Data Processing Agreement

Schedule 1 to the Tendermark Terms of Service

Data Processing Terms

Effective: inherited from the Tendermark Terms of Service in the version in force between the parties
Version: 1.0

Contents

This Data Processing Agreement governs our processing of personal data on behalf of our customers in connection with the Tendermark Services. It is Schedule 1 to the Tendermark Terms of Service and is accepted by customers at signup as part of those Terms; it is also published here in full for ease of reference by procurement and data-protection teams. A standalone signing version is available on request — see section 16.

---

1. About this Schedule

1.1 This Schedule 1 (**"Data Processing Terms"** or **"DPA"**) forms part of the Tendermark Terms of Service (the **"Terms"**) and is incorporated into the Terms by reference. It is accepted by the same click-through mechanism as the Terms and does not need to be separately signed.

1.2 This Schedule applies whenever we process Customer Personal Data on your behalf as your processor. It is designed to satisfy UK GDPR Article 28 and, where applicable, the equivalent requirements of the Data Protection Act 2018.

1.3 If there is any conflict between this Schedule and the main body of the Terms, this Schedule prevails to the extent of the conflict in relation to processing of personal data.

---

2. Definitions

2.1 Terms defined in the Terms have the same meaning in this Schedule. In addition:

- **"Applicable Data Protection Law"** means the UK GDPR, the Data Protection Act 2018, and PECR, together with any associated guidance from the ICO, in each case as amended and in force from time to time.
- **"Controller"**, **"Processor"**, **"data subject"**, **"personal data"**, **"processing"**, **"personal data breach"** and **"supervisory authority"** have the meanings given to them in the UK GDPR.
- **"Customer Personal Data"** means personal data that we process on your behalf in the course of providing the Services — that is, personal data contained in Your Content (as defined in the Terms). This includes personal data about your clients, contractors (including the contractors you invite to price tenders), and other third parties that appears in the tenders you author, upload or process through the Services.
- **"Sub-processor"** means any third party engaged by us to process Customer Personal Data on our behalf.
- **"UK GDPR"** means the United Kingdom General Data Protection Regulation as defined in the Data Protection Act 2018.

---

3. The parties' roles

3.1 In respect of Customer Personal Data, **you are the Controller** and **we are the Processor**.

3.2 This Schedule governs only our processing of Customer Personal Data. Our processing of personal data about you as our customer (your name, email, billing identifiers and similar) is a separate matter in which we act as controller; that processing is described in our Privacy Policy and is not governed by this Schedule.

3.3 **Contractor identity gate — characterisation.** When a contractor confirms their own name, email and firm name on the invitation gate screen, that collection is on your instructions and serves your purposes (recording accurate contractor identity for the tender you issued). In respect of that collection, we act as your Processor under this Schedule, not as a joint controller within the meaning of UK GDPR Article 26.

---

4. Scope and subject-matter of processing

4.1 We will process Customer Personal Data only:

(a) to provide the Services to you in accordance with the Terms;

(b) on your documented instructions (including your legitimate use of the Services, which is a documented instruction for these purposes); and

(c) as required by applicable law (in which case, unless the law prohibits it on important public interest grounds, we will notify you of that requirement before processing).

4.2 **Annex A** sets out the subject-matter, duration, nature and purpose of the processing, the categories of data subjects and the types of personal data. Annex A may be updated when material changes to the Services are made.

4.3 We will immediately inform you if, in our opinion, an instruction from you infringes Applicable Data Protection Law. We may suspend processing (without liability for any failure to provide the Services during that suspension) while we seek clarification.

---

5. Our obligations as processor

5.1 We will:

(a) process Customer Personal Data only for the purposes set out in clause 4 and Annex A;

(b) ensure that persons authorised to process Customer Personal Data are committed to confidentiality or are under an appropriate statutory obligation of confidentiality;

(c) implement and maintain appropriate technical and organisational measures to protect Customer Personal Data (see clause 7 and Annex B);

(d) assist you, taking into account the nature of the processing and the information available to us, in meeting your own obligations under Applicable Data Protection Law (see clause 11);

(e) only engage Sub-processors in accordance with clause 8;

(f) only transfer Customer Personal Data outside the United Kingdom in accordance with clause 9;

(g) notify you of personal data breaches in accordance with clause 10;

(h) at your choice, delete or return all Customer Personal Data after the end of the Services in accordance with clause 13;

(i) make available to you all information necessary to demonstrate compliance with our obligations as processor, and allow and contribute to audits in accordance with clause 12.

---

6. Your obligations as controller

6.1 You warrant and represent that:

(a) you have a valid lawful basis under Applicable Data Protection Law for all processing of Customer Personal Data carried out by us on your behalf;

(b) you have provided all legally required notices, and obtained all legally required consents, from the individuals whose personal data is included in Your Content — including from your clients, contractors you invite, and any other third parties whose personal data appears in the tenders you process;

(c) your instructions to us (including your legitimate use of the Services) are lawful and compliant with Applicable Data Protection Law;

(d) you will not provide us with special category personal data (as defined in UK GDPR Article 9) or personal data relating to criminal convictions or offences (Article 10), except to the incidental extent such data is present in free-text fields despite your reasonable steps to avoid it. The Services are not designed to process special category data and you should not include it deliberately;

(e) you will ensure that any personnel of yours who access the Services are authorised by you and bound by appropriate confidentiality and data protection obligations; and

(f) you are responsible for the accuracy, quality and legality of Customer Personal Data.

---

7. Security measures

7.1 We will implement and maintain appropriate technical and organisational measures to protect Customer Personal Data against unauthorised or unlawful processing and against accidental loss, destruction or damage. These measures are set out at **Annex B**.

7.2 We may update these measures over time provided the level of protection is not materially reduced.

---

8. Sub-processors

8.1 **General authorisation.** You authorise us to engage the Sub-processors listed at **Annex C**, and to replace or add Sub-processors provided we comply with this clause.

8.2 **Sub-processor obligations.** We will enter into a written contract with each Sub-processor imposing data-protection obligations materially no less protective than those in this Schedule. We remain fully liable to you for the acts and omissions of any Sub-processor we engage.

8.3 **New or replacement Sub-processors.** We will publish any intention to add or replace a Sub-processor on our website and/or notify you by email at least **14 days** before the new Sub-processor begins processing Customer Personal Data.

8.4 **Objection.** If you have a reasonable objection to a new Sub-processor, you must notify us in writing within the 14-day notice period, setting out the basis for your objection (which must relate to data protection concerns). We will work with you in good faith to resolve the concern. If we cannot resolve it, you may terminate the Services by giving us written notice, with a pro-rata refund of any prepaid fees attributable to the period after termination.

---

9. International transfers

9.1 We will not transfer Customer Personal Data outside the United Kingdom except:

(a) to a jurisdiction covered by a UK adequacy regulation; or

(b) under an appropriate safeguard recognised under UK GDPR Article 46. Our standard safeguard is the **UK Addendum to the EU Standard Contractual Clauses** (as issued by the ICO under s.119A of the Data Protection Act 2018), in conjunction with the underlying EU Standard Contractual Clauses.

9.2 Each Sub-processor listed in Annex C that processes Customer Personal Data outside the United Kingdom does so under a transfer mechanism appropriate to that Sub-processor's circumstances: either the UK extension to the EU–US Data Privacy Framework (where the Sub-processor holds an active certification and the UK government's Data Bridge applies) or the UK Addendum to the EU Standard Contractual Clauses. The specific mechanism per Sub-processor is set out in Annex C. Each instrument is deemed executed between us and the relevant Sub-processor in accordance with the Sub-processor's own data processing terms.

9.3 **Onward transfers.** In relation to those transfers, we act as the data exporter and the relevant Sub-processor acts as the data importer. By accepting this Schedule, you provide your general written authorisation, for the purposes of UK GDPR Article 28(2), to those onward transfers being made on the safeguards described in clause 9.2. This authorisation is subject to your right to object to the engagement of a Sub-processor under clause 8.4.

9.4 We will make available to you, on reasonable request, a copy of the transfer safeguards in force with a specific Sub-processor, or a link to the Sub-processor's published terms that contain them.

---

10. Personal data breaches

10.1 We will notify you **without undue delay** and in any event within **72 hours** after becoming aware of a personal data breach affecting Customer Personal Data.

10.2 Our notification will (so far as the information is known to us at the time):

(a) describe the nature of the breach, including the categories and approximate number of data subjects and records concerned;

(b) identify a point of contact for further information;

(c) describe the likely consequences of the breach; and

(d) describe the measures we have taken or propose to take to address the breach and mitigate its effects.

10.3 Where information is not known at the time of initial notification, we will provide it as soon as reasonably practicable thereafter.

10.4 You are responsible for any notification to the supervisory authority or to affected data subjects required under Applicable Data Protection Law in respect of a breach. We will provide reasonable assistance to help you comply with those obligations.

10.5 We will maintain an internal record of personal data breaches involving Customer Personal Data, to support our own compliance with UK GDPR Article 33(5).

---

11. Assistance to you

11.1 Taking into account the nature of the processing and the information available to us, we will assist you in complying with your obligations under Applicable Data Protection Law in respect of:

(a) responding to requests from data subjects to exercise their rights (access, rectification, erasure, restriction, portability, objection, withdrawal of consent);

(b) carrying out data protection impact assessments;

(c) consulting with supervisory authorities where required;

(d) notifying personal data breaches; and

(e) maintaining security of processing.

11.2 **Forwarding data subject requests.** If we receive a request from a data subject concerning Customer Personal Data we process on your behalf, we will not respond to it directly (except to acknowledge receipt and redirect the data subject to you) and will forward the request to you without undue delay.

11.3 **Fees for assistance.** Assistance that is manifestly excessive, that requires significant engineering or manual work, or that goes beyond what is required by Applicable Data Protection Law, may be charged at our reasonable rates. We will agree those rates with you in advance wherever practicable.

---

12. Audit rights

12.1 We will, on reasonable written request, make available to you information necessary to demonstrate our compliance with our obligations under this Schedule and Applicable Data Protection Law.

12.2 **Audits.** We will allow for, and contribute to, audits (including inspections) conducted by you or an auditor you authorise, subject to the following reasonable conditions:

(a) you must give us at least 30 days' written notice, except in the event of a suspected personal data breach;

(b) audits must be conducted during normal business hours and with minimum disruption to our operations;

(c) audits must be no more frequent than once in any 12-month period, except where a supervisory authority or a suspected personal data breach reasonably requires more;

(d) auditors must be bound by confidentiality obligations;

(e) audits must not extend to information of other customers or to our commercially confidential information not reasonably needed for the audit; and

(f) you will bear the reasonable costs of the audit, and our reasonable costs of supporting it, unless the audit reveals our material non-compliance with this Schedule.

12.3 **Written documentation in lieu of on-site audit.** As at the effective date of this Schedule, we do not hold independent third-party assurance certifications (such as SOC 2 or ISO 27001) for the Services. In place of an on-site audit, we will make available to you written documentation of our technical and organisational measures (including those summarised at Annex B), our sub-processor arrangements, and our incident and breach history relevant to Customer Personal Data. If we later obtain relevant third-party assurance reports, we may make those available instead of, or in addition to, that documentation; where a report reasonably addresses the scope of your audit request, it will satisfy our audit obligation for that period.

13. Return and deletion of Customer Personal Data

13.1 On termination of the Terms (or at any earlier point if you request), we will, at your choice:

(a) **return** Customer Personal Data to you in a reasonable machine-readable format; or

(b) **delete** Customer Personal Data from our production systems.

13.2 Return or deletion will take place within 30 days of your request or the termination date (whichever is earlier), except to the extent applicable law requires continued storage.

13.3 **Backups.** Deletion from backup systems will occur in accordance with our backup retention schedule. During that period, backups are not accessed for any purpose other than disaster recovery.

13.4 **Anonymised Benchmarking Commons records.** Anonymised records already written to the Benchmarking Commons do not contain personal data within the meaning of UK GDPR and are not subject to this clause. This consequence of opting in is explained to you at the point of opt-in and in the Privacy Policy.

13.5 **Audit log retention.** The audit log described in the Privacy Policy section 8 is retained for the same period as the related tender content. Where return or deletion of Customer Personal Data is requested under clause 13.1, audit log entries for the affected tenders are included in that return or deletion, subject only to any retention required by law or by a live dispute, investigation or regulatory request.

14. Data about contractors and other third parties

14.1 This clause supplements this Schedule in respect of personal data about individuals who are not your personnel and not your clients — in particular, contractors you invite through the Services or whose returns you upload.

14.2 You acknowledge that:

(a) contractor personal data introduced to the Services (whether by you, or directly by a contractor at the invitation gate) is Customer Personal Data within the meaning of this Schedule;

(b) you, as Controller, are responsible for the lawful basis on which that personal data is processed, including for the contractor having been given the information required under UK GDPR Articles 13 or 14 where applicable; and

(c) our processing of that personal data as Processor is on the terms of this Schedule.

14.3 The Privacy Policy contains information for contractors who receive invitation links, including how they can exercise their rights against us and against you. That information is in addition to, and does not reduce, your obligations under UK GDPR Articles 13 and 14 in respect of the contractor.

14.4 Our audit log (see Privacy Policy section 8) captures contractor IPs at specific state transitions. Our processing of those IPs is on the basis of our own legitimate interests (controller capacity) in fraud prevention, dispute resolution and audit trail — see Privacy Policy. The existence of this controller-capacity processing does not change our Processor status in respect of the rest of contractor personal data.

---

15. Liability and precedence

15.1 Liability of each party under this Schedule is subject to the limitations and exclusions set out in the Terms.

15.2 This Schedule forms part of the Terms. If there is any conflict between the Terms and this Schedule in respect of processing of personal data, this Schedule prevails.

15.3 If there is any conflict between this Schedule and any other data-protection-related document (including any DPA we have entered into with a Sub-processor), this Schedule prevails in respect of the relationship between you and us.

---

16. Standalone signing version

16.1 Where your firm's procurement processes require a wet-signed standalone version of this Schedule, we will provide a signing version on reasonable notice at no cost. Contact **hello@tendermark.ai**.

16.2 The signed standalone version will not change the substance of the obligations; it will reproduce the text of this Schedule with an appropriate signature block.

Annex A — Details of processing

Subject-matter of processing: Hosting, storing and processing Customer Personal Data as necessary to provide the Tendermark Services (extraction, normalisation and comparison of tender returns; invitation of contractors to price tenders online; generation of tender analysis reports; optional anonymised contribution to the Benchmarking Commons).

Duration of processing: For the duration of the Terms between the parties, and thereafter only in accordance with clause 13 and section 15 of the Privacy Policy.

Nature and purpose of processing: Storage, transmission, structured extraction, normalisation, comparison, aggregation (for anonymised benchmarking only), transactional email delivery to named contractors, audit logging, and generation of tender analysis report output.

Categories of data subjects:

- Your personnel and colleagues
- Your clients (insofar as they are individuals, or individuals associated with corporate clients)
- Contractors and their personnel (including those invited to price a tender and those whose returns you upload)
- Individuals whose names or other identifiers appear in free-text fields of tender content (for example, occupants of a property)

Types of personal data:

- Names, job titles, firm names
- Email addresses, phone numbers (if provided)
- Postal addresses (project or property addresses, client addresses where included)
- IP addresses of contractors at the state transitions captured by the audit log
- Professional context (trade, role, firm affiliation)
- Free-text notes and descriptions that may incidentally contain personal data
- Any special category or criminal offence data is out of scope — see clause 6.1(d)

Annex B — Technical and organisational measures

B.1 Encryption

- TLS for all data in transit to and from the Services.
- Encryption at rest for database and object storage, provided by our infrastructure sub-processors (Supabase and Cloudflare).

B.2 Access control

- Role-based access control at the application level (row-level security) so that users access only their own data.
- Production access to our infrastructure is restricted to a defined set of personnel.
- Multi-factor authentication is required for access to production systems.

B.3 Authentication and credentials

- Passwords are stored using modern password-hashing algorithms; plaintext passwords are never stored or logged.
- Session tokens are short-lived and invalidated on sign-out.
- Public-share and invitation tokens are 122-bit random identifiers generated via `crypto.randomUUID()`. Invitation token routes are rate-limited on both token and IP axes (60 requests per minute per axis by default, controlled by a feature flag). Share token routes are not rate-limited. Neither token type is included in analytics events or application logs.

B.4 Network security

- DDoS protection and TLS termination via Cloudflare.
- HTTPS enforced throughout the application.
- Hosting on Vercel with standard platform security controls.

B.5 Logging and audit trail

- Append-only audit log of state transitions on invitation and return events (see Privacy Policy section 8).
- Application and infrastructure logs retained for security monitoring; tokens and secrets are scrubbed from logs.

B.6 Vendor security

- Sub-processors are selected in part for their security posture.
- Written data-protection contracts are in place with each Sub-processor.

B.7 Incident management

- Documented incident response process.
- Breach notification within 72 hours as per clause 10.

B.8 Data minimisation and segregation

- The Benchmarking Commons is stored in a separate table with no personal data. Stripping runs before write (see Privacy Policy section 6).
- Backups are segregated and access-controlled.

B.9 Personnel

- All personnel who process Customer Personal Data are bound by written confidentiality obligations.
-

All personnel receive data protection training appropriate to their role, and are kept informed of updates to our data-protection practices.

B.10 Review

- We review these measures periodically and whenever there is a material change to the Services.

Annex C — Approved sub-processors

Current as of the effective date of this Schedule. We may update this list in accordance with clause 8.

Sub-processor	Purpose	Processing location	Transfer mechanism for transfers out of the UK
Supabase	Database, authentication, file storage	European Union (EU region)	Not required (UK adequacy for EEA)
Anthropic	AI-powered extraction, normalisation, analysis	United States	UK Addendum to EU SCCs, deemed executed on use (under Anthropic's DPA). Transfer Risk Assessment on file.
Stripe	Payment processing	United States	UK extension to the EU–US Data Privacy Framework (active certification); UK Addendum to EU SCCs as backup
Vercel	Application hosting	United States	UK extension to the EU–US Data Privacy Framework (active certification); UK Addendum to EU SCCs as backup
Cloudflare	DNS, CDN, DDoS protection	United States	UK extension to the EU–US Data Privacy Framework (active certification); UK Addendum to EU SCCs as backup
PostHog	Product analytics, feature flags	European Union (EU Cloud)	Not required
Resend	Transactional email delivery	European Union	Not required

Anthropic — no training on Customer Personal Data. Under Anthropic's commercial API terms as in force at the effective date of this Schedule, the data we submit (including Customer Personal Data contained in the content we send for analysis) is not used to train Anthropic's models.

Stripe — payment-card data. Stripe processes payment card data directly from the cardholder; we do not see or store full card numbers. Our use of Stripe is therefore principally for controller purposes (billing identification) rather than as a Sub-processor of Customer Personal Data, but Stripe is included in this Annex for completeness.