inlockly

LEGAL

Cookie Policy

Which cookies and similar technologies the Inlockly™ website and app use, what they're for, and how you can manage them.

Version 2.1 · November 2, 2026

© 2026 Inlockly™ · All rights reserved

Contents

01 Summary 3

02 What cookies and similar technologies are 3

03 Website (inlockly.com) 3

04 App (app.inlockly.com, apps, and extensions) 4

05 How to manage files 6

06 Changes to this Policy 7

Cookie Policy (the "**Policy**"), version 2.1, effective November 2, 2026. The controller is IMPERIT Dawid Łukaszek, ul. Mireckiego 26A/38, 42-208 Częstochowa, Poland ("**IMPERIT**"). Contact: privacy@inlockly.com.

Summary

We don't use analytics, advertising, or tracking cookies. Our website and App only store what they need to work and to remember your settings in your browser or on your device. That's why we don't ask for cookie consent - under Article 399 of the Polish Electronic Communications Law of July 12, 2024 (implementing the EU ePrivacy Directive), strictly necessary storage doesn't require consent.

What cookies and similar technologies are

Cookies are small text files a website stores in your browser. Browser storage (Local Storage, IndexedDB) and app storage on your device work similarly. In this Policy, we call them all "files."

Website (inlockly.com)

File	Type	Purpose	How long
`theme`	Local Storage	remembers your chosen theme (light or dark)	until you change the setting or clear your browser data

The website doesn't set cookies. Two elements come from other companies:

- **YouTube videos** only load after you click play, from `youtube-nocookie.com` (privacy-enhanced mode). After you click, YouTube (Google Ireland Ltd.) may store its own files under the Google Privacy Policy.

- **The service status badge** in the footer is served by Better Stack (`status.inlockly.com`), which receives your IP address. The badge doesn't set cookies.

App (app.inlockly.com, apps, and extensions)

The App stores files on your device that it needs for sign-in, security, autofill, and offline use. None of them are used for analytics or advertising.

Sign-in and security

File	Purpose	How long
`session.token`, `session.profile`	keeping you signed in and basic profile data	until you sign out
`session.remember_token`	"remember this device" - skipping two-step verification on a trusted device; a regular sign-out doesn't remove it, so your next sign-in on this device skips the second step	30 days from last use; it stops working earlier after a forced sign-out, when the device is signed out from another device, when your master password is changed on another device, or after account recovery
`device.fingerprint`	a random installation ID (not a device fingerprint) sent to our server; used for your device list and new-device sign-in alerts	until you clear the App's data

File	Purpose	How long
`unlock.email`, `unlock.hmac`	unlocking your Vault on this device (a verifier, not your password)	until you sign out
Biometric unlock secret (Keychain, Android Keystore, TPM)	unlocking your Vault with biometrics; the secret is protected by your device's operating system (optional)	until you turn off biometrics, sign out, or change your master password
Browser extension session storage	keys of your unlocked Vault and a pending two-step sign-in; kept in browser memory only, never on disk	keys - until the extension locks (by default, when you close the browser); two-step sign-in - 10 minutes at most

Vault, autofill, and settings

File	Purpose	How long
Vault storage (IndexedDB / app storage)	an encrypted copy of your Vault for offline use and fast syncing; it stays after you sign out so unsynced changes aren't lost	until a different account signs in on this device, or you clear your browser or App data
Autofill login copy (iOS, Android)	encrypted logins your system's autofill suggests in other apps, plus a queue of logins saved from autofill	until you sign out

File	Purpose	How long
Autofill unlock memory (phone)	so you don't have to unlock your Vault for every autofill	15 minutes by default; adjustable from "every time" to 4 hours
Website icon cache (IndexedDB)	icons shown next to items, so they don't have to be downloaded again	until you clear your browser data
`ui.language`	your chosen language	until you change the setting
`ui.vaults`, `autofill.*`, `biometric.offered`, panel and widget state	settings on this device: selected vaults, autofill, whether biometric unlock has been offered, view layout	until you change the setting
`billing.*`	completing a purchase after you return from the payment page	until the purchase is complete

The copies of your Vault and logins on your device are encrypted with a key that isn't stored in browser storage. If you turn on biometric unlock, the secret needed to unlock is stored and protected by your device's operating system.

Stripe's payment pages and the app stores store their own files under their own policies.

How to manage files

You can delete or block files in your browser settings (usually Settings → Privacy → Cookies and site data) or by clearing the app's data in your system settings. Blocking the App's files will prevent you from signing in, and deleting them will sign you out on that device - the data in your Vault stays safe on our servers.

Changes to this Policy

If we start using new files, we'll update this Policy. If they require consent (for example, analytics), we'll ask before storing them.