LEGAL

GDPR Statement

How we meet the UK GDPR and the EU GDPR — starting from the fact that your code is never our data.

ON THIS PAGE

1. Which laws this covers
2. Who is responsible for what
3. How we apply the data protection principles
4. Consent first, in the product
5. Your rights, and how requests work
6. Security measures
7. Personal data breaches
8. International transfers
9. Data protection officer and EU representative
10. Complaints

Version: 1.2

Effective date: 11 October 2026

Last updated: 28 October 2026

The short version

- **Your code is never our data.** Cotterpin runs on your machine and never receives your source code, diffs or prompts. You are the controller of your code; we are neither its controller nor its processor.
- **We are the controller** of the small amount of licensing and account data that reaches us — and we designed the product so that it is as little as possible.
- **Nothing happens without asking.** Every machine measurement, every change outside your repository to your own files or your agent tools' settings, and every call to our licence service says what and why, and declining always leaves a working default.
- To use your rights, email us; we answer within one month.

1. Which laws this covers

This statement explains how **Cotterpin Technologies Ltd** meets the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and, for people in the EU and EEA, the EU General Data Protection Regulation (EU GDPR). It sits alongside our Privacy Policy, which is our full notice to you, and the Data Processing Addendum for Team and Enterprise customers.

2. Who is responsible for what

DATA	WHO IS THE CONTROLLER	OUR ROLE
Your source code, diffs, prompts, test output, reports and receipts	You (or your organisation)	**None.** It stays on your machine, or goes from your

DATA	WHO IS THE CONTROLLER	OUR ROLE
		machine straight to your own model provider. We never receive it.
What your agent or a Cotterpin task sends to your model provider (Claude, Codex, Grok or Gemini)	You, under your own account with that provider	**None.** The provider's terms govern it.
Licensing data: licence id, plan, machine fingerprint, Cotterpin version, machine list and its audit records, request IP addresses — on every plan, including Team and Enterprise	Cotterpin	Controller
Customer email address from Paddle, and any address typed for a claim (stored only as a SHA-256 hash)	Cotterpin	Controller
Support emails you send us	Cotterpin	Controller
Bug reports, sent by you or (from the next release) automatically where you turned that on; linked to your licence id, or anonymous	Cotterpin	Controller
Checkout, payment, tax and invoice data	Paddle.com Market Ltd, our merchant of record	Paddle is an independent controller; we receive what we need to provide your licence
Administrator and billing contact details your organisation gives us, and sign-in data once Team single sign-on is live	Your organisation	Processor, under the Data Processing Addendum

3. How we apply the data protection principles

- **Data minimisation by design.** For licensing, the software sends only the licence id, plan, machine fingerprint and version. The fingerprint is `mfp_` + HMAC-SHA256 of the machine's stable hardware id under a fixed product salt, computed on your machine; the hardware id itself is never stored or sent. Email addresses are kept only as SHA-256 hashes.
- **Purpose limitation.** Licensing data is used to issue and check licences, enforce machine limits, and protect the service. It is not used for marketing or profiling.

- **Lawfulness and transparency.** Our lawful bases are listed for each kind of data in the Privacy Policy. `cotterpin privacy` prints, on your machine, exactly what leaves it.
- **Storage limitation.** Each kind of data has a retention period in our Data Retention Policy.
- **Accuracy.** You can see and correct the machines on your licence yourself with `cotterpin machines`.
- **Integrity and confidentiality.** See section 6.
- **Accountability.** We keep a record of our processing activities (Article 30), owned by our director, and review it and this statement whenever what the software or our services collect changes.

4. Consent first, in the product

The software follows one rule: *say what we are going to do and why; the developer can approve or decline; if declined, run in serial or take the default that needs no scan.*

- Each machine measurement (cores, memory, disk, a one-second calibration run, live load) is asked about separately. Its results never leave your machine.
- Every change outside your repository to your own files or your agent tools' settings, every hook and agent-tool adapter installation, and every call to a provider or to our licence service asks first. Cotterpin's own records in its configuration directory (such as the empty guarded-session files that keep an agent session's guards on after it leaves a repository) are kept without asking; they hold nothing about your code.
- Declining is never an error: work runs one job at a time, or Cotterpin runs in Watch.
- In a non-interactive shell, anything not approved in advance counts as declined.
- `cotterpin consent` shows every answer, and `cotterpin consent revoke <id>` withdraws one.
- Telemetry is off and this release contains no telemetry sender. There is no Team or Enterprise dashboard.
- Bug reports are sent only by you, after you read them; from the next release, also automatically, but only for a repository and kind of report you turned that on for yourself (your operating system confirms it is you), never your code, and never where your organisation forbids it. `cotterpin bug-autosend off <kind>` withdraws that consent. See the Privacy Policy.

5. Your rights, and how requests work

You have the right to be informed, of access, to rectification, to erasure, to restrict processing, to data portability, to object, and not to be subject to solely automated decisions with legal or similarly significant effects (we make none).

1. **Ask.** Email privacy@cotterpin.io. You don't need to use any particular words.
2. **Help us find your records.** We store your email only as a hash and your machine only as a fingerprint, so we may ask for the email address you used, or for your licence id (shown by `cotterpin machines`). We ask only for what we need to confirm it is you.
3. **Timeline.** We acknowledge your request within 5 business days and answer within one month of receiving it. For complex or numerous requests we may extend this by up to two further months,

telling you why within the first month.

4. **Cost.** Free, unless a request is manifestly unfounded or excessive.
5. **Data held by others.** For payment data, we will pass your request to Paddle or you can contact Paddle directly at paddle.net. For what you sent your model provider, contact that provider.

Some things you can do yourself at any time: withdraw a consent with `cotterpin consent`, remove a machine with `cotterpin machines remove`, remove what Cotterpin added to a repository with `cotterpin uninstall`, remove an agent tool adapter with `cotterpin adapters uninstall` (or everything Cotterpin put on your machine with `cotterpin --uninstall`), and delete your stored consent answers by deleting `consent.json` in your Cotterpin configuration directory.

6. Security measures

- Licence tokens are signed with keys held in AWS KMS; the private keys never leave KMS.
- Paddle API and webhook secrets are held only in AWS Secrets Manager. Every Paddle notification is signature-checked, and replays are refused.
- The licence service runs in AWS `eu-west-1` (Ireland), with access limited to the actions it needs.
- Personal identifiers are stored as one-way hashes where the service does not need the original.
- Releases are signed and verified on your machine before they run.
- Only our director can reach personal data. Administrative access to our AWS account needs multi-factor authentication, and our admin page needs a Microsoft Entra ID sign-in that only the director's account can complete. Anyone who joins us later will get access only to what their role needs, and will be bound in writing to keep personal data confidential.

See our Security page and Security and Responsible Disclosure Policy.

7. Personal data breaches

If we become aware of a personal data breach, we will contain it, assess the risk and record it. Where it is likely to result in a risk to people's rights and freedoms, we will notify the ICO (and, where the EU GDPR applies, the relevant EU authority) within **72 hours** of becoming aware of it. Where the risk is high, we will also tell the people affected without undue delay. Team and Enterprise customers are notified as set out in the Data Processing Addendum.

8. International transfers

How data moves between countries, and the safeguards we rely on, is in the Privacy Policy and the Sub-processors list.

9. Data protection officer and EU representative

- **Data protection officer:** we are not required to appoint one. Our director is responsible for data protection and reads privacy@cotterpin.io.
- **EU representative (Article 27 EU GDPR):** we are appointing a representative in the EU, and will name them here. Until then, people in the EU can contact us directly at privacy@cotterpin.io.
- **ICO registration number:** ZC266082

10. Complaints

You can complain to the Information Commissioner's Office at ico.org.uk, or, in the EU and EEA, to the data protection authority where you live or work. We would appreciate the chance to put things right first.