DRIMT a Co-Labs Group product

Data Processing Agreement

GDPR Article 28 · Version 1.1 · 15 November 2026

Parties

Processor: Co-Labs SRL (publisher of Drimt), 12 Cantersteen Street, 1000 Brussels, Belgium, company number BE0790543664.

Controller (customer): fill in below.

COMPANY NAME

REGISTERED ADDRESS

COMPANY / VAT NUMBER

This Data Processing Agreement (“DPA”) forms part of the Terms of Service (drimt.ai/terms) (the “Agreement”) between Co-Labs SRL, 12 Cantersteen Street, 1000 Brussels, Belgium, company number BE0790543664, publisher of Drimt (“Processor”, “we”), and the business customer using Drimt (“Controller”, “you”). It applies automatically to every paid or trial workspace and takes precedence over the Agreement for anything relating to personal data.

1. Definitions

Terms such as “personal data”, “processing”, “controller”, “processor”, “data subject” and “personal data breach” have the meaning given in Regulation (EU) 2016/679 (“GDPR”). “Customer Data” means personal data you or your users submit to Drimt, including logs, documents, integrations data and user accounts.

2. Roles and scope

You are the controller of Customer Data and we process it as your processor. We are a separate controller only for our own account management, billing and website data, as described in our Privacy Policy (drimt.ai/privacy). Annex 1 describes the processing.

3. Your instructions

- We process Customer Data only on your documented instructions: the Agreement, this DPA, and your configuration and use of Drimt.
- We tell you without delay if we believe an instruction breaks the GDPR or other EU or Member State law.
- If EU or Member State law requires other processing, we tell you first, unless that law forbids it.
- You are responsible for having a lawful basis for the Customer Data you submit.

4. Confidentiality

Everyone we authorize to process Customer Data is bound by confidentiality obligations and only accesses it as needed to provide, secure or support the service.

5. Security

We implement the technical and organizational measures in Annex 2, appropriate to the risk under Article 32 GDPR. We may update them as long as the overall level of protection does not decrease.

6. Subprocessors

- You give general authorization for the subprocessors listed on our Subprocessors (drimt.ai/subprocessors) page (Annex 3).
- We inform you of any intended addition or replacement at least 30 days in advance, by email or in-app. You may object on reasonable data protection grounds within that period. If we cannot address your objection, you may terminate the affected service. No refund is due for fees already paid.
- We impose on each subprocessor data protection obligations at least as protective as this DPA and remain liable to you for their performance.

7. International transfers

Customer Data is hosted in the European Union. Where a subprocessor processes it outside the European Economic Area, we rely on an adequacy decision (including the EU-U.S. Data Privacy Framework) or the European Commission’s Standard Contractual Clauses, with supplementary measures where needed. AI providers receive anonymized inputs only.

8. Assistance

- **Data subject requests:** we help you answer requests to exercise GDPR rights, mainly through in-app export and deletion tools. If a data subject contacts us directly, we forward the request to you and do not answer it ourselves unless you ask us to.
- **Impact assessments and consultations:** we give reasonable help with data protection impact assessments and prior consultations with supervisory authorities (Articles 35 and 36 GDPR).

9. Personal data breaches

We notify you without undue delay, and in any case within 48 hours, after becoming aware of a personal data breach affecting Customer Data. The notice describes, as far as known, the nature of the breach, the categories and approximate number of data subjects and records, the likely consequences, and the measures taken or proposed. We give updates as more information becomes available and help you meet your own notification duties under Articles 33 and 34 GDPR.

10. Return and deletion

You can export Customer Data at any time while your workspace is active. When the Agreement ends, we delete Customer Data within 90 days, unless EU or Member State law requires us to keep it. Backups are overwritten on their normal cycle.

11. Audits

We make available all information needed to demonstrate compliance with Article 28 GDPR, including security documentation and the results of independent assessments when available. If that is not enough, we allow and contribute to audits, including inspections, by you or an independent auditor you appoint who is bound by confidentiality. Audits are agreed in advance, with reasonable notice, and run without disrupting the service.

12. Liability, term and law

Liability under this DPA follows the limits in the Agreement, except where the GDPR does not allow them. This DPA lasts as long as we process Customer Data on your behalf. It is governed by the same law and courts as the Agreement.

Annex 1 — Description of the processing

- **Subject matter and purpose:** providing the Drimt platform: collecting and analysing security logs and documents, risk and compliance assessments (NIS2, DORA, ISO 27001, GDPR, EU AI Act), reporting, and support.
- **Nature:** collection, storage, anonymization, analysis (including AI-assisted analysis), retrieval, export and deletion.
- **Duration:** the term of the Agreement plus the deletion period in section 10.
- **Data subjects:** your employees, contractors and users; people appearing in logs or documents you submit, such as customers, suppliers or end users of your systems.
- **Categories of data:** names, business contact details, account and user IDs, IP addresses, device and log data, and any personal data contained in documents you upload.
- **Special categories:** none intended. Do not submit them unless strictly needed and agreed with us in writing.

Annex 2 — Technical and organizational measures

- Hosting in the European Union.
- Encryption in transit (TLS) and at rest.
- Anonymization of logs by our Crypto Anonymization Engine before any AI analysis.
- Workspace isolation and row-level access controls, so each customer only reaches its own data.
- Role-based access for staff, on a need-to-know basis, with two-step sign-in.
- Bot protection on public forms and DDoS protection at the network edge.
- Regular backups, with restores tested so data can be recovered after an incident.
- Logging and monitoring of access to production systems.
- Security controls aligned with ISO 27001, reviewed regularly.
- Incident response procedure, including the breach notice in section 9.

Annex 3 — Subprocessors

Subprocessors in use on 15 November 2026. Later changes follow section 6 and are published at drimt.ai/subprocessors.

Subprocessor	Purpose	Location	Transfer safeguard
Lovable	Website and application hosting, database, sign-in, file storage, visitor analytics and AI gateway	European Union	GDPR (EU processing)
Supabase	Database and authentication infrastructure behind our hosting platform	European Union	GDPR (EU processing)
Cloudflare	Content delivery, edge hosting, DDoS protection and Turnstile bot checks on forms	Global edge network (EU and United States)	Standard Contractual Clauses, EU-U.S. Data Privacy Framework
Stripe	Payment processing, subscriptions, invoicing and tax	Ireland and United States	Standard Contractual Clauses, EU-U.S. Data Privacy Framework
Resend	Transactional emails (demo confirmations, contact replies, pitch deck delivery)	United States	Standard Contractual Clauses
Google (Gemini)	AI analysis and report generation, via our hosting provider's AI gateway	European Union and United States	Standard Contractual Clauses, EU-U.S. Data Privacy Framework
OpenAI	AI analysis, EU AI Act readiness assessment and text embeddings, via our hosting provider's AI gateway	United States	Standard Contractual Clauses, EU-U.S. Data Privacy Framework

Subprocessor	Purpose	Location	Transfer safeguard
Cal.com	Booking demo calls and meetings	European Union and United States	Standard Contractual Clauses

Signatures

Signed in two copies, each party keeping one. The customer signs first and emails the signed PDF to privacy@drimt.ai; Co-Labs SRL countersigns and returns the final copy. Data protection questions: privacy@drimt.ai.

For the Processor

Co-Labs SRL (publisher of Drimt)

NAME

Daniel Sum

TITLE

Administrator & DPO

DATE

PLACE

Brussels

SIGNATURE

For the Controller

The customer named on page 1

NAME

TITLE

DATE

PLACE

SIGNATURE