

Data Processing Agreement

Klimo AI LLC — Klimo Capture

Version 1.0 · 15 September 2026

This agreement covers how Klimo AI LLC ("Klimo", "we") handles the data you put into Klimo Capture ("the Service"). It forms part of the Terms of Service at <https://klimo.ai/terms>. Where this agreement and the Terms disagree about personal data, this agreement wins.

It is written to be read. Nothing in it is a summary of something longer held somewhere else.

1. Roles

You are the controller of the data you upload and enter. Klimo is the processor, and acts only on your instructions: using the Service **is** the instruction. We do not decide what your data is used for, and we do not use it for our own purposes.

2. What is processed

- **Solicitation documents** you upload. These are public procurement records.
- **Your company profile** — the Vault: legal identity and registration numbers, codes, certifications, insurance types and limits, past performance, key personnel, capacity, and revenue history.
- **Account data**: the email address of each person with a seat, their role, and a record of sensitive reads and exports.

What is never processed, because it is never collected: Social Security or taxpayer identification numbers, bank or routing numbers, government identification numbers, and classified, CUI or ITAR-marked material. Uploads are scanned for those markings and for Social Security number patterns, and a file that trips the check is deleted rather than stored.

The people whose personal data may appear are your own staff and the references and contacts you choose to enter.

3. Where it is processed

In the United States. The database and file storage are Supabase; the application and background jobs run on Railway; the website is served by Vercel.

4. Subprocessors

Subprocessor	Purpose
Supabase	Database, file storage, authentication
Anthropic	The AI that reads packets and reasons about fit
Railway	Application and background jobs
Vercel	Website hosting
Resend	Deadline emails
Twilio	Deadline text messages, where enabled
Telegram	Operator alerts to Klimo staff. No customer data.

We will tell you before adding a subprocessor that processes your data, and you may object; if we cannot resolve the objection you may terminate and take an export with you.

Anthropic, specifically. Their commercial API retention is 30 days by default, and retained data is never used for training. We do not use the Batch API for your documents and never route them through a Covered Model. Anthropic may retain data flagged by their automated trust and safety systems for up to two years, or where required by law.

5. Security measures

- Row-level security in the database: your company's rows are unreadable to any other company, enforced by policy rather than by application code, and proven by an automated test suite on every change.
- Encryption at rest, and TLS 1.2 or better in transit.
- Signed, expiring download links: five minutes for a document, 24 hours for an export.
- Two-factor authentication available on every account, required on Team accounts.
- Role separation, including a read-only counselor seat that cannot see revenue or insurance limits and cannot export.
- Virus scanning before any file is read.
- An audit record of every read of financial data and every export.
- Error reports carry no IP address, no location, no request contents and no document or Vault text.
- Daily backups of the database and uploaded files, with 30-day retention.

6. Personnel

Access to production data is limited to Klimo staff who need it to operate the Service, and is subject to confidentiality obligations that survive the end of their engagement.

7. Your rights over the data

- **Export.** You can export everything at any time from Settings: a JSON file of every row your company owns and a ZIP of every file you uploaded.
- **Deletion.** An owner can delete the account from Settings. Rows, stored files and export artifacts are removed within seven days.
- **Assistance.** If someone whose personal data you entered makes a request to you, we will help you answer it. Because you can read, export, correct and delete everything yourself, most requests need nothing from us.

8. Retention

We keep your data while your account is open. Our policy is to keep nothing longer than 12 months after a solicitation's close date. Export artifacts expire after 24 hours. On deletion, see section 7.

9. Breach notification

If we become aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, or unauthorised disclosure of or access to your data, we will notify you without undue delay and in any case within 72 hours of becoming aware, with what we know, what we are doing, and what we suggest you do.

10. Audits

On reasonable notice, and no more than once a year unless required by a regulator, we will answer a written security questionnaire and provide the documentation we have. Klimo does not hold a SOC 2 report or a FedRAMP, TX-RAMP or StateRAMP authorisation, and does not claim to.

11. End of the agreement

When your account ends, you may export your data. After that we delete it as described in section 7, except where the law requires us to keep something, in which case it stays subject to this agreement for as long as we hold it.

12. Liability and law

Liability under this agreement is subject to the limitations in the Terms of Service. Texas law governs.

Contact

security@klimo.ai — Klimo AI LLC, Texas, United States.