Security Overview

COMPLIANCE

Standards we hold ourselves accountable to.

We publish what we've achieved, what we're auditing, and what's on the roadmap. No claims without evidence.

SOC 2: Audit roadmapped — Type I target Q1 2027, Type II target Q4 2027. Annual recertification thereafter.

GDPR: Aligned — Operates in accordance with EU GDPR principles. DPA available on request.

CCPA: Aligned — California Consumer Privacy Act rights honored for all California users.

ISO 27001: Roadmapped — Planned after SOC 2 Type II completion.

DATA HANDLING

What we keep, for how long .

Every category of data we touch, where it lives, and when it's deleted. Defaults are conservative; workspaces can tighten them.

Meeting audio	Streamed for live transcription and processed in memory only — audio is never written to storage. Sageio does not use it to train models.
Transcripts & translations	Stored in your workspace until you delete them or the account is deleted.
Summaries & action items	Stored alongside the source transcript and follow the same retention policy.
Account & workspace metadata	Retained while the account is active. Deleted within 30 days of account closure or a verified deletion request.
Billing data	Payments processed by LemonSqueezy as Merchant of Record. Sageio stores subscription metadata only — never payment card details.
Data residency	Multi-region deployment available. EU, US, and Asia-Pacific regions supported on Enterprise plans.
Internal access	Production access requires explicit business need, is time-bound, and is logged for audit.

ENCRYPTION

Modern protocols, no exceptions .

Encryption is a default, not a tier. The standards below apply to every workspace, on every plan.

- TLS 1.3 for every client connection, with HSTS enforced on Sageio domains.
- AES-256-GCM at rest across application databases and object storage.
- Provider-managed encryption keys via AWS KMS, rotated on schedule.
- Meeting audio encrypted on the wire from bot to processing layer.

- Encrypted backups, retained 30 days, restored on a tested schedule.

ACCESS CONTROLS

The keys to your workspace, on your terms .

Identity, roles, and audit trails configured the way enterprise IT teams expect. Not bolted on — built in from the first user.

- SAML 2.0 single sign-on, available on Enterprise plans.
- OIDC sign-in via Google and Microsoft for self-serve workspaces.
- Role-based access control with four tiers: Owner, Admin, Member, and Viewer.
- Audit log of every admin and data-access action, retained 12 months.
- Configurable session timeout and IP allowlist on Enterprise plans.

SUB-PROCESSORS

The vendors we depend on, named publicly .

Sageio relies on a small set of established providers for storage, identity, and AI processing. The full list, with purpose and data location, lives in the DPA.

INCIDENT RESPONSE

When something breaks , you hear from us first.

Customer notification is the first hour of response, not the last. Affected customers get direct notice and ongoing updates until resolution.

Detection runs via continuous monitoring. On-call engineers declare and assign an incident commander within 30 minutes. For any incident involving customer data, affected customers are notified by email within 24 hours of confirmation, with interim updates while investigation continues. A written post-incident review is shared within 7 days.