

Data Processing Agreement

Version v1.2.1 · Effective from publication date

SCOPE & ROLES

Who does what , with whose data.

Under this DPA, the Customer is the data controller and Sageio acts as a processor on the Customer's behalf. Sageio processes personal data only to deliver the contracted services — real-time meeting translation, transcription, and summarization — and only under the Customer's documented instructions. This DPA forms part of the Subscription Agreement between Sageio and the Customer; in the event of conflict, the DPA prevails for matters of personal data processing. It applies to all processing activities carried out in connection with the Sageio platform.

DATA PROCESSED

What we process, and why we may .

| Category of data | Purpose of processing | Legal basis (GDPR Art. 6) | Retention |
|---|--|---|--|
| Meeting audio | Speech-to-text transcription and translation during the meeting. | Art. 6(1)(b) — performance of contract. | Streamed for live transcription and processed in memory only; never written to storage. Not used for model training. |
| Meeting transcripts & translations | Storage and retrieval by the Customer's workspace members. | Art. 6(1)(b) — performance of contract. | Retained until deleted by the Customer or upon account deletion. |
| Summaries & action items | AI-generated meeting outputs derived from the transcript. | Art. 6(1)(b) — performance of contract. | Follows the transcript retention. |
| Account identifiers (name, email, role) | Authentication, workspace access, and audit logging. | Art. 6(1)(b) — performance of contract. | Duration of the account plus 30 days after closure. |
| Workspace & usage metadata | Service operation, billing reconciliation, and abuse prevention. | Art. 6(1)(b) and Art. 6(1)(f) — legitimate interest in service integrity. | 12 months from generation. |
| Audit logs | Security monitoring and Customer access review. | Art. 6(1)(f) — legitimate interest in security. | 12 months from generation. |
| Billing identifiers | Subscription management. Payment card data is processed by LemonSqueezy as Merchant of Record and is not stored by Sageio. | Art. 6(1)(b) — performance of contract. | Duration of the account plus 7 years for tax records. |

SUB-PROCESSORS

The full chain of custody .

| Sub-processor | Purpose | Processing location |
|---------------------|--|---|
| Amazon Web Services | Cloud hosting, object storage, encryption key management. | Customer-selected region (default: Singapore, Asia-Pacific). EU and US on Enterprise plans. |
| Neon | Managed PostgreSQL database for application data. | Region matched to Customer's primary AWS region. |
| Vercel | Hosting for marketing site and customer-facing web application. | Global edge network. Origin: customer-selected region. |
| Clerk | Authentication, single sign-on, and identity management. | United States. |
| Deepgram | Speech-to-text transcription of meeting audio. | United States. |
| OpenAI | Real-time speech-to-text transcription of meeting audio (default engine for new workspaces) and transcription of uploaded audio files. | United States. |
| DeepL | Translation of interim transcript segments and final translation for selected target languages. | Germany (EU). |
| Google (Gemini API) | Translation refinement of finalized transcript segments; AI-generated summaries and action items. | United States. Data not used to train Google models per paid-tier Gemini API terms. |
| Resend | Transactional email delivery (account and service notices; meeting-summary emails sent at the user's request). | United States. |

Plausible (cookieless website analytics) operates only on our marketing site and does not process platform personal data under this DPA; it is disclosed in the Privacy Policy.

Lemon Squeezy (a Stripe company) is not a sub-processor: as Merchant of Record it determines its own purposes for payment, tax, and invoicing, and acts as an independent data controller under its own privacy policy.

PROCESSOR COMMITMENTS

Article 28, written into the contract .

Sub-processor changes

Sageio maintains the current sub-processor list at sageio.net/subprocessors. Sageio will give Customer at least 30 days' notice (by email or in-app notice) before adding or replacing a sub-processor. Customer may object on reasonable data-protection grounds within the notice period; if the parties cannot resolve the objection, Customer may terminate the affected services and receive a pro-rata refund of prepaid fees for the unused period. Sageio imposes data-protection obligations equivalent to this DPA on each sub-processor and remains liable for their performance.

Personal-data breach notification

Sageio will notify Customer without undue delay, and in any event within 24 hours of confirming a personal-data breach affecting Customer personal data, and will provide the information reasonably required for Customer's obligations under Articles 33–34 GDPR, with updates as the investigation proceeds.

Deletion and return

Upon termination or expiry of the services, Sageio will, at Customer's choice, delete or return all Customer personal data within 30 days, and delete remaining copies, except where applicable law requires retention. Personal data in encrypted backups is purged on the standard 30-day backup rotation cycle.

Assistance and audits

Taking into account the nature of the processing, Sageio will assist Customer with appropriate technical and organizational measures in responding to data-subject requests, and with Customer's obligations under Articles 32–36 GDPR, including data-protection impact assessments and prior consultations. Sageio will make available information reasonably necessary to demonstrate compliance with Article 28 — including summaries of penetration tests and, when available, audit reports — and will allow audits, including inspections, by Customer or its mandated auditor, no more than once per twelve months, on 30 days' notice, at Customer's expense and subject to confidentiality.

Confidentiality and instructions

Sageio ensures that persons authorized to process personal data are committed to confidentiality. Sageio will inform Customer without undue delay if, in its opinion, an instruction infringes applicable data-protection law.

Customer warranties

Customer warrants that it has established a lawful basis for the processing it instructs under this DPA, including any notices to and consents from meeting participants required by applicable law and — where meeting content incidentally contains special categories of personal data — a condition under Article 9(2) GDPR. Sageio does not use meeting content to identify any person by voice and creates no biometric templates.

Term, governing law, and liability

This DPA takes effect with, and lasts for the duration of, the Subscription Agreement; it is governed by the same law, and the limitations of liability in the Terms of Service apply to it, except where mandatory data-protection law provides otherwise.

These commitments form part of the DPA. The English text is the authoritative version; localized translations will follow the signed-off text.

SECURITY MEASURES

Engineering meets commitment .

Sageio implements technical and organizational measures appropriate to the risk of processing, including encryption in transit (TLS 1.3) and at rest (AES-256-GCM), role-based access control, audit logging, regular penetration testing, and a documented incident response process. Production access requires explicit business justification, is time-bound, and is logged. The complete catalog of measures, including current compliance program status, is published on the Security page and updated as the program evolves.

INTERNATIONAL TRANSFERS

Cross-border data, lawfully moved .

Where personal data is transferred outside the European Economic Area, the United Kingdom, or other jurisdictions with equivalent restrictions, Sageio relies on the European Commission's Standard Contractual Clauses (Module Two: Controller-to-Processor) and, where applicable, the UK International Data Transfer

Addendum. For transfers to jurisdictions covered by an adequacy decision, Sageio relies on that decision. Sub-processors are bound to equivalent obligations through contractual flow-down. Transfer impact assessments are conducted for each sub-processor processing personal data outside the data exporter's jurisdiction.

The SCCs (Module Two: Controller-to-Processor) and the UK International Data Transfer Addendum are incorporated into this DPA by reference. Annex I (parties; description of processing) is constituted by the parties' details and the "Data processed" table above, which may incidentally include special categories of data contained in meeting content; Annex II (technical and organizational measures) by the "Security measures" section; Annex III (authorized sub-processors) by the "Sub-processors" table. In case of conflict, the SCCs prevail.

DATA SUBJECT RIGHTS

Your users' rights , our obligations.

- Right of access — confirmation and a copy of personal data processed.
 - Right to rectification — correction of inaccurate or incomplete data.
 - Right to erasure — deletion within 30 days of a valid request, subject to legal retention requirements.
 - Right to restriction — limitation of processing in defined circumstances.
 - Right to data portability — export in a structured, machine-readable format.
 - Right to object — including to processing based on legitimate interest.
 - Right to lodge a complaint with the relevant supervisory authority.
-

CONTACT

Real people, named inboxes .

Sageio is operated by 好客網路股份有限公司 (Unified Business No. 29041135), a company registered in Taiwan. Registered address: No. 205, Hulin Street, Xinyi District, Taipei City, Taiwan (臺北市信義區虎林街205號). Privacy contact: privacy@sageio.net.

Privacy: privacy@sageio.net · Security: security@sageio.net

Sageio — cross-language meetings, without the language barrier. This document reproduces the content published at sageio.net.