LEGAL

Privacy Policy

Cotterpin runs on your machine. This policy says exactly what personal data reaches us, why, how long we keep it, who else is involved, and what never leaves your machine at all.

ON THIS PAGE

1. Who is responsible
2. Asking first
3. The software: licensing
4. Your code and your model provider
5. What stays on your machine
6. Telemetry
7. Payments and Paddle
8. This website
9. Support and email
10. Who processes data for us
11. International transfers
12. How long we keep it
13. Security
14. Your rights
15. Children
16. Changes to this policy
17. Contact and complaints

Version: 1.2

Effective date: 11 October 2026

Last updated: 28 October 2026

The short version

- **To Cotterpin, for licensing, only:** your licence id, plan, a fingerprint of your machine (a keyed hash computed on your machine — never the hardware id itself) and the Cotterpin version. Only after you approve it.
- **Your code goes only to the model provider you choose**, under your own account, after you approve it. It never comes to us.
- **Telemetry is off.** This release contains no telemetry sender, and there is no Team or Enterprise dashboard.
- **This website runs Google Analytics only if you accept it** in its cookie notice; otherwise it sets no cookies of its own. See the Cookie Policy.
- **Card details never reach us.** Paddle, our merchant of record, takes payment in its own checkout.
- For every paid customer, our licence service keeps only a SHA-256 **hash** of the email address Paddle gives us (and, if you claim a purchase, of the address you type).

1. Who is responsible

Cotterpin Technologies Ltd (company number 17498532, registered office 18 Massingberd Way, London, SW17 6AB) is the controller of the personal data described in this policy, under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 and, where it applies

to you, the EU General Data Protection Regulation (EU GDPR). Our ICO registration number is ZC266082. We are appointing a representative in the EU under Article 27 of the EU GDPR and will name them here; until then, people in the EU can contact us directly at privacy@cotterpin.io.

We are **not** the controller or processor of your source code: it never reaches us (section 4). How we meet the GDPR, and how to use your rights, is set out in our GDPR Statement.

For payments, **Paddle.com Market Ltd** is our merchant of record and is a separate controller of the data it collects at checkout (see section 7).

Privacy questions: privacy@cotterpin.io.

2. Asking first

The Cotterpin software follows one rule before it measures your machine, contacts our licence service or sends anything to a model provider:

> "We MUST ALWAYS say WHAT we are going to do and WHY we need to do it. The developer can approve/decline. If decline, then we run in serial or always take the unscanned, default option."

Each request names what will be read or sent, where from, why, and what happens if you decline. Declining is never an error: machine measurements fall back to running one job at a time, and licensing falls back to Watch. In a non-interactive shell, anything you have not approved in advance counts as declined. You can see and change every answer with `cotterpin consent`, and `cotterpin privacy` prints the equivalent statement on your machine.

Machine measurements (processor cores, memory, disk, a one-second calibration run and live load) are used only on your machine to decide how much work to run at once. **Their results are not sent to us.**

3. The software: licensing

When you approve it, the software contacts our licence service to register your machine (the first time you subscribe or link it to the dashboard), subscribe, manage machines, open billing or fetch an update (`cotterpin init`, `subscribe`, `machines`, `billing`, `update --fetch`).

DATA	WHY	LAWFUL BASIS
Licence id and plan (inside the licence token we issued)	To know which licence and plan apply	Contract
Machine fingerprint: `mfp_` + HMAC-SHA256 of the machine's stable hardware id (`IOPlatformUUID` on macOS, `/etc/machine-id` on Linux) under a fixed product salt, computed on your machine	To register a machine once, identify it at checkout, enforce the 3-machine limit, and bind a licence to a machine. The hardware id itself is never sent or stored	Contract; legitimate interests (preventing abuse of machine registration)

DATA	WHY	LAWFUL BASIS
Cotterpin version	To serve the right release and refuse incompatible requests	Contract
Machine list and an audit record of each add, move or remove	So you can manage your machines, and to keep a record of licence changes	Contract; legitimate interests (security, fraud prevention)
The source IP address of each request	Rate-limiting the public machine registration and claim routes, and protecting the service from abuse	Legitimate interests (security)
Your email address, only if you run `cotterpin subscribe --claim <email>` and approve it	To email you a one-time code (8 digits, valid 15 minutes, 5 attempts) and bind a website purchase to this machine. We store only a SHA-256 hash of the address	Contract

Nothing about your code, files, file paths, repositories or provider accounts is sent to the licence service.

The licence service runs on Amazon Web Services in the EU (Ireland) region, `eu-west-1`: licence records in Amazon DynamoDB, signing keys in AWS KMS. Website purchases are claimed with a one-time code emailed from **licences@cotterpin.io** through Amazon Simple Email Service (SES), in the same EU (Ireland) region.

The licence service also keeps two logs in Amazon CloudWatch Logs, each for 30 days: a request log holding only a request id, time, route, status and response time (no IP address, identity or request content), and a service log holding only the stage and error code of a failure. To limit abuse, it counts requests per hour against a one-way hash of the source IP address (and, for claims, of the email address); those counters expire after 2 hours. See the Data Retention Policy.

Bug reports you send (coming with the next release)

Sending bug reports to us is coming with the next release of Cotterpin; the current release sends none. This section describes how it will work, and applies from that release. We will update it if anything changes before then.

When Cotterpin stops on an internal error, finds a fault in its own working (a check it could not run, a stopped run nothing could repair, a defect a run's review found in Cotterpin itself, or a check whose findings were rejected as not real), or you run `cotterpin report-bug`, it prepares a bug report on your machine and shows it to you in full. By default it is sent to our licence service only when you

have read it and pressed **s**; cancel and it is never sent. Without automatic sending (below), nothing is sent from an agent's run or a non-interactive shell: the report waits there until you review it.

- **What a report holds:** its reference; the Cotterpin, language pack and Python versions, your operating system and processor family; for an internal error, its type, the command's name and up to five lines of the trace inside Cotterpin's own code (never the error message); for a fault in Cotterpin's own working, a fixed set of fields, each from a closed list Cotterpin defines: the kind of fault, the route, stage and check it happened in, Cotterpin's own refusal codes, the language packs and agent tools in use with their versions, counts and durations, and a fingerprint (a one-way hash of the failure with paths and numbers removed, so the same fault seen on different machines can be grouped without its text); the refusals Cotterpin recorded in the period you choose, each reduced to its time, rule, code, outcome, agent tool and count; and what you write about it. Your description is refused before sending if it holds a secret, a file path or code.
- **What it never holds:** your code, diffs or file contents, file paths, the commands your agent ran, prompts and agent replies, repository, branch and remote names, commit messages, user and machine names, environment variables, secrets, error messages, and the session record itself.
- **Who sent it:** with a licence, the report is linked to your licence id, so `cotterpin bug-report` can show its status and we can credit and thank you; without one, it is anonymous. To limit abuse, the source IP address is counted as a one-way hash that expires within two hours.
- **Why:** to find and fix the fault, tell you its status, and credit bug reports. **Where:** our licence service in the EU (Ireland), `eu-west-1` . If the service cannot be reached, the report stays on your machine, prepared, with the reason, and `cotterpin report-bug --draft <id>` sends it again; nothing is sent any other way.

Sending automatically, if you choose to (from the next release). The next release lets you send these reports without reviewing each one. It is off unless you turn it on.

- **Per repository and per kind.** You turn it on for one repository and one kind of report at a time (Cotterpin's own faults, checks whose findings were rejected, or internal errors) with `cotterpin bug-autosend on <kind>` . Your operating system asks you to confirm it is you, so an agent cannot turn it on for you. Nothing else is ever sent automatically, and never your code.
- **What is sent** is exactly the report described above, nothing more. A copy of every report sent automatically is kept on your machine, in an outbox in your user configuration directory, so you can read what left.
- **You can see it and stop it.** Each session tells you it is on and how many reports were sent that week. `cotterpin bug-autosend off <kind>` stops it; `cotterpin bug-autosend status` shows what is on. You can still send or discard any report by hand.
- **Your organisation can forbid it** for a repository (`bugAutoSend: forbidden` in the repository's Cotterpin policy); then no one can turn it on there.

Lawful basis: your consent — you send each report yourself, or you turn automatic sending on for a repository and kind, and you can withdraw that at any time by turning it off; and legitimate interests in protecting the service. A report, linked or anonymous, sent by hand or automatically, is kept until the fault it describes is closed, then for 12 months.

Team single sign-on

If your organisation uses Team single sign-on (Okta, Microsoft Entra ID, Google Workspace or GitHub), signing in with `cotterpin login` sends your browser to your organisation's identity provider, and our licence service checks what the provider confirms. To assign and renew your seat, it stores only:

- the provider's stable identifier for you, and your email address;
- your Team membership: the machines bound to your seat, and whether you are a Team administrator or have been revoked.

The provider's sign-in tokens are never stored by us: a sign-in record holding one is cleared the moment your machine collects it; one that is never collected stops working after 10 minutes and is deleted automatically about an hour later. Your machine renews its Team licence with your provider at least every 7 days, so someone your organisation removes at its provider stops renewing. Your organisation's client secret for the provider is held only in AWS Secrets Manager. Lawful basis: contract with your organisation, and our legitimate interest in giving its seats only to the people it confirms. These records are kept while the Team licence exists and are deleted with the licence record (see the Data Retention Policy).

4. Your code and your model provider

When a task you started needs a model, Cotterpin sends the source files that task selected, its prompt and its instructions **to the provider you chose for that job** (for example Anthropic's Claude, OpenAI's Codex or xAI's Grok), under your own subscription or API key. It asks you before sending anything to a provider; if you decline, nothing is sent.

- Before sending, Cotterpin removes `.env` files, private keys, certificate stores and credential files, and redacts recognisable secrets (provider tokens, cloud access keys, private key blocks, bearer tokens and similar).
- This data goes directly from your machine to your provider. **It does not pass through, and is not stored by, Cotterpin.** We are not a controller or processor of it.
- Your provider's own terms and privacy policy govern what it does with what it receives.
- API keys are read from the environment variable you name at the moment of the call, and are never written to a file or log.

Redaction is pattern-based: a secret with no recognisable shape, placed in a selected source file, could still be sent. Keep secrets out of source files.

Known limit. The `.env` and credential-file exclusion applies wherever a task sends a selected part of your repository. An older route of the hardened (supervised) Mac mode sends the whole tracked tree without that exclusion; until it applies the same rule, do not commit `.env` or credential files to a repository you run on that route. We will remove this note once that route applies the same rule.

5. What stays on your machine

- **Run progress and spend** — inside your repository's own git directory; never a tracked file and never sent anywhere.
- **Session reports and receipts** — in your repository.

- **Your consent answers** — in your user configuration directory, outside every repository.
- **Your licence token** — `licence.json` in the same directory, readable only by you.
- **The agent tool adapters you install** — in each tool's own user folder (for example `~/.claude/skills/cotterpin`), with a record of each install in your user configuration directory; never in a repository.
- **Guarded sessions** — one empty file per agent session that has worked in a repository set up with Cotterpin, named by that session's id, in your user configuration directory, so its guards stay on when the agent leaves the repository. It holds nothing about your code or the session's work.

We cannot see or access any of this.

Team packs (from Cotterpin 0.3.0): your team's own rules live in your repository, under `.cotterpin/packs/`, and travel through your own git. Cotterpin checks them on your machine and never uploads, stores or receives them.

6. Telemetry

Telemetry is **off**, and this release contains no telemetry sender at all. Bug reports are not telemetry: each is sent by you, or, from the next release, automatically only where you have turned that on yourself for a repository and kind (see Sending automatically). The setting exists so that anything which ever reports usage can only be turned on by you, explicitly, through `cotterpin consent`; no repository setting can turn it on for you. There is **no Team or Enterprise dashboard** in this release, so nothing is sent to one. If we ever add telemetry or a dashboard, it will be opt-in: we will update this policy first and ask you before anything is sent.

7. Payments and Paddle

Paid plans are sold by **Paddle.com Market Ltd**, our merchant of record and reseller. Paddle collects your name, email address, billing country and address, payment details and tax information at checkout, as an **independent controller** under Paddle's privacy policy. **We never receive your card or payment details.**

Paddle shares with us what we need to provide your licence and support you: your email address, the plan, number of seats, subscription status and billing periods, and order and invoice references. Our licence service stores only a SHA-256 hash of the email address, alongside the subscription state. Paddle's seller dashboard also lets us view your order details there, which we use only to administer your subscription, answer your questions and meet our legal obligations. We do not copy those order details into any other system; our admin tools only display them from Paddle when we need them.

Lawful basis: contract, and legal obligation (accounting records).

8. This website

- **Analytics, only with your consent.** If you press Accept in the cookie notice, Google Analytics 4 (Google Ireland Limited, our processor) counts visits and the pages viewed, using a random identifier for your browser in the `_ga` cookies, with your approximate location and device type. Google Analytics 4 does not log or store IP addresses. Nothing is loaded from Google until you accept, and you can withdraw at any time with “Cookie settings” in the footer. Google may process this data in the United States under the EU–US Data Privacy Framework and its UK

Extension. Google keeps this analytics data for 2 months. No advertising trackers. The site keeps your cookie choice in your browser's local storage; only our staff-only admin area uses what its sign-in needs (see the Cookie Policy).

- **Hosting.** The site is hosted on Microsoft Azure Static Web Apps. Microsoft receives your IP address and request details when you load a page, and may keep them in logs for security, under Microsoft's own retention rules. Microsoft serves the site from its global network, so the server that answers may be outside the UK. We do not use these logs to track visitors.
- **Fonts.** The Inter and JetBrains Mono fonts are served from this website itself. No page loads fonts from Google or any other third-party font service; the only third-party script is Google Analytics, and only after you accept it.
- **Checkout.** Paddle's checkout script (Paddle.js) is loaded only when you ask for a checkout — by clicking a Buy link, or when `cotterpin subscribe` opens our checkout page. Paddle then collects the data in section 7 and may set the cookies its checkout needs. See the Cookie Policy.

Lawful basis: legitimate interests (running and securing the website); consent (analytics); contract (checkout).

Founding Developers applications

If you apply for a Founding Developers place on our pricing page, we keep what the form asks: your name, your email address, the language pack, the agent tools you use, your operating system, how often you use agents, a sentence about your codebase and, if you give them, a public profile link and where you heard about us. Your email address is stored as you typed it, because we need it to send your invitation and programme emails; unlike a paying customer's address, it is not reduced to a hash.

- **Why:** to choose each cohort and run the programme. Nothing else.
- **Where:** our licence service on Amazon Web Services (see sub-processors). Your network address is used, as a one-way hash that expires within two hours, only to limit how many applications one network can send.
- **How long:** until the programme ends for you, then deleted — or sooner if you ask (privacy@cotterpin.io). If you are not offered a place, your answers are deleted 3 months after the cohort you applied for fills.
- **Applying switches nothing on.** Nothing is sent from your machine until you install Cotterpin and approve it there.

Lawful basis: steps you ask us to take before entering into an agreement (UK GDPR Article 6(1)(b)).

9. Support and email

- **Support** is by email, received through our email provider (see section 10). We process your name, email address and whatever you write to us to answer it. Lawful basis: contract, or legitimate interests if you are not a customer.
- **Security reports** sent to security@cotterpin.io are used to investigate and fix the issue, and to credit you if you wish.

- **Licence claim codes** are emailed through Amazon Simple Email Service from licences@cotterpin.io.

We do not send marketing email. If we ever offer a newsletter, you will only receive it if you opt in, and we will update this policy first.

10. Who processes data for us

PROVIDER	WHAT FOR	ROLE
Amazon Web Services	The licence service: computing (Lambda), its database (DynamoDB), signing keys (KMS), secrets (Secrets Manager) and claim emails (SES). Region: EU (Ireland), `eu-west-1`, including SES	Processor
Paddle.com Market Ltd	Selling paid plans, payment, tax, invoices, refunds	Independent controller (merchant of record)
Microsoft (Azure Static Web Apps)	Hosting this website	Processor
Microsoft (Microsoft 365)	Receiving and sending our email	Processor
Google Ireland Limited (Google Analytics 4)	Counting website visits, only with your consent	Processor

We do not sell personal data, and we do not share it with anyone else except where the law requires it. The full list, with locations and what each one receives, is on our Sub-processors page.

11. International transfers

Our licence service is in the EU (Ireland), which the UK recognises as adequate. Some of our providers may process data in other countries, including the United States. Where they do, we rely on UK adequacy regulations (including the UK–US data bridge for certified US companies), or on the International Data Transfer Agreement or the UK Addendum to the EU Standard Contractual Clauses; for transfers out of the EU, on an EU adequacy decision or the EU Standard Contractual Clauses. Each transfer, and what we rely on for it:

- **Amazon Web Services** (licence service, Ireland): no transfer outside the EU; the UK recognises the EU as adequate.
- **Microsoft** (website hosting and email): may process data in the United States; Microsoft is certified under the EU–US Data Privacy Framework and its UK Extension, and its data protection addendum includes the Standard Contractual Clauses.

- **Google** (analytics, only with your consent): may process data in the United States; Google is certified under the EU–US Data Privacy Framework and its UK Extension, and its data processing terms include the Standard Contractual Clauses.
- **Paddle** (payments): Paddle is an independent controller and sets out its own transfers in its privacy policy.

12. How long we keep it

In summary below; where each record lives and how it is deleted is in our Data Retention Policy.

DATA	KEPT FOR
Licence, plan, machine fingerprints, email hash	While the licence exists, then 12 months after it ends
Machine change audit records	With the licence record: 12 months after the licence ends
Machine registrations (one per machine fingerprint), and trial records made before 28 October 2026	24 months after the record was made
One-time claim codes	Valid 15 minutes; the record expires automatically after 30 minutes
Bug reports you send (from the next release), or that are sent automatically where you turned that on (from the next release)	Until the fault is closed, then 12 months. The outbox copy on your machine stays until you delete it
Rate-limit counters (a one-way hash of the source IP address, or of a claim's email address)	2 hours, then automatically expired
Applied Paddle notification ids	35 days, then automatically expired
Licence service logs (no IP address, identity or request content)	30 days
Support emails, security reports, data protection requests and our replies	2 years after the conversation, report or request is closed
Order and invoice records (held by Paddle; any copies we hold)	As long as tax and accounting law requires, typically 6 years

13. Security

Licence tokens are signed with keys held in AWS KMS. Paddle API and webhook secrets are held only in AWS Secrets Manager. Calls to Paddle use verified TLS, and every Paddle notification is signature-

checked before it is read. Machine fingerprints and email addresses are stored only as one-way hashes. If a personal data breach is likely to put your rights at risk, we will tell the ICO within 72 hours and tell you without undue delay where the law requires it. See our Security page for more.

14. Your rights

Under UK GDPR you have the right to access the personal data we hold about you, to have it corrected or erased, to restrict or object to its use, to data portability, and to withdraw consent at any time where we rely on it. To withdraw a consent given in the software, use `cotterpin consent`. To remove a machine from your licence, use `cotterpin machines remove`. For anything else, contact us (section 17). We will answer within one month; if a request is complex we may extend that by up to two further months, and will tell you why within the first month. How requests work is set out in our GDPR Statement.

Where we rely on legitimate interests, you can object, and we will stop unless we have compelling grounds that override yours. We make no decisions about you based solely on automated processing that have legal or similarly significant effects.

Because we store your email address only as a hash and your machine only as a fingerprint, we may need you to tell us your email address or run a command on your machine so we can find your records.

15. Children

Cotterpin is a professional developer tool and is not intended for anyone under 18, and we do not knowingly collect personal data from anyone under 18. If you think we have, contact privacy@cotterpin.io and we will delete it.

16. Changes to this policy

We will update this policy whenever what the software sends, or who processes data for us, changes — before the change takes effect. A release that changes what a measurement reads asks for your consent again.

17. Contact and complaints

Email privacy@cotterpin.io or write to Cotterpin Technologies Ltd, 18 Massingberd Way, London, SW17 6AB.

If you are unhappy with how we have handled your data, you can complain to the Information Commissioner's Office at ico.org.uk (0303 123 1113). If you are in the EU or EEA, you can also complain to the data protection authority where you live or work. We would appreciate the chance to put things right first.