inlockly

LEGAL

Privacy Policy

What personal data we process in the Inlockly™ app and on our website, why and on what legal basis, who we share it with, how long we keep it, and what rights you have.

Version 2.0 · October 26, 2026

© 2026 Inlockly™ · All rights reserved

Contents

01 Summary 3

02 Who we are 3

03 Definitions 3

04 What data we process 4

05 Purposes and legal bases 6

06 Who we share data with 7

07 International transfers 8

08 How long we keep data 8

09 Your rights 9

10 Deleting your account 10

11 App permissions 10

12 Children 11

13 Security 11

14 Changes to this Policy 11

Privacy Policy (the "**Policy**"), version 2.0, effective October 26, 2026.

Summary

- **We can't see what's in your vault.** Your passwords, notes, cards, and other items are encrypted on your device with a key we don't have. Our servers only ever store them encrypted, and we can't read them or hand them over in readable form.
- **We process account data to run the service:** your email address, name, device and sign-in data, and billing data.
- **Our servers are in the European Union** (Amazon Web Services, Frankfurt region). Some providers, such as payment processors, may also process data outside the EEA - we list them below.
- **We don't sell your data** or use it for advertising.

Who we are

The controller of your personal data is **IMPERIT Dawid Łukaszek**, ul. Mireckiego 26A/38, 42-208 Częstochowa, Poland, Tax ID (NIP): 9492259428, REGON: 524405263 ("**IMPERIT**," "**we**," "**us**"). IMPERIT develops and provides the Inlockly™ password manager.

For anything related to your personal data, email privacy@inlockly.com. We have not appointed a data protection officer.

Business groups. When a company or other organization uses Inlockly in a group (Team or Business plan) to manage data about its employees or contractors, that organization is the controller of the data in the group, and IMPERIT processes it on the organization's behalf under our Data Processing Agreement. Your Inlockly account and billing data remain data controlled by IMPERIT.

Definitions

- **App** - Inlockly™ in any form: the web app (app.inlockly.com), the desktop, phone, and tablet apps, and the browser extensions.

- **Website** – www.inlockly.com.
- **Vault** – your encrypted collection of items (passwords, notes, cards, documents, and other data).
- **Group** – a family, team, or business account where several people share folders of items.

What data we process

Vault data (encrypted)

The contents of your items, their names, website addresses, attachments, and version history are encrypted on your device before they reach our servers (end-to-end encryption, zero-knowledge model). We don't have the key, so we can't read them. On the server, we only see the technical data needed for syncing: the number and size of items, when they changed, and which vault, folder, or group they belong to. For details, see our Security Whitepaper.

Account data

- email address, first and last name;
- profile photo (optional);
- language and app settings;
- account security data: a master password verifier (not the password itself), encrypted keys, two-step verification settings, YubiKey keys, and hashed backup codes;
- your newsletter consent (if you give it).

We don't know your master password and will never ask you for it.

Devices and sign-ins

When you sign in and use the App, we record: your IP address, approximate location derived from it (country, region, city), device type, operating system, browser, App version, the time and result of the sign-in, and whether the device or country is new. We use this for security: we show you your sign-in activity, email you about sign-ins from a new country, and block password-guessing attempts.

Website icons

To show a website's icon next to an item, the App asks our server for the icon of a domain name (for example, `example.com`). Our server fetches the icon from that website and stores it under a hash of the domain name - we don't store the domain name itself in readable form. The website we fetch the icon from sees our server, not you. You can turn website icons off in the App settings.

Groups

In groups, we process membership, roles, departments, permissions, and invitations, plus the group activity log (for example, a member was added, an item was created or deleted, permissions changed). In Business plan groups, we also record an **item usage log**: who viewed an item, revealed or copied a password, copied a 2FA code, used autofill, or printed an item, and when. We never record the contents of the item.

The group owner and admins with the relevant permission can see in the management console: the member list and roles, the group activity log, members' sign-in activity (time, device, country), and - on the Business plan - the item usage log. They can't see your private vault.

Payments

When you buy on our website, Stripe handles the payment: we share your email address and billing details with Stripe, and we receive a customer ID, payment and subscription status, and invoice data. We never see your card details. When you buy in the App Store or Google Play, Apple or Google handles the payment, and we only receive information about the purchase and the subscription status.

Support

When you contact us by email, through the form in the App, or through our support portal, we process your email address, name, and the content of your request.

Website

Our website doesn't use analytics, advertising tools, or social media plugins. Our servers keep standard logs (IP address, time, page address, browser). For details, see our Cookie Policy.

Purposes and legal bases

Purpose	Data	Legal basis (GDPR)
Creating and running your account, syncing your vault, groups, sharing	account, vault (encrypted), groups	Art. 6(1)(b) - performance of a contract
Account security: sign-in activity, alerts, abuse prevention, two-step verification	devices and sign-ins	Art. 6(1)(f) - legitimate interests (protecting accounts and the service)
Group activity and item usage logs	groups	Art. 6(1)(b) (group feature) and (f); in business groups - on the organization's instructions (Data Processing Agreement)
Payments, invoices, tax and accounting obligations	payments, account	Art. 6(1)(b) and (c)
Account emails (activation, security, billing, important changes)	email	Art. 6(1)(b) and (f)
Newsletter	email, name	Art. 6(1)(a) - consent
Support requests and complaints	support	Art. 6(1)(b), (c), and (f)
Establishing, exercising, or defending legal claims	data relevant to the matter	Art. 6(1)(f)

We don’t make decisions based solely on automated processing that produce legal effects concerning you or similarly significantly affect you. Automatic lockouts after several failed sign-in attempts are temporary and protect your account.

Who we share data with

We use providers that process data on our behalf under data processing agreements, or - like app stores and payment processors - as separate controllers:

Provider	Role	Data	Where
Amazon Web Services EMEA SARL	servers, database, file storage, email delivery	all account data and the encrypted vault	EU (Frankfurt)
Stripe Payments Europe, Ltd.	payments and invoices on our website	email, billing details, payment data	EU and US
Apple Inc.	App Store sales, iOS device verification (DeviceCheck)	purchase data, device token	US and other
Google Ireland Ltd.	Google Play sales	purchase data	EU and US
Cloudflare, Inc.	sign-up form protection (Turnstile)	IP address, browser data	US and other
Yubico AB	verifying YubiKey one-time codes	the key’s OTP code	EU (Sweden)
IPinfo, Inc.	looking up the country of an IP address when our local database isn’t enough	IP address	US
Atlassian Pty Ltd	support portal	email, name, request content	EU and US

Provider	Role	Data	Where
Better Stack, Inc.	service monitoring and status page	IP address of status page visitors	EU and US

Data may also be shared with our accounting firm (invoice data), legal advisers in the event of a dispute, and public authorities where required by law. We'll tell you about a request from an authority if the law allows it. We can only ever hand over vault contents in encrypted form, because we don't have the key.

International transfers

We store account and vault data in the European Union. Some of the providers listed above (Stripe, Apple, Google, Cloudflare, IPinfo, Atlassian, Better Stack) may process data in the US or other countries outside the European Economic Area. These transfers rely on a European Commission adequacy decision (the EU-US Data Privacy Framework, for certified companies) or the Commission's standard contractual clauses (Articles 45 and 46 GDPR). You can request a copy of these safeguards at privacy@inlockly.com.

How long we keep data

Data	Retention
Account and vault	until you delete your account; after you request deletion, a 30-day grace period (you can cancel), then permanent deletion
Deleted items (trash, sync markers)	until you empty the trash; sync markers for 90 days
Item version history	30 days (personal vault), 180 days (groups)
Sign-in activity	90 days

Data	Retention
Item usage log (Business plan)	365 days
Group activity log	until the group is deleted
Group	until deleted; after deletion is requested, a 30-day grace period
Expired share links	30 days of history without the encrypted contents
Website icons	30 days after last use
Invoices and billing data	5 years from the end of the tax year (tax law)
Support requests	up to 3 years after the request is closed (limitation period for claims)
Newsletter	until you withdraw consent
Server logs	up to 90 days

Your rights

You have the right to:

- access your data and get a copy (Art. 15 GDPR);
- correct your data (Art. 16);
- have your data erased (Art. 17);
- restrict processing (Art. 18);
- data portability (Art. 20) - you can export your vault in the App at any time;
- object to processing based on legitimate interests (Art. 21);
- withdraw your consent at any time, without affecting the lawfulness of processing before you withdraw it;

- lodge a complaint with a supervisory authority - in Poland, the President of the Personal Data Protection Office (UODO, ul. Stawki 2, 00-193 Warsaw, uodo.gov.pl), or the authority in the EU country where you live or work.

To exercise your rights, email privacy@inlockly.com. We'll respond within one month. If we process the data in a business group on an organization's behalf, we'll forward your request to that organization.

Deleting your account

You can delete your account in the App: **Settings → Account → Danger zone → Delete account**. If you own a group, first transfer ownership to another member or delete the group. After you request deletion, your account is kept for 30 days (we'll email you a reminder 3 days before the end), and you can restore it during that time. After that, we permanently delete your account, vault, and related data, keeping only what the law requires us to keep (such as invoices). If you can't sign in, email support@inlockly.com from your account's email address. Step-by-step guide: Help Center.

Uninstalling the App doesn't delete your account.

App permissions

The App only asks for access when a feature you use needs it. You can revoke access in your system settings:

- **internet** - syncing (required);
- **camera** - profile photo and scanning a two-step verification QR code (optional);
- **photos and files** - choosing a profile photo, QR code, or attachment, plus import and export (optional);
- **biometrics** (Face ID, fingerprint) - unlocking your vault; your operating system handles it, and the App only receives the result ("yes" or "no"), never biometric data (optional);
- **NFC** - reading a code from a YubiKey (optional);
- **autofill** - filling in sign-ins in other apps and websites (optional).

Children

You can use Inlockly on your own if you're at least 16 years old. Younger people may use the App with the consent of a parent or legal guardian – in practice, in a family group that the parent or guardian adds them to and for which they're responsible.

Security

We encrypt your vault on your device (AES-256-GCM, with the key derived from your master password using Argon2id). Data on our servers is protected by access controls, network isolation, and encryption. Only people who need access to account data to run the service have it. For details, see our Security Whitepaper.

Changes to this Policy

We update this Policy when the App, our providers, or the law change. The current version is always on this page. We'll notify you of material changes by email or in the App before they take effect. Previous versions are available on this page.