

Clave — Privacy Policy

Version: 2025-09-09 • Effective: 09 September 2025 • Applies through: 09 September 2026 (or until replaced)

This Privacy Policy explains how Clave (“Company,” “we,” “our,” “us”) collects, uses, shares, and protects personal data when you use the Service. If you do not agree with this Policy, do not use the Service.

Summary: We use your data to provide and improve the Service. We do not sell personal data. We do not use Customer Content to train models unless you explicitly opt in.

1) Data We Collect

- Account: name, email, auth identifiers, timezone/locale.
- Collaboration: project names/descriptions, member emails/roles.
- Customer Content: notes, templates, recordings, transcripts, chat messages, attachments, action items, highlights.
- Integrations: configuration and scopes for connected services you authorize.
- Usage/Logs: device, IP, timestamps, pages viewed, crash/performance metrics.
- Cookies: session, preference, analytics (where permitted).
- From third parties at your direction: calendar events and participants, metadata from GitHub/Notion/Jira/Linear/Slack/Telegram/Google services.
- Sensitive data: not required; if you include it in content, we process only to provide the Service.

2) How We Use Data

Provide, operate, and maintain the Service; generate agendas/summaries/insights/action items you request; index content for search (including vector embeddings); connect/sync integrations; communicate about updates and support; prevent abuse/security incidents; analyze usage; comply with law and enforce Terms.

Model Training: No use of Customer Content to train models unless you opt in in settings or via separate agreement. We may use de-identified, aggregated telemetry for improvement.

3) Legal Bases (GDPR/UK GDPR)

Performance of contract; legitimate interests (security, improvement); consent (integrations, recording/transcription, marketing, model-training opt-in); legal obligations.

4) Sharing

Service providers/subprocessors under DP terms; third-party integrations you connect (only as necessary to fulfill actions such as creating issues or posting messages); model/API providers used to generate outputs under contractual/technical safeguards; professional advisers; authorities where required by law; business transfers with notice where required. We do not sell personal data.

5) International Transfers

We may transfer data internationally using appropriate safeguards (e.g., SCCs).

6) Retention

We retain data while the account is active and as necessary for the purposes described. Typical periods: logs 12–24 months; backups 30–90 days; billing records up to 7 years. Deleted content leaves production promptly and is purged from backups on their cycle.

7) Security

Administrative, technical, and physical measures, including encryption in transit and at rest where applicable, access controls, audit logging, and vulnerability management. No method is 100% secure.

8) Your Rights

Depending on your location: access, rectify, delete, port, object/restrict, and withdraw consent. Exercise rights via hello@clave.so. We will verify identity. Authorized agent requests (e.g., under CCPA/CPRA) are supported.

9) Cookies

We use necessary cookies and, where required, analytics cookies with consent. You can manage cookies in the app and your browser.

10) Children

The Service is not intended for children under 16 (or older where required).

11) Third-Party Services

Your use of connected services is governed by their policies. Google Limited Use: our use of Google API data complies with the Google API Services User Data Policy.

12) Communications

Transactional communications are required to operate the Service. Marketing emails require consent and include an opt-out.

13) Changes

We may update this Policy; material changes will be notified. Continued use after the effective date constitutes acceptance.

Controller/Contact

Email: hello@clave.so