

Data Processing Agreement

Flatfight · Last updated 2 October 2026

This Data Processing Agreement ("DPA") covers the personal data we process for your business when you use Flatfight. It meets Article 28 of the GDPR, forms part of our [Terms of Service](#), and applies automatically when you accept them. No signature is needed. If your procurement process needs a signed copy, download the PDF, sign it and email it to privacy@flatfight.com, and we will countersign it.

1. Parties and roles

The **customer** is the business that holds the Flatfight account. It is the controller of the personal data described in Annex I. The **processor** is:

Dripwork
Business ID (Y-tunnus) 3519918-7
Ylioppilaantie 6, 90130 Oulu, Finland
privacy@flatfight.com

Terms such as "personal data", "processing", "controller", "processor", "data subject" and "personal data breach" have the meanings given in the GDPR. Where the customer is itself a processor for another controller, we act as its sub-processor on the same terms.

This DPA does not cover data for which we are a controller, such as your team's account details, sign-in records and billing records. Our [Privacy Policy](#) covers those.

2. Processing only on your instructions

We process the personal data only on the customer's documented instructions. These instructions are:

- the Terms of Service and this DPA;
- the customer's use and configuration of Flatfight, for example connecting Stripe, sending activity data, approving a submission, turning on autopilot or choosing a retention period;
- other written instructions that are consistent with the Terms.

We process the data otherwise only where EU or Member State law requires it, and in that case we tell the customer first unless that law forbids it. We will tell the customer if, in our opinion, an instruction infringes data protection law. We never sell the personal data, use it for our own purposes, or use it to train AI models.

3. Confidentiality

Only people who need access to provide, secure or support Flatfight can access the personal data, and they are bound by confidentiality. Today that is Dripwork's own staff only.

4. Security

We implement the technical and organisational measures in Annex II, taking into account the state of the art, the cost, the nature of the processing and the risks to data subjects (Article 32). We may update these measures as long as the overall level of protection does not decrease.

5. Subprocessors

The customer gives general authorisation for us to use subprocessors. The current subprocessors are listed in Annex III and on our [security page](#). Before we add or replace a subprocessor, we notify the account owner by email at least 30 days in advance. The customer may object on reasonable data protection grounds within that period. If we cannot address the objection, the customer may end the agreement before the change takes effect and receive a refund of fees prepaid for the period after it ends.

We impose data protection obligations on each subprocessor that are no less protective than this DPA, and we remain responsible to the customer for their performance.

6. International transfers

We host and back up personal data in the EU. Where a subprocessor processes personal data outside the European Economic Area, the transfer is covered by the European Commission's Standard Contractual Clauses (Module 3, processor to processor) or by an adequacy decision, together with any supplementary measures needed. Annex III shows the safeguard for each subprocessor.

7. Helping you meet your obligations

- **Data subject requests.** If a cardholder contacts us directly, we refer them to the customer and do not answer on the customer's behalf unless instructed. The customer can find, export and delete data from the app. Where it cannot, we help within a reasonable time.
- **Impact assessments.** We give the customer the information it reasonably needs for a data protection impact assessment or a prior consultation with a supervisory authority about Flatfight.

8. Personal data breaches

We notify the customer without undue delay, and in any case within 48 hours, after becoming aware of a personal data breach affecting its data. The notice includes the information Article 33(3) requires, as far as it is available, and we update it as we learn more. We take reasonable steps to contain the breach and limit its effects. Notifying the customer is not an admission of fault.

9. Deletion and return

- The customer can export its data as a ZIP file at any time from Settings.

- Decided disputes, evidence and activity data are deleted automatically after the retention period the customer chooses. Open disputes are kept until they are decided.
- When the customer deletes its account, we delete its personal data from our live systems immediately. Copies in encrypted backups are overwritten within 60 days, and we never restore them into the live service except to recover from a disaster.
- When the customer disconnects Stripe, we delete the stored Stripe credentials immediately.

10. Audits

We make available the information needed to show compliance with Article 28, including answers to reasonable security questionnaires (once a year, or more often after a breach). If that is not enough, the customer may have an independent auditor, bound by confidentiality, audit our compliance. The customer must give 30 days' notice, the audit must not cover other customers' data, and the customer bears the cost. Audits are limited to once every 12 months unless a supervisory authority requires one or there has been a personal data breach.

11. Liability

Each party's liability under this DPA is subject to the limits in the Terms of Service, except where those limits cannot apply under the GDPR. Nothing in this DPA limits a data subject's rights under Article 82.

12. Duration, precedence and law

This DPA applies for as long as we process personal data for the customer. If it conflicts with the Terms on data protection, this DPA prevails. If it conflicts with Standard Contractual Clauses that apply to a transfer, those Clauses prevail. This DPA is governed by Finnish law, and the Oulu District Court has jurisdiction, as in the Terms.

Annex I: Details of processing

Subject matter	Preparing, scoring and submitting responses to the customer's Stripe payment disputes.
Duration	For the term of the agreement, then until deletion under section 9.
Nature	Collection from Stripe and from the customer, storage, organisation, analysis, drafting with an AI model, generation of PDF documents, transmission to Stripe on approval, and deletion.
Purpose	To let the customer contest disputes and accept weak cases, and to report on outcomes.
Data subjects	The customer's customers (cardholders and users of the customer's product), and people whose messages the customer uploads.

Categories of data	Name, email address, billing and shipping address; purchase IP address; card checks (AVS, CVC, 3D Secure), card brand, last four digits and fingerprint (no full card numbers); payments, subscriptions, invoices and refunds; product activity such as logins, downloads and usage, with time, IP address, user agent, device and account identifiers; customer messages; the customer's policies; dispute details and evidence.
Special categories	None intended. The customer must not send special category data.
Frequency	Continuous, for as long as Stripe is connected.
Retention	Set by the customer: 6 to 36 months after a dispute is decided (default 18).

Annex II: Technical and organisational measures

Hosting and network

- Production servers and backups in the EU (Helsinki, Finland). Firewall open only for SSH, HTTP and HTTPS; SSH by key only; brute-force protection; automatic security updates.
- All traffic over HTTPS (TLS), with HTTP Strict Transport Security.

Encryption

- Stripe access tokens, refresh tokens and restricted keys are encrypted at rest with authenticated encryption (Fernet: AES-128 with HMAC-SHA256). The keys are kept outside the database and can be rotated.
- Activity API keys and sign-in links are stored only as hashes.
- Backups are encrypted with age to an offline key before they leave the server, and each has a checksum.

Access control and isolation

- Sign-in by single-use email links that expire after 15 minutes. Sessions can be revoked.
- Every data query is scoped to the signed-in customer, and stored files can only be read from that customer's own folder.
- The Stripe permissions requested are the minimum needed. Flatfight cannot move money, create charges or issue refunds.
- Production access is limited to the operator.

Integrity and accountability

- Append-only audit log of submissions, acceptances, edits, connection and setting changes, protected by a database trigger.
- Evidence is sent to Stripe only in one explicit submission after approval, never staged in advance.
- AI drafts are checked against the gathered facts. Sentences that cite facts we do not hold are rejected.
- Content Security Policy, CSRF protection and secure cookies in the web app.

Data minimisation and confidentiality

- Application logs and error reports record events and identifiers, not request bodies, and secrets are redacted from them automatically. Job queues carry identifiers only.
- Web server logs exclude query strings, cookies and authorisation headers, and are deleted after 30 days.
- The free calculator processes keys and dispute data in memory only.

Availability and recovery

- Nightly encrypted backups, kept 14 days (daily) and 8 weeks (weekly). Restores are tested.
- Health checks and error monitoring.

Annex III: Subprocessors

Subprocessor	Purpose	Personal data	Location	Transfer safeguard
Hetzner Hetzner Online GmbH, Gunzenhausen, Germany	Hosting of the application, database, generated files and encrypted backups	All service data	Helsinki, Finland (EU)	Within the EEA
Anthropic Anthropic, PBC, San Francisco, United States	Drafting the written summary of an evidence package from the facts we gathered	Facts for the dispute being drafted: may include the customer's name, email, IP address, billing address, activity events, policy text and message excerpts	United States	Standard Contractual Clauses
Resend Plus Five Five, Inc., San Francisco, United States	Sending sign-in links and dispute notifications to your team	Your team's email addresses and notification text (amount, reason, deadline). No customer contact details	EU sending region (Ireland); provider based in the United States	Standard Contractual Clauses
Sentry Functional Software, Inc., San Francisco, United States	Error monitoring	Technical error reports. Request bodies, cookies and secrets are stripped before sending	EU data region (Germany); provider based in the United States	Standard Contractual Clauses

Customer (controller)

Company:

Processor

Dripwork

Name and title:

Signature and date:

Name and title:

Signature and date:
