DOKUMENTY PRAWNE

Polityka prywatności

Jakie dane osobowe przetwarzamy w aplikacji Inlockly™ i na stronie internetowej, w jakim celu i na jakiej podstawie, komu je przekazujemy, jak długo je przechowujemy oraz jakie prawa Ci przysługują.

Wersja 2.0 · 26 października 2026

© 2026 Inlockly™ · Wszelkie prawa zastrzeżone

Spis treści

01 Najważniejsze w skrócie 3
02 Kto jest administratorem danych 3
03 Pojęcia 4
04 Jakie dane przetwarzamy 4
05 Cele i podstawy prawne 6
06 Komu przekazujemy dane 7
07 Przekazywanie danych poza EOG 9
08 Jak długo przechowujemy dane 9
09 Twoje prawa 10
10 Usunięcie konta 10
11 Uprawnienia Aplikacji na urządzeniu 11
12 Dzieci 11
13 Bezpieczeństwo 11
14 Zmiany Polityki 12

Polityka prywatności (dalej: „**Polityka**"), wersja 2.0 obowiązująca od 26 października 2026 roku.

Najważniejsze w skrócie

- **Treści skarbca nie znamy.** Hasła, notatki, karty i inne pozycje szyfrujesz na swoim urządzeniu kluczem, którego nie mamy. Na serwerze leżą wyłącznie w postaci zaszyfrowanej i nie możemy ich odczytać ani nikomu przekazać w postaci jawnej.
- **Dane konta przetwarzamy, żeby usługa działała:** adres e-mail, imię i nazwisko, dane urządzeń i logowań, dane rozliczeniowe.
- **Serwery są w Unii Europejskiej** (Amazon Web Services, region Frankfurt). Niektórzy dostawcy, np. operatorzy płatności, mogą przetwarzać dane także poza EOG - wymieniamy ich niżej.
- **Nie sprzedajemy danych** i nie używamy ich do reklam.

Kto jest administratorem danych

Administratorem Twoich danych osobowych jest **IMPERIT Dawid Łukaszek** z siedzibą w Częstochowie, ul. Mireckiego 26A/38, 42-208 Częstochowa, Polska, NIP: 9492259428, REGON: 524405263 (dalej: „**IMPERIT**", „**my**"). IMPERIT tworzy i udostępnia menedżer haseł Inlockly™.

W sprawach danych osobowych napisz na adres privacy@inlockly.com. Nie wyznaczyliśmy inspektora ochrony danych.

Grupy firmowe. Gdy firma lub inna organizacja korzysta z Inlockly w grupie (plan Zespołowy lub Biznesowy) i zarządza w niej danymi swoich pracowników lub współpracowników, administratorem tych danych w grupie jest ta organizacja, a IMPERIT przetwarza je w jej imieniu na podstawie Umowy powierzenia przetwarzania danych. Twoje konto Inlockly i dane rozliczeniowe pozostają danymi, których administratorem jest IMPERIT.

Pojęcia

- **Aplikacja** – Inlockly™ w każdej postaci: aplikacja webowa (app.inlockly.com), aplikacje na komputery, telefony i tablety oraz rozszerzenia przeglądarek.
- **Strona internetowa** – strona www.inlockly.com.
- **Skarbiec** – zaszyfrowany zbiór Twoich pozycji (haseł, notatek, kart, dokumentów i innych danych).
- **Grupa** – konto rodzinne, zespołowe lub firmowe, w którym kilka osób dzieli foldery z pozycjami.

Jakie dane przetwarzamy

Dane skarbca (zaszyfrowane)

Treść pozycji, ich nazwy, adresy stron, załączniki i historia wersji są szyfrowane na Twoim urządzeniu, zanim trafią na serwer (szyfrowanie end-to-end, model zerowej wiedzy). Nie mamy klucza, więc nie możemy ich odczytać. Na serwerze widzimy tylko dane techniczne potrzebne do synchronizacji: liczbę i rozmiar pozycji, daty zmian oraz to, do jakiego skarbca, folderu lub grupy należą. Szczegóły opisuje Raport Bezpieczeństwa.

Dane konta

- adres e-mail, imię i nazwisko;
- zdjęcie profilowe (opcjonalnie);
- język i ustawienia aplikacji;
- dane zabezpieczeń konta: weryfikator hasła głównego (nie samo hasło), zaszyfrowane klucze, ustawienia weryfikacji dwuetapowej, klucze YubiKey, kody zapasowe w postaci skrótów;
- zgoda na newsletter (jeśli jej udzielisz).

Hasła głównego nie znamy i nigdy o nie nie poprosimy.

Urządzenia i logowania

Przy logowaniu i korzystaniu z Aplikacji zapisujemy: adres IP, przybliżoną lokalizację ustaloną z adresu IP (kraj, region, miasto), typ urządzenia, system operacyjny, przeglądarkę, wersję Aplikacji, czas i wynik logowania oraz informację, czy urządzenie lub kraj są nowe. Służy to bezpieczeństwu: pokazujemy Ci aktywność logowania, ostrzegamy mailem o logowaniu z nowego kraju i blokujemy próby odgadnięcia hasła.

Ikony witryn

Żeby pokazać ikonę strony obok pozycji, Aplikacja pyta nasz serwer o ikonę dla nazwy domeny (np. `example.com`). Nasz serwer pobiera ikonę z tej strony i przechowuje ją pod skrótem (hashem) nazwy domeny - samej nazwy nie zapisujemy w postaci jawnej. Strona, z której pobieramy ikonę, widzi nasz serwer, a nie Ciebie. Wyświetlanie ikon możesz wyłączyć w ustawieniach Aplikacji.

Grupy

W grupach przetwarzamy członkostwo, role, działy, uprawnienia i zaproszenia oraz dziennik zdarzeń grupy (np. dodanie członka, utworzenie lub usunięcie pozycji, zmiana uprawnień). W grupach w planie Biznesowym zapisujemy też **dziennik użycia pozycji**: kto i kiedy wyświetlił pozycję, odkrył lub skopiował hasło, skopiował kod 2FA, użył autouzupełniania lub wydrukował pozycję. Nie zapisujemy przy tym treści pozycji.

Właściciel i administratorzy grupy z odpowiednim uprawnieniem widzą w konsoli zarządzania: listę członków i ich role, dziennik zdarzeń grupy, aktywność logowania członków (czas, urządzenie, kraj) oraz - w planie Biznesowym - dziennik użycia pozycji. Nie widzą Twojego prywatnego skarbca.

Płatności

Przy zakupie przez stronę płatność obsługuje Stripe: przekazujemy mu adres e-mail i dane potrzebne do faktury, a od niego otrzymujemy identyfikator klienta, status płatności i subskrypcji oraz dane faktur. Danych karty nie widzimy. Przy zakupie w App Store lub Google Play płatność obsługuje Apple lub Google; otrzymujemy od nich tylko informację o zakupie i stanie subskrypcji.

Wsparcie i kontakt

Gdy piszesz do nas e-mailem, przez formularz w Aplikacji albo przez portal wsparcia, przetwarzamy Twój adres e-mail, imię i nazwisko oraz treść zgłoszenia.

Strona internetowa

Strona internetowa nie używa narzędzi analitycznych, reklamowych ani wtyczek mediów społecznościowych. Serwer zapisuje standardowe logi (adres IP, czas, adres strony, przeglądarka). Szczegóły: Polityka cookies.

Cele i podstawy prawne

Cel	Dane	Podstawa prawna (RODO)
Założenie i prowadzenie konta, synchronizacja skarbca, grupy, udostępnianie	konto, skarbiec (zaszyfrowany), grupy	art. 6 ust. 1 lit. b - wykonanie umowy
Bezpieczeństwo konta: aktywność logowania, alerty, ochrona przed nadużyciami, weryfikacja dwuetapowa	urządzenia i logowania	art. 6 ust. 1 lit. f - prawnie uzasadniony interes (ochrona kont i usługi)
Dziennik zdarzeń i użycia pozycji w grupie	grupy	art. 6 ust. 1 lit. b (funkcja grupy) i lit. f; w grupach firmowych - na polecenie organizacji (umowa powierzenia)
Płatności, faktury, obowiązki podatkowe i księgowe	płatności, konto	art. 6 ust. 1 lit. b i c

Cel	Dane	Podstawa prawna (RODO)
Wysyłanie wiadomości o koncie (aktywacja, bezpieczeństwo, rozliczenia, ważne zmiany)	e-mail	art. 6 ust. 1 lit. b i f
Newsletter	e-mail, imię	art. 6 ust. 1 lit. a - zgoda
Obsługa zgłoszeń i reklamacji	wsparcie i kontakt	art. 6 ust. 1 lit. b, c i f
Ustalenie, dochodzenie i obrona roszczeń	dane potrzebne w danej sprawie	art. 6 ust. 1 lit. f

Nie podejmujemy decyzji opartych wyłącznie na zautomatyzowanym przetwarzaniu, które wywołują wobec Ciebie skutki prawne lub w podobny sposób istotnie na Ciebie wpływają. Automatyczne blokady po kilku nieudanych próbach logowania są czasowe i służą ochronie konta.

Komu przekazujemy dane

Korzystamy z dostawców, którzy przetwarzają dane w naszym imieniu na podstawie umów powierzenia, albo - jak operatorzy sklepów i płatności - jako odrębni administratorzy:

Dostawca	Rola	Dane	Miejsce przetwarzania
Amazon Web Services EMEA SARL	serwery, baza danych, pliki, wysyłka e-maili	wszystkie dane konta i zaszyfrowany skarbiec	UE (Frankfurt)
Stripe Payments Europe, Ltd.	płatności i faktury na stronie	e-mail, dane do faktury, dane płatności	UE i USA

Dostawca	Rola	Dane	Miejsce przetwarzania
Apple Inc.	sprzedaż w App Store, weryfikacja urządzeń iOS (DeviceCheck)	dane zakupu, token urządzenia	USA i inne
Google Ireland Ltd.	sprzedaż w Google Play	dane zakupu	UE i USA
Cloudflare, Inc.	ochrona formularza rejestracji (Turnstile)	adres IP, dane przeglądarki	USA i inne
Yubico AB	weryfikacja jednorazowych kodów YubiKey	kod OTP klucza	UE (Szwecja)
IPinfo, Inc.	ustalenie kraju z adresu IP, gdy nie wystarcza nasza lokalna baza	adres IP	USA
Atlassian Pty Ltd	portal wsparcia	e-mail, imię i nazwisko, treść zgłoszenia	UE i USA
Better Stack, Inc.	monitoring usług i strona statusu	adres IP osób odwiedzających stronę statusu	UE i USA

Dane mogą też otrzymać: biuro rachunkowe (dane z faktur), kancelaria lub doradca w razie sporu oraz organy publiczne, gdy wymaga tego prawo. O żądaniu organu powiadomimy Cię, jeśli prawo na to pozwala. Treść skarbca możemy przekazać tylko w postaci zaszyfrowanej, bo nie mamy klucza.

Przekazywanie danych poza EOG

Dane konta i skarbca przechowujemy w Unii Europejskiej. Niektórzy dostawcy z tabeli wyżej (Stripe, Apple, Google, Cloudflare, IPinfo, Atlassian, Better Stack) mogą przetwarzać dane w USA lub innych krajach poza Europejskim Obszarem Gospodarczym. Odbywa się to na podstawie decyzji Komisji Europejskiej o odpowiednim stopniu ochrony (EU-US Data Privacy Framework – dla podmiotów certyfikowanych) albo standardowych klauzul umownych przyjętych przez Komisję (art. 45 i 46 RODO). Kopię zabezpieczeń możesz otrzymać, pisząc na privacy@inlockly.com.

Jak długo przechowujemy dane

Dane	Okres
Konto i skarbiec	do usunięcia konta; po zleceniu usunięcia 30 dni karencji (możesz je cofnąć), potem trwałe usunięcie
Usunięte pozycje (kosz, znaczniki synchronizacji)	do opróżnienia kosza; znaczniki synchronizacji 90 dni
Historia wersji pozycji	30 dni (skarbiec osobisty), 180 dni (grupy)
Aktywność logowania	90 dni
Dziennik użycia pozycji (plan Biznesowy)	365 dni
Dziennik zdarzeń grupy	do usunięcia grupy
Grupa	do usunięcia; po zleceniu usunięcia 30 dni karencji
Wygasłe linki udostępniania	30 dni historii bez zaszyfrowanej treści
Ikony witryn	30 dni od ostatniego użycia
Faktury i dane rozliczeniowe	5 lat od końca roku podatkowego (przepisy podatkowe)

Dane	Okres
Zgłoszenia do wsparcia	do 3 lat od zamknięcia sprawy (przedawnienie roszczeń)
Newsletter	do wycofania zgody
Logi serwerów	do 90 dni

Twoje prawa

Masz prawo:

- dostępu do swoich danych i otrzymania ich kopii (art. 15 RODO);
- sprostowania danych (art. 16);
- usunięcia danych (art. 17);
- ograniczenia przetwarzania (art. 18);
- przenoszenia danych (art. 20) - treść skarbca możesz w każdej chwili wyeksportować w Aplikacji;
- sprzeciwu wobec przetwarzania opartego na prawnie uzasadnionym interesie (art. 21);
- wycofania zgody w dowolnym momencie, bez wpływu na zgodność z prawem przetwarzania przed jej wycofaniem;
- wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych (ul. Stawki 2, 00-193 Warszawa, uodo.gov.pl).

Żeby skorzystać z praw, napisz na privacy@inlockly.com. Odpowiemy w ciągu miesiąca. Jeśli dane w grupie firmowej przetwarzamy w imieniu organizacji, przekażemy jej Twoje żądanie.

Usunięcie konta

Konto usuniesz w Aplikacji: **Ustawienia → Konto → Strefa niebezpieczna → Usuń konto**. Jeśli jesteś właścicielem grupy, najpierw przekaż własność innemu członkowi albo usuń grupę. Po zleceniu usunięcia konto czeka 30 dni (dostaniesz przypomnienie e-mailem na 3 dni przed końcem) - w tym czasie możesz je przywrócić. Potem trwale usuwamy konto,

skarbiec i dane z nim związane; zachowujemy tylko dane, które musimy przechowywać na podstawie przepisów (np. faktury). Jeśli nie możesz się zalogować, napisz na support@inlockly.com z adresu konta. Opis krok po kroku: Centrum pomocy.

Odinstalowanie Aplikacji nie usuwa konta.

Uprawnienia Aplikacji na urządzeniu

Aplikacja prosi o dostęp tylko wtedy, gdy jest potrzebny do wybranej funkcji. Dostęp możesz cofnąć w ustawieniach systemu:

- **internet** – synchronizacja (wymagane);
- **aparat** – zdjęcie profilowe i zeskanowanie kodu QR weryfikacji dwuetapowej (opcjonalne);
- **zdjęcia i pliki** – wybór zdjęcia profilowego, kodu QR lub załącznika, import i eksport (opcjonalne);
- **biometria** (Face ID, odcisk palca) – odblokowanie skarbca; obsługuje ją system, a Aplikacja otrzymuje tylko wynik („tak" albo „nie"), bez danych biometrycznych (opcjonalne);
- **NFC** – odczyt kodu z klucza YubiKey (opcjonalne);
- **autouzupełnianie** – wpisywanie loginów w innych aplikacjach i stronach (opcjonalne).

Dzieci

Z Inlockly mogą samodzielnie korzystać osoby, które ukończyły 16 lat. Osoba młodsza może korzystać z Aplikacji za zgodą rodzica lub opiekuna prawnego – w praktyce w grupie rodzinnej, do której doda ją rodzic lub opiekun, odpowiedzialny za tę zgodę.

Bezpieczeństwo

Treść skarbca szyfrujemy na Twoim urządzeniu (AES-256-GCM, klucz wyprowadzany z hasła głównego funkcją Argon2id). Dane na serwerach są chronione kontrolą dostępu, izolacją sieci i szyfrowaniem. Dostęp do danych konta mają tylko osoby, które potrzebują go do obsługi usługi. Szczegóły: Raport Bezpieczeństwa.

Zmiany Polityki

Politykę zmieniamy, gdy zmienia się Aplikacja, dostawcy lub przepisy. Aktualna wersja jest zawsze na tej stronie. O istotnych zmianach poinformujemy Cię e-mailem lub w Aplikacji przed ich wejściem w życie. Poprzednie wersje udostępniamy na tej stronie.