Privacy Policy

Tendermark Ltd

Effective: 1 May 2026
Version: 1.0

Contents

1. About this Policy

1.1 This Privacy Policy explains how Tendermark Ltd handles personal data when you use the Tendermark website and platform (the **"Services"**).

1.2 We are committed to protecting your privacy and handling personal data in line with the UK General Data Protection Regulation (**"UK GDPR"**), the Data Protection Act 2018 and the Privacy and Electronic Communications Regulations 2003 (**"PECR"**).

1.3 The Services are a business tool for UK-based RICS-certified building surveyors and surveying firms. We do not offer the Services to consumers or to anyone under 18.

1.4 This Policy should be read alongside our Terms of Service, including **Schedule 1 (Data Processing Terms)** which applies when we process personal data on your behalf as your processor.

2. Who we are and how to contact us

2.1 The data controller for personal data we hold about you (as our customer and user) is:

> ***Tendermark Ltd** (company number **17161246**)*
> *66 Paul Street*
> *London EC2A 4NA*
> *United Kingdom Email: **hello@tendermark.ai***

2.2 We have not appointed a statutory Data Protection Officer, because we are not required to under UK GDPR Article 37. For all data protection questions, contact **hello@tendermark.ai**.

---

3. Our role as controller and processor

3.1 **We act as controller** in relation to personal data about you and your use of the Services — your name and firm name, your email address and login credentials, your subscription and billing identifiers, and data about how you use the Services.

3.2 **We act as processor on your behalf** in relation to personal data that is part of the tender content you upload, author or collect through the Services — personal data about your clients, your contractors, your projects, and the free-text material you or a contractor enter into the Services.

3.3 This dual role matters because different legal frameworks apply to each. Section 5 of this Policy describes what we do as controller. Sections 6–9 describe what we process as processor on your instructions. The full terms of our processor role are at **Schedule 1** of the Terms of Service.

3.4 If you are a contractor who has received an invitation to price a tender through the Services, please see **section 7** — which explains how your personal data is handled and how to contact the surveyor who invited you.

---

4. The personal data we handle

4.1 **Account and profile data** (controller):

- your full name
- your firm name
- your email address
- your password (stored only as a secure hash — we cannot read it)
- your monthly comparison volume (professional context you provide during onboarding)
- your preference and entitlement state (for example, whether you have opted in to the Benchmarking Commons; whether your free tender has been used)
- a pseudonymous identifier linking you to your record at our payment processor (we do **not** store your full card number)

4.2 **Project, tender and client data** (processor):

- project names, notes, postcode prefixes or regions, approximate values
- tender names and references
- the content of each Schedule of Works you author or upload (which may include property addresses, client references and other material in free-text line-item descriptions)

4.3 **Contractor data** (processor — personal data about third parties you introduce to the Services; see section 7):

- contractor name, email address and firm name
- identity details the contractor confirms on the invitation gate screen (name, email, firm name, as entered by the contractor)
- invitation metadata (when the invitation was sent, opened, saved and submitted)
- IP addresses captured at each step of the contractor's interaction with an invitation (see section 8)

4.4 **Return content** (processor — content of each tender return):

- response type, price, per-item note, raw text extracted from uploaded files
- contractor-entered pricing and notes for invitation-flow submissions

4.5 **Usage data** (controller):

- information about how you use the Services, collected via our analytics provider PostHog (EU cloud) — this includes events such as which pages you visit within the app, which features you use, and device and browser context
- technical log data (IP address, user agent, timestamp) for security and diagnostic purposes

4.6 **Communications data** (controller):

- any emails and other messages you send us
- records of any support interactions

4.7 **Anonymised commons data** (no personal data): anonymised pricing signals are stored separately in the Benchmarking Commons — see **section 6**. This data contains no personal data and cannot be traced back to you, your clients or any contractor.

4.8 **Incidental personal data in free text.** Some fields in the Services — project notes, line-item descriptions, contractor notes, and raw text extracted from uploaded returns — accept free-text input. You or a contractor may include personal data in those fields (for example, a property address). We process that data as part of the tender content; it is your responsibility (as the surveyor) to manage what goes into those fields.

---

5. How we use personal data, and our lawful bases

5.1 As **controller**, we process personal data for the following purposes, on the lawful bases indicated:

Purpose	Lawful basis
Creating and managing your account; authenticating you when you sign in	Contract (UK GDPR Article 6(1)(b)) — performance of the Terms of Service
Providing the Services to you, including processing your tender content and generating outputs	Contract
Taking payment and issuing invoices	Contract; legal obligation (Article 6(1)(c)) for statutory record-keeping
Sending you transactional emails (for example, password resets, tender status notifications)	Contract
Analysing how you use the Services to improve them (via PostHog)	Legitimate interests (Article 6(1)(f)) — our interest in maintaining and improving a professional B2B service. Balanced against your rights; you can decline non-essential analytics cookies at the cookie banner (see section 13)
Maintaining security of the Services, investigating fraud, and keeping the audit log	Legitimate interests — our interest, and your interest, in a secure and auditable platform (see section 8)
Contributing anonymised pricing signals to the Benchmarking Commons (subject to your opt-out)	Legitimate interests (Article 6(1)(f)) — see section 6
Complying with legal and regulatory obligations	Legal obligation
Defending ourselves against legal claims, where necessary	Legitimate interests

5.2 As **processor**, we handle personal data in the tender content on your instructions — as documented in the Terms of Service and **Schedule 1**. Your legitimate use of the Services is treated as an instruction to process. You are the controller for that data and you are responsible for having a lawful basis to provide it to us.

5.3 **We do not sell personal data.** We do not use personal data for targeted advertising. We do not profile users for automated decisions that produce legal or similarly significant effects.

---

6. The Benchmarking Commons

6.1 The Benchmarking Commons is a shared dataset of anonymised pricing signals derived from the tenders you process, used to improve benchmarking for Tendermark users. Participation is optional. It is a core feature of the product and we want you to understand it fully.

6.2 **Professional precedent.** The Benchmarking Commons model is based on the approach used by the Building Cost Information Service (**BCIS**), which has operated a professional data commons for the surveying profession for more than 60 years with RICS backing. Under that long-established model, the surveyor contributing data is the participant and the data provider; the anonymised aggregate is made available to the profession. Tendermark applies that model to minor works, with one conservative refinement: contribution to our commons is opt-in, not assumed.

6.3 **Two distinct processing activities.** There are two things going on when you use the Services, and they are treated separately:

- **Activity 1 — Processing a tender for your own use.** This is the core Service: extracting and comparing returns for your own account. This is what you are paying for. We process this on the **lawful basis of contract**.
- **Activity 2 — Contributing anonymised pricing signals to the Benchmarking Commons.** This is a separate processing activity. We process this on the **lawful basis of legitimate interests** (UK GDPR Article 6(1)(f)). The legitimate interest is the benefit to Tendermark users and the surveying profession of better minor-works benchmarking data, consistent with the long-established BCIS model. We have carried out a Legitimate Interests Assessment, which is available on request by emailing **hello@tendermark.ai**.

6.4 **Your right to object.** Because Activity 2 is based on legitimate interests, you have a right under UK GDPR Article 21 to object to it at any time. We operationalise this right through an opt-in/opt-out toggle in your account settings: toggling off stops all future contributions to the Benchmarking Commons from your account. The opt-in toggle is the primary way to exercise this right; you can also object by emailing **hello@tendermark.ai**.

6.5 **No effect on service.** Your opt-in status has no effect on:

- your access to the Services;
- any feature of the Services;
- the price you pay;
- the quality of support you receive.

6.6 **What is stripped before anything is stored in the Commons.** Before any record is written to the Benchmarking Commons, we remove:

- all contractor names
- all contractor and property addresses
- all client names and client references
- all surveyor and firm names
- all project names
- any free-text content that could identify any party
- any other content that could be used to identify any party

6.7 **What is retained.** Only anonymised pricing signals are retained: trade category (normalised), a generalised description of the work (rewritten by AI to remove specifics), unit of measurement, unit rate, total, project type, broad region (broader than postcode area), and the quarter in which the contribution was made.

6.8 **Contributions are irrevocable once anonymised.** Because we strip all links back to you, your clients and the contractor before writing to the Commons, there is no personal-data record to retrieve once a contribution has been made. If you toggle off future contributions, the toggle takes effect immediately, but past anonymised records stay in the aggregate. This is unavoidable because those records contain no personal data that could be used to identify or locate your prior contributions.

6.9 **This is explained at the point of opt-in.** Our onboarding screen sets out, before you accept, exactly what is stripped, exactly what is retained, and exactly what toggling off does and does not do. This is a deliberate design choice that reflects ICO guidance on how irrevocable anonymised contributions should be communicated.

6.10 **How to stop contributing.** You can toggle off contributions at any time from the **Pricing Commons** section of your account settings. No justification is required. We will not nag you or prompt you to toggle back on.

6.11 **Further questions about contributions.** If you want to discuss your contribution history, or you believe you contributed data in error, email **hello@tendermark.ai**.

---

7. Data about contractors

7.1 Contractors named in tenders, and contractors who receive an invitation to price a tender via the Services, are data subjects under UK GDPR. They are not customers of Tendermark.

7.2 **Our role.** When you invite a contractor through the Services, or when you upload a return from a contractor:

- **You are the data controller** for the contractor's personal data. You introduced that data to the Services; your lawful basis for processing it is a matter for you.
- **We are your processor** in relation to contractor personal data. The terms on which we process it on your behalf are at **Schedule 1 of the Terms of Service**.

7.3 **What we collect about contractors:**

(a) when you invite a contractor, we collect the name, email and (if you provide it) firm name you enter;

(b) when a contractor opens an invitation link, we capture their IP address (see section 8);

(c) when a contractor confirms their details on the gate screen, we collect the name, email and firm name they enter themselves;

(d) at each subsequent save and submit, we record a timestamp and the contractor's IP address in our append-only audit log.

7.4 **Direct collection from the contractor.** The identity gate — where the contractor types in their own name, email and firm name before they begin pricing — is a direct collection from the contractor to the Services. That collection is on the surveyor's instructions and for the surveyor's purposes; it records the contractor's accurate identity for the tender the surveyor has issued. We act as processor on the surveyor's behalf for that collection, not as a joint controller.

7.5 **Information for contractors.** A contractor who has received an invitation and who has questions about their personal data can:

- email the surveyor who invited them (their primary point of contact), whose name and firm are shown on the invitation page;
- email us at **hello@tendermark.ai** with the invitation link and their query; or
- exercise their rights directly against us under section 16 of this Policy.

7.6 **No marketing to contractors.** We do not use contractor email addresses or other contractor personal data to market Tendermark to contractors.

---

8. The audit log

8.1 The Services include a **tamper-resistant audit log** (`tender_return_events`) that records every state transition on every tender return, including:

- when an invitation was sent, resent or revoked;
- when a contractor opened an invitation link;
- when a contractor confirmed their details;
- each time a contractor saved progress;
- when a contractor submitted;
- when a surveyor converted an invitation to an upload or extended a deadline.

8.2 **What is captured.** For each event: the event type, the type of actor (surveyor, contractor, or our system), the actor's user identifier (if the actor is a surveyor), the contractor's IP address (if the actor is a contractor), a timestamp, and event-specific metadata (for example, the deadline change or the number of responses saved).

8.3 **Why this exists.** The audit log:

- lets us resolve "I never priced that" disputes with a timestamped record of every action taken on an invitation;
- supports compliance with the audit-trail expectations of the RICS AI Standard (effective 9 March 2026);
- protects against and helps investigate fraudulent or malicious use of invitation links.

8.4 **Lawful basis.** We process audit log data on the basis of our **legitimate interests** — and the legitimate interests of surveyors, contractors and the profession — in a secure, auditable platform. For contractor IPs specifically, the legitimate interests are fraud prevention, dispute resolution, and audit trail. These interests are balanced against the contractor's reasonable expectation that their interaction with a priced tender is recorded for the surveyor's professional record. The log is append-only — we do not edit or delete log entries in the ordinary course.

8.5 **Retention.** We retain audit log entries for the same period as the associated tender content (see section 15). The log is append-only — we do not edit or delete individual entries in the ordinary course of operations. If you request deletion of Customer Personal Data, or close your account, audit log entries for the affected tenders are deleted alongside the rest of your content, subject only to any retention required by law or by a live dispute, investigation or regulatory request.

8.6 **Access.** Audit log entries are visible in the application only to the surveyor who owns the tender the return belongs to. They are not public, not visible to other users, and not visible to contractors. They may be accessed by Tendermark personnel under strict access controls to investigate incidents or respond to a lawful request.

---

9. Public sharing — share links and invitation links

9.1 The Services generate two kinds of token-based public link:

- **Share links** — read-only links you generate to share a completed tender analysis report with a client or other party.
- **Invitation links** — write-enabled links you send to a contractor so they can price a tender online.

9.2 **Share links.**

(a) A share link renders the completed report in read-only form and displays your name and firm as the preparer of the report.

(b) A share link is valid until the share expiry you configure. After expiry, the link returns a generic "no longer valid" response and reveals nothing about the content.

(c) Anyone holding the share link can read the content. You are responsible for deciding with whom to share it.

9.3 **Invitation links.**

(a) An invitation link permits the invited contractor to enter their details, price line items, save progress and submit. It does not grant access to anyone else's data.

(b) Tokens are random 122-bit identifiers generated using `crypto.randomUUID()`. They are not guessable in any practical sense.

(c) Tokens are transmitted over HTTPS only, included in the email link to the contractor but never displayed in link text. Tokens are not stored in analytics (PostHog) or in application logs.

(d) Invitation links expire at the deadline you set, after which they return the same generic "no longer valid" response. All error states on invitation links — expired, revoked, already submitted, invalid — return the same generic message, to prevent probing of the token space.

(e) Per-token and per-IP rate limits apply to invitation endpoints.

9.4 A contractor who prices a tender through an invitation link can download a PDF copy of their submission at the time of submission and receives it by email.

---

10. Artificial intelligence and our use of Anthropic

10.1 The Services use large language models provided by **Anthropic** (via Anthropic's commercial API) to extract structured data from uploaded tender documents, to normalise line-item descriptions before contribution to the Benchmarking Commons, and to support report drafting.

10.2 **What is sent to Anthropic.** When we call Anthropic's API, we send the content we need to process to complete the task — for example, the text content of a Schedule of Works, the content of a contractor return, or a line-item description we need to normalise.

10.3 **Anthropic does not use your data to train its models.** Under Anthropic's commercial API terms as in force at the effective date of this Policy, the data we submit — including your tender content, contractor returns, and any derived analysis — is **not used to train Anthropic's models**. Your data is processed solely to provide you with the Tendermark Services. If Anthropic's commercial API terms change in a way that materially affects this statement, we will update this Policy in accordance with section 18.

10.4 **What the AI does and does not do.** The AI extracts, normalises and summarises information. It does not make professional judgements, give opinions, or take decisions on your behalf. All outputs are for you to review and verify — see the output-reliance clause in the Terms of Service (clause 12).

10.5 **No automated decision-making with legal or similarly significant effects.** We do not make automated decisions concerning you within the meaning of UK GDPR Article 22.

---

11. Sub-processors and who we share data with

11.1 We use the following sub-processors to provide the Services. Each has been chosen for its security posture and its compatibility with UK GDPR obligations. We have a written data processing agreement with each.

Sub-processor	Purpose	Location of processing	International transfer mechanism
Supabase	Database, authentication, file storage	European Union (EU region)	Not required (UK adequacy regulations apply to EEA transfers)
Anthropic	AI-powered extraction, normalisation and analysis	United States	UK Addendum to EU SCCs
Stripe	Payment processing	United States	UK extension to the EU–US Data Privacy Framework, with

			UK Addendum to EU SCCs as backup
Vercel	Application hosting, edge delivery	United States	UK extension to the EU–US Data Privacy Framework, with UK Addendum to EU SCCs as backup
Cloudflare	DNS, CDN, DDoS protection	United States	UK extension to the EU–US Data Privacy Framework, with UK Addendum to EU SCCs as backup
PostHog	Product analytics and feature flags	European Union (EU Cloud)	Not required
Resend	Transactional email delivery	European Union	Not required

11.2 We may also share personal data with:

- **professional advisers** (lawyers, accountants, auditors) under duties of confidentiality, where reasonably necessary;
- **law-enforcement and regulatory authorities** where we are legally required to do so;
- a **prospective or actual purchaser** of our business or assets, subject to confidentiality, in connection with a sale, merger, reorganisation, or due diligence.

11.3 **We do not sell personal data, and we do not share it for marketing purposes with third parties.**

11.4 We keep our sub-processor list current. If we add or change a material sub-processor, we will update this Policy and notify customers in line with section 18.

12. International transfers

12.1 Some of our sub-processors (marked in section 11 as requiring a transfer mechanism) process personal data outside the United Kingdom, principally in the United States.

12.2 **Our transfer safeguards depend on the sub-processor:**

- For **Stripe, Vercel and Cloudflare**, we rely primarily on the **UK extension to the EU–US Data Privacy Framework** (commonly called the "UK–US Data Bridge"). The UK government has determined, by regulations made under the Data Protection Act 2018, that the United States provides an adequate level of data protection in respect of personal data transferred to organisations certified under the Data Privacy Framework. Each of these three sub-processors is actively certified. As a secondary safeguard, each has also put the UK Addendum to the EU Standard Contractual Clauses in place through its own data processing terms, which would apply if its Data Privacy Framework certification were ever suspended or withdrawn.
- For **Anthropic**, which is not currently certified under the Data Privacy Framework, we rely on the **UK Addendum to the EU Standard Contractual Clauses** (as issued by the Information Commissioner's Office under s.119A of the Data Protection Act 2018), together with the underlying EU Standard Contractual Clauses. This instrument is in place as part of Anthropic's own data processing terms, deemed executed when we use their services.

12.3 For transfers to Anthropic, we have carried out a Transfer Risk Assessment in line with ICO guidance. For transfers to Stripe, Vercel and Cloudflare, we rely on the adequacy finding underlying the Data Privacy Framework and monitor each sub-processor's certification status; if any certification is suspended or withdrawn, our UK Addendum backup mechanism takes effect and a Transfer Risk Assessment is completed at that point.

12.4 You can request a copy of the transfer safeguards we rely on for any specific sub-processor by emailing **hello@tendermark.ai**.

13. Cookies and analytics

13.1 We use a small number of cookies and similar technologies on the Services.

13.2 **Strictly necessary cookies** are required for the Services to function — for example, to keep you signed in and to support secure payment. These cannot be disabled.

13.3 **Analytics cookies** (PostHog) help us understand how the Services are used. PostHog is hosted in the EU and acts as our processor. We use it solely to analyse aggregate usage of our own service and to improve it — we do not share analytics data with any third party for advertising, targeting, or any other purpose. Because the processing meets the "statistical purposes" exception under the Privacy and Electronic Communications Regulations 2003 (as amended by the Data (Use and Access) Act 2025, effective 5 February 2026), we do not require your consent to set these cookies. You can still turn analytics off at any time via the **Cookie preferences** link in the site footer; doing so does not affect your access to any feature of the Services.

13.4 **Payment cookies** (Stripe) are set by Stripe at the point of checkout to process your payment. They are necessary for that purpose.

13.5 **How we inform you.** On your first visit, a small notice at the bottom of the page summarises our use of cookies and links to this Policy and to the Cookie preferences page. The notice is informational — it does not ask for your consent, because none is required for the cookies we actually use. You can change your analytics preference at any time via the **Cookie preferences** link, which remains accessible from every page.

13.6 We **do not** use advertising cookies, tracking cookies for third-party advertising purposes, retargeting cookies, or any cross-site tracking technology.

14. Security

14.1 We take security seriously. Our technical and organisational measures include:

- **Encryption** — TLS for all data in transit; encryption at rest for our database and file storage, via Supabase;
- **Access controls** — role-based access to production systems; production access limited to named personnel; authentication via strong credentials with multi-factor authentication for privileged roles;
- **Network** — DDoS protection and TLS termination via Cloudflare; HTTPS enforced;
- **Application-level isolation** — row-level security in our database so that users can only access their own data;
- **Secure tokens** — public tokens are random 122-bit identifiers, rate-limited, and never logged;
- **Audit trail** — append-only event log (see section 8);
- **Vendor controls** — we use reputable sub-processors with documented security programmes;
- **Incident response** — we maintain a documented incident response process and will notify affected customers of qualifying breaches in line with UK GDPR.

14.2 No system is perfectly secure, and we cannot guarantee the security of information transmitted to us over the internet. You are responsible for keeping your account credentials confidential.

15. How long we keep personal data

15.1 We keep personal data only as long as we need it for the purposes for which we collected it, and in line with legal and regulatory obligations.

15.2 Our current retention periods are:

Category	Retention	Reason
Account and profile data	Lifetime of account + 6 months after closure	Allows account reactivation; allows resolution of queries after closure
Tender content (SoWs, returns, line items, responses)	Lifetime of account + 6 months after closure	As above
Contractor data (names, emails, firm names, IPs in the audit log)	Lifetime of account + 6 months after closure	Integral part of the tender record; retained and deleted with it
Audit log (`tender_return_events`)	Same as the associated tender content (see above)	Integral part of the tender record; retained and deleted with it
Transactional email and support correspondence	6 years	Limitation period for contract claims under the Limitation Act 1980; dispute resolution
Billing and tax records (invoice metadata, Stripe customer identifier)	7 years from the end of the tax year to which they relate	UK tax-law minimum (6 years); held for a 1-year safety margin
Benchmarking Commons anonymised records	Indefinite	No personal data is retained; once anonymised, there is nothing to delete (see section 6)
Server-side technical logs and security logs	90 days in the hot tier; archived for up to 12 months	Security monitoring and investigation

15.3 **All retention periods are indicative.** We may retain personal data longer where we reasonably consider it necessary to defend or bring legal claims, or where required by law.

---

16. Your rights under UK GDPR

16.1 Subject to the conditions set out in UK GDPR, you have the following rights in respect of personal data we hold about you as controller:

- **Right of access** — to obtain a copy of your personal data and information about how it is processed;
- **Right to rectification** — to have inaccurate personal data corrected;
- **Right to erasure** — in certain circumstances, to have personal data deleted;
- **Right to restrict processing** — in certain circumstances;
- **Right to data portability** — in certain circumstances, to receive a copy of your personal data in a structured, commonly used, machine-readable format;
- **Right to object** — where we rely on legitimate interests (including for the Benchmarking Commons and for product analytics described in section 5), you may object at any time. For the Benchmarking Commons, you exercise this right through the account-settings toggle (see section 6.4); for other legitimate-interests processing, email **hello@tendermark.ai**;
- **Right to withdraw consent** — where we rely on consent (for example, your acceptance of analytics cookies), you may withdraw consent at any time without affecting the lawfulness of processing before withdrawal.

16.2 **Benchmarking Commons — specific rules.** Toggling off the Benchmarking Commons (your right to object under Article 21) stops future contributions. Past anonymised contributions stay in the aggregate because, by design, we do not retain a link between those records and you — there is nothing identifiable to erase. This is explained at the point of opt-in and is a material part of participation.

16.3 **Data subject requests from your clients and contractors.** If your client or a contractor named in a tender makes a rights request relating to data in your account, that request is your responsibility as the controller. Schedule 1 (Data Processing Terms) of the Terms of Service describes how we will assist you in responding.

16.4 **How to make a request.** Email **hello@tendermark.ai**. We will respond within one month of receiving your request, or tell you within that period if we need longer because your request is complex.

16.5 No fee is charged for a rights request in the ordinary course. We may charge a reasonable fee or decline to act where a request is manifestly unfounded or excessive, as allowed by UK GDPR.

---

17. Children

The Services are not directed at, and are not available to, anyone under the age of 18. We do not knowingly collect personal data from children.

---

18. Changes to this Policy

18.1 We may change this Privacy Policy from time to time — for example, to reflect changes in the Services, in applicable law, or in our sub-processor list.

18.2 If we make a material change that affects your rights, we will notify you by email to the address on your account and by an in-product notice, at least 30 days before the change takes effect.

18.3 Non-material changes take effect on posting of the revised Policy, with the effective date at the top of the document updated accordingly.

18.4 We keep an archive of superseded versions of this Policy. Contact **hello@tendermark.ai** if you need a copy.

---

19. Complaints

19.1 If you have a concern about how we handle your personal data, please email **hello@tendermark.ai** first. We will do our best to resolve it.

19.2 You also have the right to complain to the UK regulator, the **Information Commissioner's Office (ICO)**:

> *Information Commissioner's Office*
> *Wycliffe House, Water Lane*
> *Wilmslow, Cheshire SK9 5AF*
> *United Kingdom Helpline: **0303 123 1113***
> *Website: **https://ico.org.uk***
