIONE PRZEZ FAKTUROWNIĘ DO DECYZJI I UZUPEŁNIENIA PRZEZ PAŃSTWA

Działania Fakturowni są w formularzu; prosimy dopisać swoje.

Według informacji podmiotu przetwarzającego: unieważnienie dotychczasowych linków do panelu kontrahenta i wygenerowanie nowych; dezaktywacja wykradzionych kluczy; monitorowanie wspólnie z CERT Polska, czy dane nie zostały upublicznione; zgłoszenie incydentu Policji.

Administrator [do wyboru i uzupełnienia]: ostrzeżenie kontrahentów przed fałszywymi fakturami i wezwaniami do zapłaty [data]; potwierdzanie zmian numerów rachunków niezależnym kanałem. Decyzja o zawiadomieniu osób – po otrzymaniu informacji o zakresie danych z konta.

Część 10. Zawiadomienie osób

10 Czy osoby zostały zawiadomione?

DO DECYZJI I UZUPEŁNIENIA PRZEZ PAŃSTWA

- W zgłoszeniu wstępnym zaznaczyć „**Nie ocenilem jeszcze**”. Formularz sam wskazuje, że po podjęciu decyzji składa się zgłoszenie uzupełniające – tak właśnie zrobią Państwo po otrzymaniu informacji o zakresie danych z konta.
- Pozostałe pola pkt 10 (data, liczba osób, środki komunikacji, treść zawiadomienia) pozostawić puste. Jak je wypełnić w zgłoszeniu uzupełniającym – część 6.

Część 11. Przetwarzanie transgraniczne

11 Naruszenie ma charakter transgraniczny

DO DECYZJI I UZUPEŁNIENIA PRZEZ PAŃSTWA

Zwykle nie zaznacza się – pojedynczy kontrahenci z innych krajów nie czynią naruszenia transgranicznym. Zaznaczają Państwo, jeśli mają Państwo jednostki w innych krajach UE albo znaczna część Państwa klientów – osób prywatnych – mieszka w innych krajach Europejskiego Obszaru Gospodarczego. (Wielka Brytania na liście formularza nie należy do EOG.)

6. Zgłoszenie uzupełniające – krok po kroku

Kiedy je złożyć

Zgłoszenie uzupełniające składa się **bez zbędnej zwłoki**, gdy pojawią się nowe informacje lub zapadną decyzje (art. 33 ust. 4 RODO). Przepisy nie wyznaczają na nie osobnego terminu; jeżeli UODO wskaże sposób lub termin przekazania informacji, prosimy się do niego zastosować.

Kiedy	Co uzupełnić
Po udostępnieniu panelu ze szczegółami Państwa konta i jego sprawdzeniu	Zakres danych z Państwa konta (4A), liczby osób i wpisów (5), kategorie danych (6), opis osób (7) – po Państwa weryfikacji.
Po ocenie ryzyka	Odpowiedź i uzasadnienie w 8B; odpowiedź w 10.
Po wysłaniu zawiadomień do osób	Data, liczba zawiadomionych osób, kanały i treść zawiadomienia bez danych konkretnych osób (10).
Gdy otrzymają Państwo od nas nowe ustalenia	Zmiany wskazane w naszej wiadomości – z powołaniem się na nią.
Gdy okaże się, że zgłoszenie było bezprzedmiotowe	Wyjaśnienie i uzasadnienie – zob. niżej.

Można złożyć jedno zgłoszenie uzupełniające ze wszystkimi zmianami albo kilka – w miarę ustalania kolejnych informacji.

Jak je wypełnić

- Użyć tego samego formularza. W pkt 1 zaznaczyć „**Zgłoszenie uzupełniające/zmieniające**” i podać **datę poprzedniego zgłoszenia** oraz **sygnaturę sprawy nadaną przez UODO** (jest w piśmie lub wiadomości z urzędu). Jeśli sygnatury jeszcze nie ma – podać datę złożenia zgłoszenia wstępnego i sposób jego złożenia.
- Wypełnić **wszystkie pola aktualnymi informacjami**, a nie tylko te, które się zmieniły – tak, aby zgłoszenie uzupełniające dawało pełny obraz sprawy.
- Na początku pola 4A krótko opisać, co się zmieniło względem poprzedniego zgłoszenia, i usunąć zdanie o wstępnym charakterze zgłoszenia, jeśli to już ostatnie uzupełnienie.
- Jeżeli w zgłoszeniu wstępnym w pkt 10 zaznaczyli Państwo „Nie oceniłem jeszcze” – teraz wskazać decyzję. Po wysłaniu zawiadomień do osób trzeba przesłać ich treść (pkt 10).

Przykład początku pola 4A w zgłoszeniu uzupełniającym:

Niniejsze zgłoszenie uzupełnia zgłoszenie wstępne z [data] (sygn. [sygnatura UODO]). Zmiany względem zgłoszenia wstępnego: [np. zakres danych oraz liczby osób i wpisów ustalone na podstawie informacji przekazanych przez podmiot przetwarzający w panelu konta (pkt 4A, 5, 6, 7); ocena ryzyka (pkt 8B); informacja o zawiadomieniu osób (pkt 10)]. Pozostałe informacje ze zgłoszenia wstępnego pozostają aktualne.

Ocena ryzyka (pkt 8B) – w zgłoszeniu uzupełniającym

- Gdy wiedzą już Państwo, jakie dane z konta zostały pobrane, oceniają Państwo, czy naruszenie może powodować **wysokie ryzyko** dla osób z faktur. „Tak” oznacza obowiązek zawiadomienia tych osób (art. 34 RODO); „Nie” – zawiadamiać nie trzeba, ale trzeba umieć to uzasadnić.
- Na wysokie ryzyko wskazują zwłaszcza: numer PESEL lub dokumentu tożsamości, prywatny numer rachunku, dane o zdrowiu lub inne dane szczególne, dane dzieci. Same imię i nazwisko ze służbowymi danymi kontaktowymi zwykle nie stwarzają wysokiego ryzyka.
- Jeśli wysokie ryzyko dotyczy tylko części osób, zaznacza się „Tak” i wskazuje tę grupę w uzasadnieniu – zawiadamia się wtedy tylko tę grupę. Dla danych, których administratorem jest Fakturownia, oceniliśmy ryzyko jako wysokie – może to być dla Państwa punkt odniesienia.

Przykłady uzasadnienia do dostosowania:

Tak: Wysokie ryzyko dotyczy osób, których dane objęte naruszeniem obejmują [numer PESEL / prywatny numer rachunku bankowego / informacje, z których można wnioskować o zdrowiu] – [liczba] osób. Dane zostały celowo skopiowane przez osobę nieuprawnioną i mogą zostać użyte do [podszywania się i zaciągania zobowiązań / oszustw finansowych]. Te osoby zawiadamiamy. Dla pozostałych osób dane obejmują wyłącznie [imiona i nazwiska, służbowe dane kontaktowe, adresy i NIP działalności, dane z faktur] – naruszenie stwarza dla nich ryzyko, ale nie wysokie.

Nie: Dane objęte naruszeniem obejmują wyłącznie [imiona i nazwiska, służbowe dane kontaktowe, adresy i NIP działalności gospodarczej, dane z faktur]; nie obejmują numerów PESEL, dokumentów tożsamości, prywatnych numerów rachunków ani danych szczególnych kategorii. Naruszenie stwarza ryzyko, ale w ocenie administratora nie wysokie. [Kontrahentów ostrzeżliśmy przed fałszywymi fakturami i wezwaniami do zapłaty.]

Zawiadomienie osób (pkt 10) – w zgłoszeniu uzupełniającym

- Wysokie ryzyko, zawiadomienia wysłane – „**Tak**”, z datą, liczbą zawiadomionych osób i środkami komunikacji. Wysokie ryzyko, wysyłka planowana – „**Nie, ale zostaną zawiadomione**”, z datą lub zaznaczeniem „nie znam jeszcze daty”. Zawiadomienia wysyła się bez zbędnej zwłoki.
- Brak wysokiego ryzyka – „**Nie, nie zostaną zawiadomione**”, wariant „stwierdzono brak wysokiego ryzyka” (uzasadnienie w 8B). Pozostałe wyjątki (szyfrowanie przed naruszeniem, środki zastosowane po naruszeniu) w tej sprawie praktycznie nie mają zastosowania – dane skopiowano w postaci czytelnej.
- **Czy indywidualnie:** zwykle „Tak” – e-mail, a gdy go brak, list lub telefon. Komunikat publiczny tylko wobec osób, do których nie da się dotrzeć indywidualnie.
- **Treść zawiadomienia:** do UODO przesyła się treść faktycznie wysłaną, z danymi osoby zastąpionymi oznaczeniami, np. „[imię i nazwisko]”. Wzór zawiadomienia udostępnimy razem ze szczegółami Państwa konta.

Gdy zgłoszenie okazało się bezprzedmiotowe

Może się zdarzyć, że po sprawdzeniu informacji z panelu okaże się, że incydent **nie objął danych osobowych, za które Państwo odpowiadają** – np. na koncie byli zapisani wyłącznie kontrahenci będący spółkami, bez danych osób kontaktowych, albo z panelu wynika, że z Państwa konta nie pobrano danych osób fizycznych. Wtedy w zgłoszeniu uzupełniającym wyjaśniają Państwo, że zgłoszenie wstępne okazało się bezprzedmiotowe, i podają uzasadnienie.

Wytyczne EROD 9/2022 przewidują taką możliwość: administrator przekazuje organowi aktualne informacje, a incydent odnotowuje w swojej dokumentacji jako niebędący naruszeniem; za takie zgłoszenie nie przewidziano sankcji (pkt 60).

Przykład treści pola 4A:

Niniejsze zgłoszenie uzupełnia zgłoszenie wstępne z **[data]** (sygn. **[sygnatura UODO]**). Po analizie informacji przekazanych przez podmiot przetwarzający w panelu konta administrator ustalił, że incydent u podmiotu przetwarzającego nie objął danych osobowych, których administratorem jest zgłaszający: **[uzasadnienie, np. w programie były zapisane wyłącznie dane kontrahentów będących osobami prawnymi, bez danych osób kontaktowych]**. W związku z tym zgłoszenie wstępne okazało się bezprzedmiotowe. Administrator odnotował incydent w swojej dokumentacji.

Uwaga – to nie to samo co niskie ryzyko. Jeżeli dane osób z Państwa faktur zostały skopiowane, naruszenie miało miejsce – nawet jeśli oceniają Państwo ryzyko dla tych osób jako niskie. Wtedy zgłoszenie nie jest bezprzedmiotowe: w zgłoszeniu uzupełniającym aktualizują Państwo ocenę ryzyka (8B) i decyzję o zawiadomieniu osób (10), z uzasadnieniem.

7. Dokumentacja po Państwa stronie

- Każde naruszenie administrator odnotowuje w swojej dokumentacji (rejestrze naruszeń) – także wtedy, gdy uzna, że czegoś nie zgłasza albo kogoś nie zawiadamia (art. 33 ust. 5 RODO).
- Warto zapisać: chwilę stwierdzenia naruszenia, ocenę ryzyka z uzasadnieniem, decyzje o zgłoszeniu i zawiadomieniach, podjęte działania z datami.
- Zgłoszenia uzupełniające i ich powody – w tym ustalenie, że zgłoszenie okazało się bezprzedmiotowe – także odnotowuje się w dokumentacji.
- Prosimy zachować: kopie wszystkich zgłoszeń, potwierdzenie złożenia (UPO lub dowód nadania), sygnaturę sprawy, treść wysłanych zawiadomień i listę adresatów.

8. Kontakt i bezpieczeństwo

- Inspektor Ochrony Danych Fakturowni: iod@fakturownia.pl; Fakturownia sp. z o.o.: tel. +48 22 398 7771. Bieżące ustalenia: fakturownia.pl/incydent (adres prosimy wpisać samodzielnie).
- Pytania dotyczące samego składania zgłoszenia: infolinia UODO 606 950 000 (dni robocze, 10:00–14:00).
- Fakturownia nie prosi o przesłanie jej Państwa zgłoszenia ani danych do niego i nie oferuje „pomocy w zgłoszeniu” przez linki w wiadomościach. Wiadomości w sprawie incydentu wysyłamy wyłącznie z domeny fakturownia.pl, bez załączników.

Instrukcja jest pomocą podmiotu przetwarzającego (art. 28 ust. 3 lit. f RODO) i nie stanowi porady prawnej. Za treść zgłoszenia, ocenę ryzyka i decyzję o zawiadomieniu osób odpowiada administrator danych. W razie wątpliwości warto skonsultować się z własnym inspektorem ochrony danych lub prawnikiem.