Data Processing Agreement (DPA) - VOOK SAS

Version 2026-09

Data Processing Agreement Scope

This Data Processing Agreement ("DPA") supplements Vook's Terms of Service available at vook.ai/en/terms-of-service (the "Agreement"). It is entered into between you and the entity you represent ("Customer", "you" or "your", and referred to as the "Controller" in the Annexes) and Vook SAS, a French société par actions simplifiée with a share capital of 5,000 euros, whose registered office is at 10 rue Vandrezanne, 75013 Paris, France, registered with the Paris Trade and Companies Register under number 980 855 027 (EU VAT number FR59980855027), acting as processor within the meaning of Regulation (EU) 2016/679 (the "GDPR") ("Vook").

Acceptance of Vook's Terms of Service by the Customer constitutes acceptance of this DPA. No signature is required for this DPA to take effect. Continued use of the Service constitutes continued acceptance.

Recitals

Vook operates a transcription and audio/video analysis service (the "Service"). The Customer uses the Service, which entails the processing of personal data by Vook on the Customer's behalf.

Within the meaning of Regulation (EU) 2016/679 (the "GDPR"), the Customer acts as controller and Vook acts as processor. This DPA is entered into pursuant to Article 28 GDPR and governs that processing. It supplements the main service agreement defined in Article 10.

Now, therefore, the parties have agreed as follows:

Article 1. Definitions

The terms "personal data", "processing", "controller", "processor", "sub-processor", "data subject", "personal data breach", and "supervisory authority" have the meanings given to them in the GDPR. "Sub-processor" means any third party engaged by Vook to process personal data under this DPA. The "Standard Contractual Clauses" or "SCCs" means the EU standard contractual clauses adopted by Commission Implementing Decision (EU) 2021/914. Unless otherwise stated, references to articles ("Art.") in this DPA and its annexes are to articles of the GDPR.

Article 2. Details of the processing (Art. 28(3))

- **Subject matter:** provision of the Service to the Customer.
- **Duration:** for the term of the main service agreement and until deletion or return of personal data under Article 8.
- **Nature and purpose:** hosting, transcription, speaker diarization, optional AI summarization/chat, storage, and transmission of Customer content, solely to provide the Service.
- **Types of personal data:** account/identity data (name, email, OAuth identifiers); billing data (name, postal address); usage/technical metadata (IP, request/session data, transcription titles and file names); and **Customer content** (audio/video files,

transcripts, summaries, chat) which may contain personal data and, incidentally, special-category data within that content.

- **Categories of data subjects:** the Customer's authorized users and any individuals appearing in the Customer's uploaded content.
- Full processing details: Annex 1, including the SCC Annexes I to III values.

Article 3. Obligations of Vook (Art. 28(3))

Vook shall:

(a) **Documented instructions:** process personal data only on the Customer's documented instructions (including for transfers), unless required by EU or Member State law, in which case Vook informs the Customer unless legally prohibited. This DPA and the Customer's use of the Service constitute the initial instructions.

(b) **Confidentiality:** ensure that persons authorized to process personal data are bound by confidentiality (see Annex 2 and Article 5 below).

(c) **Security:** implement the technical and organizational measures set out in Annex 2, in accordance with Art. 32.

(d) **Sub-processors:** engage sub-processors only under the conditions of Article 4.

(e) **Data subject rights:** assist the Customer, by appropriate technical and organizational measures and insofar as possible, in responding to data-subject requests under Chapter III GDPR (Article 7).

(f) **Assistance:** assist the Customer in ensuring compliance with Art. 32 to 36 (security, breach notification, data protection impact assessment (DPIA), prior consultation), taking into account the nature of the processing and the information available to Vook.

(g) **Deletion / return:** at the Customer's choice, delete or return personal data at the end of the provision of the Service, in accordance with Article 8 and Annex 3.

(h) **Compliance evidence and audits:** make available the information necessary to demonstrate compliance with Art. 28, and allow for and contribute to audits, in accordance with Article 9.

Article 4. Sub-processors

- The Customer grants Vook general written authorization to engage sub-processors. The current list is set out in Annex 4.
- Vook imposes on each sub-processor, by contract, data-protection obligations substantially equivalent to those of this DPA (Art. 28(4)), as documented in Annex 4, and remains fully liable to the Customer for the performance of its sub-processors' obligations.
- Vook informs the Customer of any intended change (addition or replacement of a sub-processor) at least 30 days in advance, by updating the publicly maintained sub-processor list at https://vook.ai/en/sub-processors and, for Customers who have registered a data-protection contact with Vook, by email to that contact. The Customer may object within that period on reasonable data-protection grounds and, absent an agreed alternative, may terminate its subscription without penalty.

Article 5. Confidentiality

All persons (founders; personnel of sub-processors) authorized to access personal data are bound to confidentiality by contract or statutory duty. Within Vook, production access is restricted to a single named administrator (see Annex 2, §1.1).

Article 6. International transfers

Processing between the Parties under this DPA does not itself involve a transfer outside the EU/EEA: Vook is established in France, and primary storage and compute are EU-located. The SCCs apply in two situations:

- **Onward transfers to sub-processors.** Where a sub-processor listed in Annex 4 is established outside the EU/EEA or subject to third-country law, the transfer is governed by the SCCs, Module 3 (processor to processor), concluded between Vook and that sub-processor through the sub-processor's own data processing agreement, and supplemented by the technical measures of Annex 2 (TLS in transit, AES-256 per-user encryption of content at rest).
- **Data Privacy Framework.** Where a sub-processor is certified under the EU–U.S. Data Privacy Framework ("DPF"), the DPF adequacy decision provides the primary transfer basis for personal data transferred to that sub-processor, with the SCCs

applying as a fallback. The sub-processor list at https://vook.ai/en/sub-processors states, per sub-processor, which mechanism applies.

- **Customers established outside the EU/EEA.** Where the Customer is established outside the EU/EEA, the SCCs, Module 4 (processor to controller), are incorporated into this DPA by reference for data flows from Vook to the Customer (including the Customer's remote access to data hosted by Vook), completed with the SCC Annex I values set out in Annex 1. For Customers established in the United Kingdom, the UK International Data Transfer Addendum applies in addition; for Customers established in Switzerland, the SCCs apply as adapted per the FDPIC's requirements.

Vook documents its assessment of destination-country laws and supplementary measures (SCC Clause 14) in Annex 5, an informational annex updated together with the sub-processor list and provided to assist the Customer's own transfer assessment.

Vook does not warrant a blanket exclusion of processing outside the EU/EEA. Primary storage and compute are EU-located, but certain sub-processors are US-incorporated companies, and AI summarization/chat sends content to a US-incorporated provider only on the user's explicit, consented action. Where the Customer subscribes to the EU-residency option for the AI feature, AI summaries and chat run on an EU endpoint, so content sent to the AI feature is processed within the EU geography (see Annexes 4 and 5).

Article 7. Data subject rights and breach notification

- **Assistance with rights:** Vook assists the Customer in fulfilling data-subject requests (access, rectification, erasure, portability, restriction, objection) under Chapter III, by means of the Service's features and operator support. Export and return are performed by the user through the in-product self-service export, for one or several transcripts at a time (PDF/DOCX/SRT/JSON/HTML/MD, chat, original audio; JSON, as a structured, machine-readable format, satisfies the portability requirement of Art. 20 GDPR). Content is per-user encrypted and cannot be decrypted by Vook, except for users who have explicitly requested that a recovery key be retained, an opt-in feature allowing account-access recovery (transcription titles and file names, as mere metadata, are however stored in cleartext); there is therefore no operator-side plaintext extract of content, and the Customer's return on termination is satisfied by its users' self-service export (see Annex 3, §2).

- **Personal data breach:** Vook notifies the Customer without undue delay, and in any event within 48 hours of becoming aware of a personal data breach affecting the

Customer's data, with the information available, and cooperates on remediation and on the Customer's obligations under Art. 33 and 34.

Article 8. Deletion and return

On termination of the Service, Vook deletes or returns the Customer's personal data in accordance with Annex 3, subject to legal-retention obligations (invoices, 10 years) and the backup-rotation window. Deletion is completed within 30 days of the request and confirmed to the Customer in writing.

Article 9. Audits

(a) **Information.** Vook makes available to the Customer all information necessary to demonstrate compliance with Art. 28 GDPR: this DPA and its annexes, the technical and organizational measures documentation (Annex 2), the sub-processor list and the status of each sub-processor's DPA (Annex 4), the transfer assessment (Annex 5), and the certifications published by its infrastructure sub-processors. Vook additionally answers one written security/compliance questionnaire from the Customer per 12-month period, within 30 days.

(b) **Audit (documentation first).** Audit requests are satisfied in the first instance by the documentation referred to in (a). Where the Customer reasonably shows that documentation to be insufficient, or following a personal data breach affecting the Customer's data, or where a supervisory authority requires it, the Customer (or an independent auditor it mandates, which must not be a competitor of Vook and must be bound to confidentiality) may audit Vook's compliance with this DPA, under the following conditions:

- at most once per 12-month period (this limit does not apply after a breach affecting the Customer's data or where a supervisory authority requires it);
- 30 days' prior written notice, with scope and duration agreed in advance;
- conducted remotely by default, during business hours, limited to one business day, without unreasonably disrupting Vook's operations;
- scope limited to what is necessary to verify compliance with this DPA in respect of the Customer's personal data. It does not extend to: (i) other customers' data, which the auditor cannot read in any event since content is per-user encrypted (Annex 2); (ii) Vook's internal financial information;

(iii) direct audits of sub-processors; for those, Vook provides the sub-processor's certifications and audit reports available under its own DPA (Annex 4).

(c) **Costs.** Each Party bears its own costs; the Customer bears its auditor's fees. Vook's assistance beyond one business day per 12-month period may be charged at its standard rates, unless the audit reveals a material non-compliance by Vook with this DPA, in which case Vook bears its own assistance costs.

(d) **Findings.** Audit results are confidential, are shared with Vook, and may be used only to verify and remediate compliance with this DPA. Vook remediates any confirmed non-compliance under a remediation plan agreed without undue delay.

Article 10. Liability, term, governing law, precedence

- **Main agreement.** Where the Parties have not signed a separate master services agreement, the "main service agreement" means Vook's Terms of Service together with the quote or order form accepted by the Customer. This Article 10 is self-contained so that it applies fully in that configuration. Acceptance of Vook's Terms of Service by the Customer constitutes acceptance of this DPA in full.

- **Term.** This DPA applies for as long as Vook processes personal data on the Customer's behalf, and survives as to the deletion and return obligations (Article 8).

- **Liability towards data subjects (Art. 82 GDPR).** Statutory and unaffected by this DPA: Vook is liable to data subjects for damage caused by processing only where it has not complied with GDPR obligations specifically directed to processors, or where it has acted outside or contrary to the Customer's lawful instructions.

- **Recourse between the Parties (Art. 82(5)).** Where a Party has paid full compensation to a data subject, it is entitled to claim back from the other Party the part of the compensation corresponding to that other Party's share of responsibility for the damage.

- **Administrative fines.** Each Party bears the administrative fines imposed on it by a supervisory authority.

- **Liability cap.** Each Party's total aggregate liability to the other Party under or in connection with this DPA, all claims and causes combined, is limited to the total

amounts paid or payable by the Customer for the Service during the twelve (12) months preceding the event giving rise to liability.

- **Exclusion of indirect damages.** Neither Party is liable to the other for indirect or consequential damages, including loss of profits, revenue, business, goodwill, or anticipated savings.
- **Mandatory-law carve-outs.** Nothing in this DPA limits or excludes a Party's liability for wilful misconduct (*dol*) or gross negligence (*faute lourde*), for bodily injury, or for any other liability that cannot be limited or excluded under applicable law.
- **Governing law / jurisdiction.** This DPA is governed by French law. Any dispute relating to its validity, interpretation, or performance falls within the jurisdiction of the courts within the purview of the Paris Court of Appeal.
- **Order of precedence (data-protection matters).** The SCCs prevail over this DPA, which prevails over the main service agreement.

Annexes

The following annexes form an integral part of this DPA:

- **Annex 1:** details of processing and SCC Annexes I to III values;
- **Annex 2:** technical and organizational measures;
- **Annex 3:** data deletion and return;
- **Annex 4:** sub-processor list;
- **Annex 5:** transfer impact assessment (informational annex, updated with Annex 4 under the mechanism of Article 4).

Annex 1: Details of Processing and SCC Annexes I to III

Annex to the Vook Data Processing Agreement (Art. 28(3) GDPR). Part 1 gives the details of processing required by Art. 28(3). Part 2 provides the values for SCC Annexes I to III (the annexes to the EU Standard Contractual Clauses, Commission Implementing Decision (EU) 2021/914), incorporated by DPA Article 6 for transfers outside the EU/EEA. Bracketed [...] fields are completed per customer.

Part 1: Details of processing (Art. 28(3))

- **Subject matter:** provision of the Vook transcription and audio/video analysis service (the "Service") to the Controller.
- **Duration:** the term of the main service agreement, and until deletion or return of personal data under DPA Article 8 and Annex 3.
- **Nature of processing:** hosting; audio/video transcription; speaker diarization; optional AI summarization and chat (triggered per user action, consent-gated); storage (AES-256 per-user encrypted for content; transcription titles and file names are cleartext metadata); transmission; deletion.
- **Purpose:** solely the provision of the Service to the Controller; no advertising use, no training of AI models on Controller content.
- **Types of personal data:**
    - account/identity data: name, email, OAuth identifiers;
    - billing data: name, postal address (captured at purchase);
    - usage/technical metadata: IP address, request/session data, product events, transcription titles and file names (stored in cleartext);
    - **Controller content:** audio/video files, transcripts, summaries, chat, which may contain any personal data appearing in recorded speech, including, incidentally, special categories (Art. 9).
- **Special-category data:** not requested or intentionally processed; may be incidentally contained in Controller content. Safeguards: per-user AES-256 encryption at rest (Vook holds no decryption key, unless the user has explicitly

requested the recovery-key option), TLS in transit, strict purpose limitation, EU-located storage and EU/EEA-located inference, per-user access isolation.

- **Categories of data subjects:** the Controller's authorized users, and any individuals appearing in or identifiable from the Controller's uploaded content.
- **Location of processing:** primary storage and application compute in the EU (Paris), hosted on Scaleway, a French provider certified ISO 27001, SOC 2, and HDS (Hébergeur de Données de Santé). These certifications are the host's; **Vook holds no certification of its own**. Transcription inference runs on EU/EEA GPU workers. Specific functions rely on non-EU/EEA sub-processors under SCCs (Annex 4); Controller content never reaches the transactional-email or frontend-hosting providers. No blanket EU/EEA exclusion is warranted (DPA Article 6).
- **Paid EU-residency option for the AI feature:** on subscription to this option, AI summaries/chat run on an EU endpoint (Vertex AI, EU multi-region), so content sent to the AI feature is processed within the EU geography. Activation is performed for the Controller upon subscription.
- **Retention:** content: until deleted by the user/Controller or account closure (then erased per Annex 3); accounts inactive for more than two (2) years: deleted automatically after prior notice, under the same erasure as Annex 3; invoices: 10 years (French accounting law); deleted-account email hash: 12 months (anti-abuse); analytics events: 13 months, then anonymous aggregates; backups: 30-day rotation; operational logs: 15 days.

Part 2: SCC Annexes I to III

Module selection :

- **EU/EEA-established Controller:** the Controller-to-Vook relationship is EU-to-EU; **no SCCs apply between the Parties** (no Chapter V transfer; the DPA itself suffices).
- **Onward transfers** from Vook to non-EU/EEA sub-processors (Annex 4): Module 3 (processor to processor), concluded through each sub-processor's own DPA, which incorporates its SCCs (documented in Vook's DPA register, available on request).
- **Controller established outside the EU/EEA:** Module 4 (processor to controller) incorporated by reference into the DPA (Article 6) for flows from Vook back to the Controller, completed with the SCC Annex I values below. UK Controllers: the UK International Data Transfer Addendum applies in addition. Swiss Controllers: SCCs as adapted per FDPIC requirements.

SCC Annex I.A: List of parties

- **Data exporter: Vook SAS**, 10 rue Vandrezanne, 75013 Paris, France (as processor making an onward transfer). Contact: CTO, jeremy@vook.ai.
- **Data importer(s):** the non-EU/EEA sub-processors listed in Annex 4, each with its role, entity, and processing location.

SCC Annex I.B: Description of transfer

- **Categories of data subjects:** end users (account holders), business customers' authorized users, and individuals appearing in uploaded content.
- **Categories of personal data:** account/identity data (name, email, OAuth identifiers); usage and technical metadata (IP, request/session data); user content in transit (transcripts/audio; AES-256 encrypted at rest, not retained on compute). Payment/card data flows directly to Stripe/PayPal and is not transferred by Vook.
- **Sensitive data:** not requested or intentionally processed; user-generated transcripts may incidentally contain it. Safeguards: encryption in transit and at rest, strict purpose limitation, role-based access restriction, ephemeral handling on compute.

- **Frequency:** continuous (per request, for the duration of the Service).
- **Nature of processing:** hosting/execution of application compute; storage and transmission incidental to providing the Service; for Google Gemini only, LLM inference on transcript text sent on explicit, consented user action.
- **Purpose:** providing the Vook transcription service.
- **Retention:** duration of the contract; no separate vendor retention beyond the Service (see Part 1 for Vook-side retention).
- **Onward transfers:** only to the sub-processors in Annex 4, under equivalent obligations (DPA Article 4).

SCC Annex I.C: Competent supervisory authority

CNIL (Commission Nationale de l'Informatique et des Libertés), France, the supervisory authority of the data exporter's establishment.

SCC Annex II: Technical and organizational measures

The measures in Annex 2 apply in full: encryption in transit (TLS) and at rest (AES-256 per-user keys, bcrypt password hashing), single-administrator production access, database network isolation, per-user data isolation, admin audit trail, EU backups, erasure pipeline with 30-day SLA.

SCC Annex III: List of sub-processors

Annex 4 references the current list of sub-processors published at https://vook.ai/en/sub-processors, which sets out for each sub-processor: name, role, personal data processed, processing location, entity, transfer basis, and DPA status.

Annex 2: Technical and Organizational Measures (TOM)

Annex to the Vook Data Processing Agreement (Art. 28 / Art. 32 GDPR). Describes the technical and organizational measures Vook (processor) maintains to protect personal data processed on the controller's behalf.

0. Overview

Vook is operated by a 3-founder team with no employees or external contractors. Production infrastructure is fully cloud-hosted in the EU/EEA. Production access is restricted to a single named administrator. The measures below follow the structure of Art. 32(1) GDPR.

1. Confidentiality

1.1 Access control

- **Named accounts** on every service; no shared accounts (except the contact@vook.ai support inbox, shared by the three founders).
- **2FA** enforced on all administrative accounts.
- **Production access restricted to a single named administrator.** The other two founders have development-environment access only. Application secrets are separated between dev and prod.
- **Database network isolation:** the production PostgreSQL instance has no public IP and is reachable only over a private network; there is no public endpoint.
- **Analytics** requires per-founder named login over HTTPS.

1.2 Encryption

- **In transit:** TLS/HTTPS enforced on all public and internal web surfaces. HTTP is redirected to HTTPS (force_https); certificates are issued and auto-renewed by the hosting providers (Let's Encrypt / provider-managed).
- **At rest:** user content (audio files, transcripts, derived artifacts) is encrypted with AES-256 before storage, under per-user key material. Transcription titles and file names are not part of the encrypted content: they are stored as cleartext metadata (and are nulled on account deletion). Passwords are hashed with bcrypt. Where the user has explicitly requested it (opt-in recovery option), a recovery copy of their encryption key is retained, wrapped via Scaleway Key Manager, to allow account-access recovery; otherwise Vook retains no key able to decrypt content.

- **Tokens:** each JWT type has its own secret, separated between dev and prod.

1.3 Data minimization & pseudonymization

- Only data necessary for the service is collected: sign-up = email + password; billing = name + postal address, captured only at purchase; transcription = audio processed then results stored, accessible only to the owner.
- Account deletion runs a full erasure pipeline: profile anonymized (name removed, email replaced by a random identifier), authentication credentials and per-user encryption keys destroyed (crypto-shredding), content records reduced to non-personal skeletons and stored objects removed, analytics events deleted, subscription cancelled and the Stripe customer object erased. The pipeline completes under a 30-day SLA with automated monitoring.

1.4 User isolation

- Every user accesses only their own data (isolation by user_id). Transcripts, audio, and billing data are strictly partitioned. There is no public-sharing feature for transcripts.

2. Integrity

- **Transport integrity:** all external traffic over TLS; inter-service traffic between backend and audio processor runs over the providers' private network.
- **Logging & traceability:** sensitive operations are logged via Datadog with structured categories (Auth, Admin, Subscription, and others) and automatic per-request user context (CLS). Log retention: 15 days.
- **Admin audit trail:** every mutating admin operation is recorded in a persistent audit log (actor, action, target user, payload; credentials are never persisted), enforced globally at the framework level rather than per-endpoint, so no admin mutation can bypass it.
- **Change control:** all code changes go through Git version control on GitHub with pull-request review; architectural decisions are recorded as ADRs.

3. Availability & resilience

- **Application redundancy:** redundant application instances with provider-managed load balancing and failover.

- **Database replication:** the production PostgreSQL instance has a near real-time replica for failover.
- **Backups:** automated daily PostgreSQL backups stored in EU object storage, with a defined retention window and integrity verification.
- **Content-store deletion protection:** the encrypted user-content store has safeguards that prevent content from being silently deleted or purged.
- **Source code:** hosted on GitHub with full history.

4. Restoration

- Data can be restored from the daily Scaleway backups (30-day window) or, for immediate failover, from the PostgreSQL replica. Analytics is derived data, reconstructable from the primary PostgreSQL database.

5. Organizational measures

- **Personnel:** 3 founders, no employees/contractors; named accounts; production access is restricted to a single named administrator.
- **Hosting location:** application hosting and object storage in the EU; GPU inference on EU/EEA workers. EU consolidation onto Scaleway is complete for application hosting, object storage and key management.
- **Sub-processors:** governed per the sub-processor annex (Annex 4); engaged under each provider's DPA + SCC where applicable.
- **Secure development:** privacy-by-design (data minimization, user isolation, encryption); dev/prod secret separation; code review; ADRs.
- **Sub-processor data handling:** GPU inference (RunPod) processes encrypted inputs and returns encrypted outputs, runs on EU/EEA workers, and is ephemeral (see Annex 5).
- **Re-identification prohibition:** deliberate re-identification of de-identified deleted-account records is prohibited as written internal policy. Access to the residual records (retained invoices, analytics skeletons) is restricted to a single named administrator, and admin operations are audit-logged. The 15-day log retention additionally bounds the window during which a deleted account's orphaned identifier remains joinable to identity in operational logs.

- **Workstation security:** full-disk encryption (FileVault) and a software firewall are enabled on all founder workstations; founders' home networks use WPA3.

6. Regular review

- The measures above are reviewed against an internal RGPD control set (../rgpd/, structured on the CNIL security guide) with per-item status tracking.

Annex 3: Data Deletion and Return

Annex to the Vook Data Processing Agreement (Art. 28(3)(g) GDPR). Describes how Vook (processor) returns and/or deletes personal data on request and at the end of the contract.

1. Scope

Personal data processed on the controller's behalf: account data, audio files, transcripts, summaries/chat content, and associated metadata. Billing data is handled under separate legal-retention rules (§5).

2. Return / export of data

- **Self-service, one or several transcripts at a time, while the account is active.** End users export their own content in-product in multiple formats: transcripts as PDF, DOCX, SRT, JSON, HTML, and Markdown; chat content as PDF, DOCX, and Markdown; plus the original audio file. JSON gives a machine-readable form suitable for portability (Art. 20).
- **API.** API-key holders export each transcription via GET /api/v1/transcriptions/:id/export (pdf, docx, html, md, srt).
- **Encryption constraint (by design).** Content is per-user encrypted (§7); Vook cannot decrypt it server-side, so export is necessarily performed by the user, under their own key. There is no operator-side extract of plaintext content. This is a deliberate privacy property of the design: not even Vook can read a user's content. The controller's return on termination is therefore satisfied by its users' self-service export rather than by Vook handing over decrypted content.
- **Bulk export (roadmap).** A single-archive "export all my data" download is on the roadmap. Because decryption happens client-side under the user's key, it too must be user-driven. Until it ships, the self-service export above (one or several transcripts at a time) is the available mechanism and already covers the Art. 15 / Art. 20 right.

3. Deletion on account closure (mechanism)

On an account-deletion request (from the app or the admin panel), Vook erases the user's personal data across every store, on one uniform principle: records that feed product analytics are kept but reduced to a non-personal skeleton; everything personal is destroyed or crypto-shredded. Concretely:

1. Cancels the active Stripe subscription and erases the Stripe customer object where lawful.

2. **Scrubs content records to a skeleton.** Transcripts, summaries, chat, and audio metadata keep only non-personal fields (durations, counts, timestamps); names, filenames, transcript text, and chat content are nulled.

3. **Crypto-shreds** the per-item and per-user encryption keys, so any remaining ciphertext (storage, backups) is permanently unreadable (§7).

4. **Removes the stored content objects** (audio, transcripts, diarization, formatted transcripts, chat) from object storage.

5. **Isolates the retained invoice from the analytics data.** The invoice, the only record kept in cleartext (10-year accounting-law retention, §5), is re-keyed to a shared internal "deleted accounts" placeholder record that carries no personal data and appears on no analytics record, while every retained analytics skeleton keeps the original identifier, now an orphan that resolves only to non-personal rows. No stored key links the two, and deliberate re-identification is additionally prohibited by written internal policy (Annex 2).

6. **Anonymizes the account.** Name removed, email replaced by a random identifier; a one-way hash of the address is retained for up to 12 months, in a standalone list linked to no account record, solely to prevent abusive re-registration of a deleted account (legitimate interest, fraud prevention), then deleted. Authentication credentials and key material are destroyed and the billing address removed.

7. **Deletes the user's analytics events (ClickHouse)** (§9) and revokes the session.

Single-item deletion (one transcript/summary/chat) applies the same erasure on demand, at any time, while the account is active.

Automatic deletion of inactive accounts. Accounts inactive for more than two (2) years are deleted automatically, after prior notice to the user and a 30-day response window, in line with Vook's privacy policy. This deletion runs the same erasure pipeline as the voluntary closure described above.

4. Deletion on contract termination

On termination of the controller relationship, Vook deletes all of the controller's end-user personal data **within 30 days** of the request, subject only to the legal-retention exception in §5 and the backup-rotation window in §6. Deletion is confirmed to the controller in writing, and propagates to sub-processors (§8). Encrypted content is rendered permanently unreadable by crypto-erasure (§7).

5. Legal-retention exception

Invoices (containing name + billing address) are retained for **10 years** after account closure, as required by French accounting law (Code de commerce, art. L123-22). They are stored in production PostgreSQL and accessible only via the admin panel (named founder accounts). This is a legal obligation that overrides deletion requests for those specific documents.

6. Residual data in backups

Deleted-account data may persist in the daily PostgreSQL backups for up to the 30-day retention window, then is removed by natural rotation. Backups are not edited per-record (industry standard, to avoid backup corruption); production-side anonymization is immediate, so residual backup data is difficult to exploit. Backup access is restricted to a single named administrator (dedicated Scaleway credentials).

7. Crypto-erasure basis (encrypted content)

User content is stored per-user encrypted (AES-256). The encryption key material lives only in the application database (there is no external copy), so destroying the key columns on deletion is the erasure: the remaining ciphertext becomes permanently unreadable, with immediate effect. This is the GDPR erasure basis where an object cannot be physically deleted at once. On the main Scaleway content bucket (Object Lock, COMPLIANCE mode) a deleted object is additionally purged physically by the storage lifecycle within 90 days; on the remaining stores (durable audio, legacy store) erasure rests on the crypto-shredding alone: residual objects persist only as permanently unreadable ciphertext until each store's lifecycle expires them or the store is retired. The same basis covers the 30-day backup residue (§6).

8. Sub-processor deletion

Subscription cancellation propagates to Stripe at deletion time, and the Stripe customer object is erased where lawful. Email delivery (SendGrid) is used as a pure SMTP relay: no contact list or per-user record is stored at SendGrid, so there is nothing to remove there; exclusion of deleted accounts from any mailing is enforced in Vook's own database. Residual records at other sub-processors are covered by each sub-processor's DPA (see Annex 4).

9. Analytics-event retention

Behavioral analytics events (which carry identifiers such as filenames, never content) are retained for a maximum of **13 months**, enforced natively by a table-level TTL in the analytics store rather than by procedure. After that they survive only as anonymous aggregates (counts with no identifiers), which carry no personal data and are kept indefinitely. On an account deletion all of the user's analytics events are deleted outright from the analytics store; only pre-signup events linked to no account remain. Erasure therefore reaches the analytics store as well as the primary store.

Annex 4: Sub-processor List

Annex to the Vook Data Processing Agreement (Art. 28 GDPR). Vook acts as processor; the Customer is the controller. The current list of authorized sub-processors, including for each: name, role, personal data processed, entity, processing location, and transfer basis, is published and continuously maintained at https://vook.ai/en/sub-processors. That page forms an integral part of this Annex 4 and is updated in accordance with Article 4 of this DPA. Prior versions of this DPA and of the sub-processor list are archived under the same URL scheme (vook-dpa-en-vYYYY-MM.pdf) so that the Customer can identify the version in force at any given date.

Annex 5: Transfer Impact Assessment (TIA)

Informational annex to the Vook Data Processing Agreement. Documents Vook's assessment of third-country laws and supplementary measures for each transfer of personal data outside the EU/EEA (Schrems II / EDPB Recommendations 01/2020; SCC Clause 14). Provided for transparency and to assist the Controller's own assessment. This annex is an assessment and not a warranty: it reflects the situation at the date below and is updated together with the sub-processor list (Annex 4), under the same notification mechanism (DPA Article 4).

1. Method

Per the EDPB's six-step roadmap: (1) transfers are mapped in Annex 4; (2) the transfer tool is identified per vendor: SCC Module 3, the EU-US Data Privacy Framework (DPF) where the importer is certified, or BCRs (PayPal); (3) destination-country law is assessed below (§2); (4) supplementary measures are identified (§3); (5) contractual formalities are documented in Vook's DPA register; (6) the assessment is re-evaluated at every sub-processor change.

2. Destination-country law assessed (United States)

All non-EU/EEA importers in Annex 4 are US-incorporated. The relevant US legal framework:

- **FISA Section 702**: permits targeted acquisition of non-US persons' communications from US "electronic communications service providers".
- **CLOUD Act**: US-incorporated companies can be compelled to produce data in their possession, custody, or control regardless of where it is stored (this is why EU-located infrastructure of a US company does not, alone, remove exposure).
- **EU-US Data Privacy Framework (2023 adequacy decision)**: introduces binding safeguards (proportionality limits on signals intelligence, the Data Protection Review Court); where an importer is DPF-certified, the adequacy decision itself provides a lawful transfer basis, with SCCs retained as fallback.

3. Supplementary measures (the load-bearing controls)

- **Per-user AES-256 encryption of content at rest**: Vook encrypts audio, transcripts, summaries, and chat before storage, under per-user keys Vook cannot use to decrypt server-side (except for users who explicitly opted into the recovery-key option, whose key is retained wrapped via Scaleway Key Manager). A compelled disclosure of stored content from any storage or infrastructure provider yields ciphertext; transcription titles and file names, stored as cleartext metadata, are the exception.
- **TLS 1.2+ in transit** on all flows.
- **EU processing residency for primary storage (Scaleway, Paris), GPU inference (EU/EEA workers), and observability data at rest (Datadog EU1).**
- **Ephemeral GPU processing**: no content retained after a job; output encrypted before return.
- **Data minimization per vendor**: each vendor receives only the categories listed in Annex 4; content never reaches the payment, email, frontend-hosting, OAuth, or alerting providers.
- **Consent gating**: the only vendor that receives plaintext content (Google Gemini) receives it solely on the user's explicit, consented action.

4. Per-vendor assessment

RunPod, Inc. (EU/EEA workers)

- Data transferred: Content: ciphertext at rest, input and output; plaintext in GPU memory during inference only
- Tool: SCC (M3, published DPA)
- What a compelled US disclosure could yield: Stored data: ciphertext. In-memory capture would require forward-looking interception of a specific live job, a materially higher bar. The model cannot run on ciphertext, so this window is inherent to how Vook runs inference today; confidential-computing hardware (NVIDIA CC mode) addresses it and is tracked, not deployed
- Residual risk: Low to moderate, disclosed

Google LLC (Gemini, global endpoint)

- Data transferred: Transcript text in-prompt, only on explicit consented user action; paid tier, no training
- Tool: SCC (M3)
- What a compelled US disclosure could yield: Prompt/response data held per Google's paid-tier terms
- Residual risk: Moderate, opt-in and disclosed; EU-endpoint option available (paid)

Stripe (US LLC leg)

- Data transferred: Payment/billing data (no content)
- Tool: DPF + SCC
- What a compelled US disclosure could yield: Payment records: data Stripe holds anyway as PCI processor
- Residual risk: Low

PayPal (US parent)

- Data transferred: Payment data (no content); independent controller
- Tool: BCRs

- What a compelled US disclosure could yield: Payment records under PayPal's own controllership
- Residual risk: Low

Twilio SendGrid (US processing)

- Data transferred: Email address + email content (no transcripts)
- Tool: SCC (M3)
- What a compelled US disclosure could yield: Email traffic only
- Residual risk: Low

Vercel, Inc. (EU+NA functions)

- Data transferred: Account/session/request metadata; content never reaches Vercel (client-side handling)
- Tool: DPF + SCC
- What a compelled US disclosure could yield: Metadata only
- Residual risk: Low

Datadog, Inc. (EU1, data at rest in Germany)

- Data transferred: Technical logs, request metadata; 15-day retention
- Tool: SCC (M3)
- What a compelled US disclosure could yield: Short-lived logs; follow-the-sun support may access EU-stored data from outside the EU
- Residual risk: Low

Google / Microsoft (OAuth)

- Data transferred: Account identifiers, email, OAuth token
- Tool: SCC (M3)
- What a compelled US disclosure could yield: Sign-in identifiers the providers hold as consumer identity providers anyway
- Residual risk: Low

Slack (Salesforce, US)

- Data transferred: Internal alert payloads; incidental personal data
- Tool: SCC (M3)
- What a compelled US disclosure could yield: Incidental metadata
- Residual risk: Low

5. Conclusion

For the core transcription service, personal-data content is per-user encrypted and EU-resident: the realistic compelled-disclosure scenarios against US-incorporated providers yield ciphertext or peripheral metadata, not readable content. The two documented exceptions are transient plaintext in GPU memory during inference (inherent to how Vook runs inference today, EU/EEA-located, ephemeral) and the opt-in AI feature (explicit consented user action, paid-tier no-training terms, with a paid EU-endpoint option). Vook therefore assesses the supplementary measures as effective for the data and transfers at stake, while, consistently with DPA Article 6, not warranting a blanket exclusion of processing outside the EU/EEA.

6. Review

Re-assessed at every addition/replacement of a sub-processor (DPA Article 4), on material changes in US surveillance law or CJEU/EDPB guidance, and at least annually.