

Komunikat w sprawie naruszenia ochrony danych osobowych w serwisie Fakturownia

Szanowni Państwo,

realizując swoje obowiązki jako administratora danych osobowych Polskie Koleje Linowe S.A. z siedzibą w Zakopanem (34-500), ul. Bachledy 7D (dalej: „Administrator” lub „Spółka”), informujemy o naruszeniu ochrony danych osobowych, do którego doszło u zewnętrznego dostawcy serwisu do wystawiania faktur, tj. Fakturownia Sp. z o.o. z siedzibą w Warszawie (dalej: „Fakturownia”), z którego korzysta Spółka. W dniu 02.10.2026 r. Spółka zawiadomiła o zdarzeniu Prezesa Urzędu Ochrony Danych Osobowych, składając zgłoszenie wstępne.

Komunikat dotyczy osób, na rzecz których Spółka wystawiała faktury w serwisie Fakturownia, w szczególności w związku ze sprzedażą biletów w kasach i Biurze Obsługi Klienta, tj. klientów indywidualnych, osób prowadzących jednoosobową działalność gospodarczą, wspólników spółek cywilnych, a także osób wskazanych na fakturach wystawianych na rzecz firm i instytucji (np. osób kontaktowych lub osób przyjmujących faktury). Dane te przetwarzamy w celu wystawienia faktur oraz wykonania obowiązków wynikających z przepisów prawa podatkowego i rachunkowego.

Administrator, który stosuje wysokie standardy ochrony Państwa danych osobowych, przekazuje poniższe informacje o zdarzeniu polegającym na nieuprawnionym dostępie do systemów Fakturowni i skopiowaniu danych. Poniżej wyjaśniamy szczegóły incydentu. Prosimy o zapoznanie się z tymi informacjami.

Co się stało?

Zgodnie z informacjami przekazanymi przez Fakturownię, w okresie od 27.09.2026 r. (ok. godz. 3:20) do 28.09.2026 r. (ok. godz. 17:45) osoba nieuprawniona uzyskała dostęp do systemów Fakturowni i skopiowała dużą część bazy danych serwisu. Incydent dotyczył wszystkich kont w serwisie Fakturownia, w tym konta, w ramach którego Spółka wystawia faktury. Fakturownia usunęła lukę 28.09.2026 r.

Według informacji Fakturowni nie stwierdzono zmiany ani usunięcia danych, a do dnia przekazania nam tych informacji nie stwierdzono również publikacji skopiowanych danych. Fakturownia analizuje incydent wspólnie z CERT Polska oraz zgłosiła go Prezesowi Urzędu Ochrony Danych Osobowych, CERT Polska i Policji. Incydent należy kwalifikować jako naruszenie poufności danych osobowych, polegające na skopiowaniu danych przez osobę nieuprawnioną.

Spółka uzyskała od Fakturowni potwierdzenie, że incydent objął dane przekazywane przez Spółkę, w odpowiedzi na skierowane przez nas zapytanie. Niezwłocznie po uzyskaniu tej informacji podjęliśmy działania wewnętrzne, w tym zabezpieczenie kont, analizę zakresu danych objętych naruszeniem oraz ocenę ryzyka (we współpracy z działem IT oraz Inspektorem Ochrony Danych).

Dane, które mogły zostać skopiowane, obejmują w szczególności: imię i nazwisko lub nazwę, adres (w tym adres korespondencyjny i adres dostawy), NIP, REGON, numer telefonu, adres e-mail, numer rachunku bankowego, dane osoby przyjmującej fakturę, a także dane z faktur i płatności (m.in. kwoty, daty, sposób i termin płatności, uwagi, tytuły przelewów).

Nie wszystkie kategorie danych będą dotyczyć każdej osoby, ponieważ zakres danych zależy od informacji wpisanych na fakturze oraz od daty dodania danych do serwisu. Incydent nie objął danych kart płatniczych.

Jakie są możliwe konsekwencje naruszenia?

Dane objęte naruszeniem to przede wszystkim dane identyfikacyjne, kontaktowe i dotyczące transakcji. Nie można jednak wykluczyć, że zostaną one wykorzystane przez osoby nieuprawnione, dlatego (z ostrożności) wskazujemy możliwe konsekwencje naruszenia:

- otrzymywanie wiadomości e-mail, SMS lub połączeń telefonicznych od osób podszywających się pod Spółkę, Fakturownię, bank, urząd lub kontrahenta (wiadomości takie mogą wyglądać wiarygodnie, ponieważ mogą zawierać prawdziwe dane z faktur);



- próby wyłudzenia od Państwa dodatkowych informacji (np. danych do logowania, kodów weryfikacyjnych, kodów BLIK, danych karty płatniczej) lub nakłonienia do dokonania płatności, w tym z wykorzystaniem fałszywych faktur, wezwań do zapłaty lub próśb o przelew na zmieniony numer rachunku;
- możliwość posłużenia się przez osoby trzecie Państwa danymi osobowymi w celu założenia na te dane konta internetowego (np. w serwisach społecznościowych) lub podszycia się pod Państwa;
- adres e-mail lub numer telefonu mógł trafić do bazy danych, z której mogą Państwo otrzymywać niechciane wiadomości (SPAM);
- poczucie utraty kontroli nad własnymi danymi osobowymi.

Co mogą Państwo zrobić, aby zaradzić naruszeniu?

Poniżej proponujemy środki, które mogą Państwu pomóc w uniknięciu negatywnych następstw naruszenia:

- prosimy o zachowanie ostrożności przy otwieraniu wiadomości e-mail i SMS, załączników oraz linków, zwłaszcza jeżeli wiadomość jest nietypowa, nieoczekiwana lub zawiera prośbę o pilne działanie albo płatność;
- prosimy nie podawać nikomu haseł, kodów weryfikacyjnych, kodów BLIK ani danych karty płatniczej; w przypadku telefonu rzekomo „z banku”, „z urzędu” lub „ze Spółki” prosimy rozłączyć się i oddzwonić na numer podany na oficjalnej stronie internetowej danej instytucji; podejrzanе SMS-y można przekazywać do CERT Polska na numer 8080;
- każdą prośbę o zapłatę na nowy lub zmieniony numer rachunku bankowego prosimy zweryfikować bezpośrednio ze Spółką, korzystając z danych kontaktowych podanych na oficjalnej stronie internetowej Spółki;
- w przypadku podejrzenia, że Państwa dane osobowe są wykorzystywane przez osoby nieuprawnione, prosimy o niezwłoczny kontakt z bankiem oraz (w razie potrzeby) z Policją, a także o przekazanie tej informacji Spółce;
- prosimy o zgłaszanie do Spółki wszelkich innych przypadków negatywnych konsekwencji wynikających z zaistniałego zdarzenia.

Jakie działania podjęliśmy oraz planujemy podjąć, aby zminimalizować ryzyko wystąpienia negatywnych konsekwencji naruszenia?

Jako Administrator podjęliśmy szereg konkretnych działań w celu zaradzenia naruszeniu i zminimalizowania negatywnych dla Państwa skutków wynikających z opisywanego zdarzenia, w tym takie, które mają na celu uniknięcie wystąpienia podobnego zdarzenia w przyszłości, takie jak:

- niezwłocznie po uzyskaniu informacji o zdarzeniu zmieniliśmy hasła do wszystkich kont użytkowników Spółki w serwisie Fakturownia; Spółka nie korzysta z interfejsu API serwisu;
- poinformowaliśmy pracowników korzystających z serwisu o zdarzeniu i przekazaliśmy im zalecenia bezpieczeństwa;
- wystąpiliśmy do Fakturowni o szczegółowe informacje dotyczące incydentu i na bieżąco monitorujemy publikowane przez nią komunikaty; według informacji Fakturowni usunęła ona dostęp osoby nieuprawnionej, wymieniła klucze i hasła usług oraz przeniosła serwis na nowe serwery;
- przeprowadziliśmy (we współpracy z Inspektorem Ochrony Danych) analizę zakresu danych oraz liczby osób objętych naruszeniem;
- w dniu 02.10.2026 r. dokonaliśmy wstępnego zgłoszenia naruszenia Prezesowi Urzędu Ochrony Danych Osobowych, które uzupełnimy po uzyskaniu pełnych informacji, i będziemy współpracować z tym organem w celu minimalizacji skutków zaistniałego zdarzenia.

Jak można się z nami skontaktować?

Jeżeli mają Państwo jakiegokolwiek pytania lub wątpliwości w związku z zaistniałym zdarzeniem, prosimy o kontakt ze Spółką drogą elektroniczną lub w formie pisemnej na wskazany wyżej adres Spółki.

W sprawach dotyczących ochrony danych osobowych możliwy jest również kontakt z naszym Inspektorem Ochrony Danych Osobowych Ludmiłą Łuczak, pod adresem e-mail: iodo@pkl.pl.

Przepraszamy za zaistniałą sytuację.

