LEGAL

Data Processing Addendum

For Team and Enterprise customers who need it: the terms on which we process personal data on your organisation's behalf.

ON THIS PAGE

1. Parties and how this addendum applies
2. Subject matter, duration, nature and purpose
3. Categories of data and data subjects
4. Our obligations as processor
5. Sub-processors
6. Security
7. Assistance
8. Personal data breaches
9. Audits
10. Deletion and return
11. International transfers
12. Liability and precedence
13. Annex: contacts

Version: 1.1

Effective date: 11 October 2026

Last updated: 28 October 2026

The short version

- This addendum is for **Team and Enterprise** customers whose organisation needs a data processing agreement with us.
- It covers only the personal data we process **on your organisation's behalf** — the administrator and billing contact details you give us and, if you use it, single sign-on data. Licensing data (licence id, plan, machine fingerprints, machine list, version, request IP addresses) is not covered: Cotterpin is its controller. It does not cover your code: Cotterpin never receives it.
- We use only the sub-processors listed on our Sub-processors page, tell you before adding one, and delete your data when the subscription ends.

1. Parties and how this addendum applies

This Data Processing Addendum ("**DPA**") is between **Cotterpin Technologies Ltd** (company number 17498532, registered office 18 Massingberd Way, London, SW17 6AB) as **processor**, and the Team or Enterprise customer ("**Customer**") as **controller**. It forms part of our Terms of Service or, for Enterprise, the written agreement between us (the "**Agreement**"). It applies when the Customer accepts it in writing, by signing a copy or by email to legal@cotterpin.io, and we confirm by reply.

Where C r's Team or and bug reports (sending for) — ou tomatic

May we use Google Analytics cookies to count visits and see which pages help? Nothing is set unless you accept, and you can change your mind any time. Cookie Policy

bug reports for its repositories (`bugAutoSend: forbidden` in a repository's Cotterpin policy); see the Privacy Policy.

2. Subject matter, duration, nature and purpose

- **Subject matter:** providing the Team or Enterprise plan under the Agreement.
- **Duration:** the term of the Agreement, plus the deletion period in section 10.
- **Nature:** storing, retrieving and using the data below to administer the Customer's account and, once available, to sign people in through the Customer's identity provider.
- **Purpose:** only to provide the service, on the Customer's documented instructions, which are the Agreement and this DPA.

3. Categories of data and data subjects

DATA SUBJECTS	PERSONAL DATA
The Customer's administrators and billing contacts	Contact details the Customer gives us for support and administration
The Customer's people signing in through single sign-on	The identity provider's stable identifier for the person, their email address, and their Team membership (the machines bound to their seat, and whether they are an administrator or revoked). Provider sign-in tokens are kept only until the person's machine collects them; an uncollected one stops working after 10 minutes and is deleted automatically about an hour later.

Licensing data is not processed under this DPA: Cotterpin is the controller of it (see section 1). A Team licence is a number of seats with up to three machine fingerprints per seat. Without single sign-on, the licence service attaches no person's identity to a seat; with it, a seat is assigned to the identity the Customer's provider confirms, and that identity data is processed under this DPA (the table above).

No special category data is processed. **No source code, diffs, prompts, test output, reports or receipts** are processed: they never leave the Customer's machines except to the model provider the Customer chose, under the Customer's own account.

4. Our obligations as processor

We will:

- process the personal data only on the Customer's documented instructions, and tell the Customer if we think an instruction breaks data protection law;
- ensu
- take t
- use s
- assist the Customer as set out in section 7;

May we use Google Analytics cookies to count visits and see which pages help? Nothing is set unless you accept, and you can change your mind any time. Cookie Policy

- delete or return the data at the end of the service (section 10);
- make available the information needed to show compliance, and allow audits (section 9).

5. Sub-processors

- The Customer gives general authorisation for the sub-processors on our Sub-processors page.
- We will tell the Customer at least 30 days before adding or replacing a sub-processor. The Customer may object on reasonable data protection grounds; if we cannot resolve the objection, the Customer may end the affected service and receive a pro-rata refund of the unused period.
- We impose on each sub-processor data protection obligations no less protective than this DPA, and remain liable to the Customer for its performance.

6. Security

Taking into account the state of the art, the cost, and the nature and risks of the processing, we maintain appropriate technical and organisational measures, including:

- licence tokens signed with keys held in AWS KMS; secrets held only in AWS Secrets Manager;
- encryption in transit (verified TLS) and at rest in the AWS services we use, including the licence database (Amazon DynamoDB, encrypted with an AWS-managed KMS key, with point-in-time recovery);
- one-way hashing of identifiers the service does not need in clear;
- least-privilege access for the licence service and for staff, with multi-factor authentication on administrative access;
- a published vulnerability disclosure process (Security and Responsible Disclosure).

7. Assistance

Taking into account the nature of the processing, we will help the Customer, by appropriate measures, to answer requests from data subjects exercising their rights, and to meet its obligations on security, breach notification, data protection impact assessments and prior consultation. We will pass any request we receive directly from a Customer's data subject to the Customer without undue delay, and will not answer it ourselves except on the Customer's instructions.

8. Personal data breaches

We will notify the Customer without undue delay, and in any case within 48 hours, after becoming aware of a personal data breach affecting the Customer's personal data. We will give the information the Customer reasonably needs to meet its own notification duties, update it as we learn more, and take reasonable steps to contain the breach.

9. Audits

We will r is DPA, starting enough, the Cust on at least 30 ach has occurred

May we use Google Analytics cookies to count visits and see which pages help? Nothing is set unless you accept, and you can change your mind any time. Cookie Policy

10. Deletion and return

When the Agreement ends, we will, at the Customer's choice, return the Customer's personal data in a common machine-readable format or delete it, within 30 days, unless law requires us to keep it. Records we keep as a controller (for example, accounting records Paddle passes to us) are governed by our Data Retention Policy.

11. International transfers

The licence service runs in AWS `eu-west-1` (Ireland). Where a sub-processor transfers the Customer's personal data out of the UK or EU, the transfer is covered by:

- for EU data, the **EU Standard Contractual Clauses** (Commission Implementing Decision (EU) 2021/914), incorporated into this DPA by reference: Module Three (processor to processor) for onward transfers by our sub-processors, with Clause 7 (docking) included, Option 2 of Clause 9 (general written authorisation, with the notice period in section 5), the optional wording in Clause 11 left out, and the law and courts of Ireland for Clauses 17 and 18;
- for UK data, the **International Data Transfer Addendum to the EU Standard Contractual Clauses** issued by the UK Information Commissioner (version B1.0), incorporated by reference, with Table 1 completed from this DPA, the clauses above as Table 2, and Annexes in Table 3 taken from sections 2, 3, 5 and 6 of this DPA;
- or an adequacy decision, where one applies.

12. Liability and precedence

Each party's liability under this DPA is subject to the limits in the Agreement, except where the law does not allow it. If this DPA and the Agreement conflict on the processing of personal data, this DPA prevails, and if the Standard Contractual Clauses or the UK Addendum conflict with either, they prevail. Nothing in this DPA limits a data subject's own rights, including the right to compensation under Article 82 of the UK GDPR and EU GDPR.

13. Annex: contacts

- **Cotterpin data protection contact:** privacy@cotterpin.io
- **Customer contact:** as given by the Customer on acceptance.

May we use Google Analytics cookies to count visits and see which pages help? Nothing is set unless you accept, and you can change your mind any time. Cookie Policy