LEGAL

Data Processing Agreement

The data processing agreement (Article 28 GDPR) for companies and organizations that store data about their employees and contractors in Inlockly™ on the Team or Business plan.

Version 2.0 · October 26, 2026

© 2026 Inlockly™ · All rights reserved

Contents

01 § 1. Parties and conclusion 3

02 § 2. Subject matter and scope 3

03 § 3. IMPERIT's obligations 4

04 § 4. Security 5

05 § 5. Sub-processors 5

06 § 6. International transfers 6

07 § 7. Audits 6

08 § 8. Personal data breaches 6

09 § 9. Termination and deletion 7

10 § 10. The Controller's obligations 7

11 § 11. Liability and final provisions 7

© 2026 Inlockly™ · inlockly.com

Data Processing Agreement (the "**DPA**"), version 2.0, effective October 26, 2026. It forms part of the agreement for Inlockly™ services concluded under our Terms of Service.

§ 1. Parties and conclusion

1. The parties are:

a) the **Controller** – the Business (company or organization) using a Group on the Team or Business plan;

b) the **Processor** – IMPERIT Dawid Łukaszek, ul. Mireckiego 26A/38, 42-208 Częstochowa, Poland, Tax ID (NIP): 9492259428 ("**IMPERIT**").

2. This DPA is concluded when the Team or Business plan is purchased (by accepting the Terms) and remains in effect for as long as the Group's Subscription, and after it ends – until the data is deleted under § 9.

3. At the Controller's request, the parties may sign this DPA in documentary or written form on the same terms – email privacy@inlockly.com.

4. Capitalized terms have the meanings given in the Terms and in the GDPR (Regulation (EU) 2016/679).

§ 2. Subject matter and scope

1. The Controller entrusts IMPERIT with processing personal data to the extent and for the purpose necessary to provide Inlockly™ services in the Controller's Group.

2. **Data subjects:** Group members (the Controller's employees, contractors, and associates), people invited to the Group, and people whose data the Controller or members store in Group items.

3. **Types of data:**

a) Group member data: first and last name, email address, profile photo, role, department, and permissions in the Group;

b) Group activity data: the Group activity log, members' sign-in activity (time, device, IP address, approximate location), and - on the Business plan - the item usage log (viewing, revealing or copying a password, copying a 2FA code, autofill, printing);

c) Group item contents - only in end-to-end encrypted form, with no IMPERIT access to the keys.

4. **Nature of processing:** storage, syncing, transmission, making data available to members according to their permissions, display in the management console, and deletion.

5. This DPA doesn't cover data for which IMPERIT is the controller (user accounts, billing, service security) - see our Privacy Policy.

§ 3. IMPERIT's obligations

IMPERIT:

a) processes data only on the Controller's documented instructions; the Terms, this DPA, and the Controller's settings and actions in the App are its instructions. If EU or Polish law requires processing, IMPERIT will inform the Controller before processing unless the law prohibits it;

b) promptly informs the Controller if, in IMPERIT's opinion, an instruction infringes data protection law;

c) ensures that people authorized to process the data are bound by confidentiality;

d) implements the security measures in § 4;

e) assists the Controller in responding to data subject requests (Articles 15-22 GDPR), primarily through App features (viewing, changing, and removing members and data, export), and otherwise on request;

f) assists the Controller in meeting its obligations under Articles 32-36 GDPR (security, breach notification, impact assessments, consultations), taking into account the nature of processing and the information available;

g) makes available the information necessary to demonstrate compliance with Article 28 GDPR and allows audits under § 7.

§ 4. Security

1. IMPERIT implements technical and organizational measures appropriate to the risk, in particular:

a) end-to-end encryption of item contents on users' devices (AES-256-GCM, Argon2id, RSA-OAEP) - IMPERIT has no access to the keys;

b) encryption in transit (TLS) and of data stored on servers;

c) least-privilege access control to systems, multi-factor authentication for staff, and network isolation;

d) backups and availability monitoring;

e) security event logging and abuse protection (attempt limits, two-step verification).

2. Our security model is described in our Security Whitepaper.

§ 5. Sub-processors

1. The Controller gives general authorization for IMPERIT to engage sub-processors. Current sub-processors processing data covered by this DPA:

Sub-processor	Scope	Location
Amazon Web Services EMEA SARL	servers, database, file storage, email delivery	EU (Frankfurt)
Yubico AB	verifying members' YubiKey codes	EU (Sweden)
IPinfo, Inc.	looking up the country of an IP address when the local database isn't enough	US
Atlassian Pty Ltd	handling support requests	EU and US

2. IMPERIT will notify the Controller by email (to the Group Owner's address) at least 14 days before adding or replacing a sub-processor. During that time, the Controller may raise a reasonable objection; if the parties can't agree, the Controller may terminate the services agreement effective on the date of the change and receive a proportional refund.

3. IMPERIT imposes the same data protection obligations on sub-processors as in this DPA and remains liable for them as for its own actions.

§ 6. International transfers

Data transferred to countries outside the European Economic Area (§ 5) is protected by a European Commission adequacy decision (the EU-US Data Privacy Framework) or standard contractual clauses (Articles 45-46 GDPR).

§ 7. Audits

1. The Controller may verify compliance with this DPA, primarily based on information and documentation provided by IMPERIT (including answers to security questionnaires).

2. If that information isn't sufficient, the Controller may conduct an audit - itself or through an independent auditor bound by confidentiality - with at least 14 days' notice, on business days, no more than once a year (unless there has been a personal data breach or a supervisory authority requires it). An audit may not compromise the security of other customers' data or include access to encryption keys. The Controller bears the cost of the audit.

§ 8. Personal data breaches

IMPERIT will notify the Controller of a personal data breach affecting data covered by this DPA without undue delay and no later than 48 hours after becoming aware of it, by email to the Group Owner's address. The notification will include the information required by Article 33(3) GDPR available at the time; IMPERIT will provide the rest as soon as it's known.

§ 9. Termination and deletion

1. When services for the Group end (the Group is deleted), IMPERIT deletes the data covered by this DPA after a 30-day grace period, during which the Controller can cancel the deletion and export the data. Backups are overwritten in the normal cycle within no more than 35 days.

2. Before deletion, the Controller can export the data using App features. On request, IMPERIT will confirm deletion.

3. The deletion obligation doesn't apply to data IMPERIT must retain by law.

§ 10. The Controller's obligations

The Controller:

a) is responsible for the legal basis for processing the data of members and other people whose data it stores in the Group;

b) informs Group members about the processing of their data, including the activity data visible in the management console (§ 2(3)(2));

c) uses its permissions in the Group in compliance with the law, in particular employment law.

§ 11. Liability and final provisions

1. The parties' liability for breaching this DPA is governed by Article 82 GDPR; otherwise, § 16 of the Terms applies.

2. In the event of a conflict between this DPA and the Terms regarding personal data protection, this DPA prevails.

3. Changes to this DPA are made in the same way as changes to the Terms (§ 20 of the Terms).

4. This DPA is governed by Polish law; disputes are resolved by the court with jurisdiction over IMPERIT's registered office.

© 2026 Inlockly™ · inlockly.com

© 2026 Inlockly™ · inlockly.com