WhisperAI Data Processing Agreement

WhisperAI Technology Inc.

Version 2 — Effective April 30, 2026 — Draft for internal review

Contents

1 Data Processing Agreement

WhisperAI Data Processing Agreement Version: v2 **Effective Date:** April 30, 2026

> **Draft status (internal):** This document is a draft prepared for internal review. It is not published on whisperai.com.

1.1 1. Definitions

For the purposes of this Data Processing Agreement ("**DPA**"):

- **"Agreement"** means the WhisperAI Terms of Service or other written agreement between Customer and Provider under which Provider makes the Services available to Customer.
- **"Applicable Data Protection Laws"** means all data protection and privacy laws applicable to a Party's Processing of Personal Data under the Agreement, including, where applicable: (a) the EU General Data Protection Regulation 2016/679 ("**EU GDPR**"); (b) the UK Data Protection Act 2018 and the UK GDPR ("**UK GDPR**"); (c) the Swiss Federal Act on Data Protection ("**FADP**"); (d) the California Consumer Privacy Act, as amended by the California Privacy Rights Act ("**CCPA/CPRA**"); and (e) any other US state privacy laws applicable to the Processing.
- **"Controller"**, **"Processor"**, **"Data Subject"**, **"Personal Data"**, **"Processing"** (and cognate verbs), **"Supervisory Authority"**, **"Sub-processor"**, and **"Special Categories of Personal Data"** have the meanings given in the EU GDPR (or, where the UK GDPR or CCPA/CPRA applies, the equivalent terms in those laws).
- **"Customer"** means the legal entity that has entered into the Agreement with Provider.
- **"Customer Personal Data"** means Personal Data Processed by Provider on behalf of Customer under the Agreement, as described in Annex 1.
- **"EEA"** means the European Economic Area.
- **"Provider"** means **WhisperAI Technology Inc.**, a corporation with its mailing address at PO Box 572551, Tarzana, CA 91357, United States.
- **"Restricted Transfer"** means a transfer of Personal Data from the EEA, the United Kingdom, or Switzerland to a jurisdiction that has not been recognized by the relevant authority as providing an adequate level of protection.
- **"Security Incident"** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data Processed by Provider or a Sub-processor.
- **"Services"** means the WhisperAI hosted transcription, translation, and related services described in the Agreement.
- **"Standard Contractual Clauses"** or **"SCCs"** means the standard contractual clauses approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, as set out at Annex 4.
- **"UK Addendum"** means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner's Office and laid before Parliament on 2 February 2022, as it may be amended.

1.2 2. Scope and Roles of the Parties

2.1 **Scope.** This DPA applies to the Processing of Customer Personal Data by Provider in the course of providing the Services. It forms part of, and is subject to, the Agreement.

2.2 **Roles.** With respect to Customer Personal Data: (a) Customer is the **Controller** (or, where Customer is itself a Processor acting on behalf of a third-party controller, the Processor on behalf of that controller); and (b) Provider is the **Processor** (or, in the second case in (a) above, a Sub-processor).

2.3 **CCPA/CPRA roles.** With respect to Personal Information governed by the CCPA/CPRA, Customer is a "Business" and Provider is a "Service Provider," and Section 14 of this DPA applies.

2.4 **Compliance.** Each Party will comply with its respective obligations under Applicable Data Protection Laws in connection with the Processing of Customer Personal Data.

1.3 3. Details of Processing

The subject matter, nature, purpose, duration of Processing, categories of Data Subjects, and types of Personal Data Processed are set out in **Annex 1 (Processing Details)**.

1.4 4. Controller Instructions

4.1 **Documented instructions.** Provider will Process Customer Personal Data only on the documented instructions of Customer, including the instructions set out in the Agreement and this DPA, and as necessary to provide and support the Services. Customer's use of the Services through configuration settings (including organization, sharing, and workspace settings) constitutes instructions to Provider.

4.2 **Legal requirements.** Provider may Process Customer Personal Data to comply with a legal obligation to which Provider is subject. Where permitted by law, Provider will inform Customer of the legal requirement before Processing.

4.3 **Unlawful instructions.** Provider will inform Customer if, in its opinion, an instruction from Customer infringes Applicable Data Protection Laws. Provider may, in such case, suspend performance of the relevant instruction until Customer confirms, amends, or withdraws it.

4.4 **Customer Responsibilities.** Customer is responsible for determining the lawfulness of its instructions to Provider, providing all notices, and obtaining all consents, permissions, or other lawful bases required for the collection, recording, upload, disclosure, and Processing of Customer Personal Data through the Services, and for ensuring that Customer Personal Data may be lawfully Processed by Provider and its Sub-processors. Customer is solely responsible for the accuracy, quality, legality, and appropriateness of the Customer Personal Data it submits to the Services and for the means by which Customer acquired it.

4.5 **Recording and audio content.** Where Customer uploads, records, or otherwise Processes audio, video, meeting, call, or voice content through the Services, Customer is responsible for complying with all applicable recording, wiretapping, consent, employment, biometric, and communications laws, including obtaining any one-party or all-party consent required in the jurisdictions of the relevant participants.

4.6 **HIPAA / Protected Health Information.** Unless Provider has separately entered into a Business Associate Agreement with Customer, Customer must not use the Services to create, receive, maintain, transmit, or otherwise Process Protected Health Information subject to HIPAA.

1.5 5. Processor Confidentiality Obligations

5.1 Provider will ensure that personnel authorized to Process Customer Personal Data are bound by written or statutory obligations of confidentiality, and are informed of the confidential nature of the Customer Personal Data.

5.2 Provider will limit access to Customer Personal Data to personnel who require such access to perform the Services or to comply with Provider's obligations under the Agreement.

5.3 **Human access limitation.** Provider personnel will not access Customer content — including audio recordings, transcripts, translations, summaries, speaker labels, or exports — except as necessary to provide support requested by Customer, to investigate abuse, fraud, security, or operational issues, to comply with law, to maintain or improve the reliability and security of the Services, or as otherwise

expressly permitted by this DPA. Any such access will be subject to access controls, least-privilege principles, and the confidentiality obligations of this Section 5, and will not be used to train, fine-tune, or improve general-purpose AI or ML models or for broad review of customer content.

1.6 6. Security Measures

6.1 **Technical and organizational measures.** Taking into account the state of the art, the costs of implementation, and the nature, scope, context, and purposes of Processing, as well as the risk to Data Subjects, Provider will implement and maintain appropriate technical and organizational measures designed to ensure a level of security appropriate to the risk, as described in **Annex 2 (Technical and Organizational Measures)**.

6.2 **Changes.** Provider may update the measures from time to time, provided that the updates do not materially diminish the overall level of protection.

1.7 7. Security Incident Notification

7.1 **Notice.** Provider will notify Customer without undue delay, and in any event within **seventy-two (72) hours** after becoming aware of a Security Incident affecting Customer Personal Data.

7.2 **Content of notice.** The notice will, to the extent then known and reasonably available to Provider, include: (a) a description of the nature of the Security Incident, including the categories and approximate number of Data Subjects and records concerned; (b) the likely consequences of the Security Incident; (c) the measures taken or proposed to address the Security Incident, including measures to mitigate its possible adverse effects; and (d) contact details for further information.

7.3 **Updates.** Where it is not possible to provide all of the information at the same time, Provider may provide it in phases without undue further delay.

7.4 **Customer obligations.** Customer is responsible for any notifications it is required to make to Supervisory Authorities and Data Subjects under Applicable Data Protection Laws.

7.5 **Method of notice.** Notices under this Section 7 will be sent to the security or administrative contact designated by Customer in its account, or, failing that, to the account owner's email address.

1.8 8. Sub-processors

8.1 **General authorization.** Customer grants Provider general written authorization to engage Sub-processors to Process Customer Personal Data, subject to the requirements of this Section 8.

8.2 **Current Sub-processors.** A list of Sub-processors engaged by Provider as of the Effective Date is set out at **Annex 3 (Sub-processors)**.

8.3 **Sub-processor obligations.** Provider will enter into a written agreement with each Sub-processor that imposes data protection obligations no less protective than those in this DPA, to the extent applicable to the nature of the services provided by the Sub-processor.

8.4 **New Sub-processors and right to object.** Provider will maintain an up-to-date list of Sub-processors either in Annex 3, on Provider's website, or at another location made available to Customer. Provider will provide at least **thirty (30) days'** prior notice of any new Sub-processor by email, in-app

notice, update to the Sub-processor list, or other reasonable electronic notice. Customer may object in writing to the engagement of a new Sub-processor on reasonable data-protection grounds within that 30-day period. If Provider is unable to make a commercially reasonable accommodation, Customer may, as its sole and exclusive remedy, terminate the affected portion of the Services without penalty by giving written notice to Provider within thirty (30) days of Provider's response.

8.5 **Liability for Sub-processors.** Provider remains liable to Customer for the performance of each Sub-processor's obligations under this DPA.

1.9 9. Data Subject Request Assistance

9.1 Taking into account the nature of the Processing, Provider will assist Customer by appropriate technical and organizational measures, insofar as possible, to fulfill Customer's obligation to respond to requests from Data Subjects exercising their rights under Applicable Data Protection Laws (including rights of access, rectification, restriction, erasure, portability, and objection).

9.2 If a Data Subject submits a request directly to Provider, Provider will, without responding to the request itself (other than to direct the Data Subject to Customer), promptly forward the request to Customer where Customer is reasonably identifiable.

9.3 The Services include self-service functionality (export, deletion, and account-level data download) that Customer may use to respond to Data Subject requests without further assistance from Provider. Provider will provide additional assistance to the extent the self-service functionality is insufficient.

1.10 10. Compliance Assistance, DPIAs, and Regulator Cooperation

10.1 Provider will provide Customer with reasonable assistance, at Customer's cost, in: (a) carrying out data protection impact assessments under Article 35 of the EU GDPR or equivalent provisions of other Applicable Data Protection Laws; and (b) consultations with Supervisory Authorities under Article 36 of the EU GDPR or equivalent provisions.

10.2 Provider will, on request, make available to Customer information reasonably necessary to demonstrate compliance with this DPA, in accordance with Section 13 (Audit and Records).

1.11 11. International Transfers

11.1 **Transfers.** Customer acknowledges that Provider and its Sub-processors may Process Customer Personal Data in jurisdictions outside the country in which Customer is located, including the United States.

11.2 **Restricted Transfers from the EEA.** Where Provider's Processing of Customer Personal Data involves a Restricted Transfer from the EEA, the Parties agree that the SCCs at Annex 4 are incorporated into this DPA and apply as follows: (a) **Module Two (Controller to Processor)** applies where Customer is a Controller; (b) **Module Three (Processor to Sub-processor)** applies where Customer is itself a Processor on behalf of a third-party controller; (c) Clause 7 (Docking) is included; (d) Clause 9(a) Option 2 (general written authorization for Sub-processors) applies, with the notice period in Section 8.4 of this DPA; (e) Clause 11(a) (independent dispute resolution) is **not** included; (f) Clause 17 (Governing law): the SCCs are governed by the law of **Ireland**; (g) Clause 18 (Forum and

jurisdiction): disputes will be resolved before the courts of **Ireland**; (h) Annexes I, II, and III of the SCCs are populated by Annexes 1, 2, and 3 of this DPA respectively.

11.3 **Restricted Transfers from the United Kingdom.** Where the Processing involves a Restricted Transfer subject to the UK GDPR, the UK Addendum is incorporated and completed using the information in this DPA and its Annexes.

11.4 **Restricted Transfers from Switzerland.** Where the Processing involves a Restricted Transfer subject to the FADP, the SCCs apply with the following modifications: (a) references to the EU GDPR are understood to include the FADP; (b) the Swiss Federal Data Protection and Information Commissioner is the competent Supervisory Authority; and (c) the term "Member State" does not prevent Data Subjects in Switzerland from exercising rights in their place of habitual residence.

11.5 **Conflict.** In the event of any conflict between this DPA and the SCCs or UK Addendum with respect to Restricted Transfers, the SCCs or UK Addendum (as applicable) prevail.

11.6 **Government access requests.** Provider will, where legally permitted, promptly notify Customer of any legally binding request by a public authority, law enforcement agency, or government authority for access to Customer Personal Data. Provider will review such requests and, where Provider reasonably believes a request is unlawful, overbroad, or inconsistent with applicable transfer safeguards, Provider will seek to limit, object to, or challenge the request as appropriate.

11.7 **Transfer impact assessments.** Upon reasonable request, Provider will make available information reasonably necessary for Customer to conduct and document transfer impact assessments relating to Restricted Transfers under this DPA, subject to confidentiality, security, and commercial-sensitivity limitations.

1.12 12. Return and Deletion of Data

12.1 **During the term.** Customer may, at any time during the term of the Agreement, export Customer Personal Data through the self-service functionality of the Services.

12.2 **On termination.** Following termination or expiration of the Agreement, Provider will retain Customer Personal Data for up to ninety (90) days to permit Customer to export Customer Personal Data or reactivate its account, unless Customer requests earlier deletion or Applicable Data Protection Laws require continued retention. After that period, Provider will delete Customer Personal Data from active production systems, subject to Section 12.3 (backups), legal obligations, fraud-prevention records, billing and tax records, audit logs, and aggregated or de-identified data from which the relevant Data Subjects cannot reasonably be re-identified. Upon Customer's earlier written deletion or return instruction, Provider will delete or return the Customer Personal Data within thirty (30) days, subject to the same exceptions.

12.3 **Backups.** Customer Personal Data residing in routine backups will be deleted in accordance with Provider's standard backup retention cycle and will not be restored to active production systems except as necessary for disaster recovery, security, or legal compliance.

12.4 **Account deletion by Data Subject or Customer.** Where Customer or a Data Subject deletes Personal Data through the self-service functionality, Provider will delete the corresponding records from active production systems on the schedule documented in Provider's Privacy Policy.

1.13 13. Audit and Records

13.1 **Records.** Provider will maintain records of its Processing activities as required by Article 30(2) of the EU GDPR and equivalent provisions of other Applicable Data Protection Laws.

13.2 **Audit information.** On Customer's written request, no more than **once per twelve (12) month period** (except where required more frequently by Applicable Data Protection Laws or a Supervisory Authority), Provider will make available to Customer: (a) a current copy of Provider's security documentation, including a description of the technical and organizational measures in Annex 2; (b) responses to Customer's reasonable written security questionnaires; and (c) any third-party audit reports or certifications Provider maintains, if any, subject to the confidentiality obligations of the Agreement.

13.3 **On-site audits.** If the information made available under Section 13.2 is not sufficient to demonstrate compliance with this DPA, Customer may request an on-site audit, subject to the following conditions: (a) the audit is conducted during normal business hours, with reasonable advance notice (not less than thirty (30) days, except in the case of a documented Security Incident or a binding order of a Supervisory Authority); (b) the audit does not unreasonably interfere with Provider's business activities or compromise the confidentiality of other customers' data; (c) the auditor is bound by written obligations of confidentiality at least as protective as those in the Agreement and is not a competitor of Provider; (d) Customer bears the costs of the audit, except where the audit identifies a material non-compliance by Provider, in which case Provider bears its own internal costs; and (e) Customer shares any audit findings with Provider on a confidential basis.

13.4 **Regulator audits.** Nothing in this Section 13 restricts the rights of a Supervisory Authority to conduct an audit under Applicable Data Protection Laws.

1.14 14. CCPA/CPRA Service Provider Terms

14.1 **Service Provider role.** With respect to Personal Information governed by the CCPA/CPRA, Provider is a "Service Provider" Processing Personal Information on behalf of Customer (a "Business") for the limited and specified Business Purposes described in Annex 1 (the "**Permitted Purposes**").

14.2 **Restrictions.** Provider will not: (a) Sell or Share (as defined in the CCPA/CPRA) Personal Information; (b) retain, use, or disclose Personal Information for any purpose other than the Permitted Purposes, including for any "commercial purpose" other than the Permitted Purposes or as otherwise permitted by the CCPA/CPRA; (c) retain, use, or disclose Personal Information outside the direct business relationship between Provider and Customer; or (d) combine the Personal Information that Provider receives from or on behalf of Customer with Personal Information that Provider receives from or on behalf of any other person or collects from its own interaction with the Data Subject, except as permitted by the CCPA/CPRA.

14.3 **Equivalent level of protection.** Provider will provide the same level of privacy protection with respect to Personal Information as required of Businesses under the CCPA/CPRA and applicable regulations.

14.4 **Customer oversight.** Customer may take reasonable and appropriate steps to help ensure that Provider uses Personal Information in a manner consistent with Customer's obligations under the CCPA/CPRA, including by requesting information under Section 13 (Audit and Records).

14.5 **Certification.** Provider certifies that it understands the restrictions in this Section 14 and will comply with them.

14.6 **Notice of inability to comply.** Provider will notify Customer if it determines it can no longer meet its obligations under the CCPA/CPRA. On such notice, Customer may take reasonable and appropriate steps to stop and remediate unauthorized use of Personal Information.

14.7 **Sub-processor flow-down.** Provider will impose obligations consistent with this Section 14 on any Sub-processor that Processes Personal Information governed by the CCPA/CPRA.

1.15 15. AI and Model-Training Restrictions

15.1 **No training on Customer content.** Provider will not, and will contractually require its AI Sub-processors not to, use Customer Personal Data — including audio recordings, transcripts, translations, summaries, and any derivative content generated from them — to train, fine-tune, or otherwise improve any general-purpose machine-learning or generative-AI model.

15.2 **Permitted model use.** Provider may use Customer Personal Data: (a) to provide the Services to Customer (including by submitting it to AI Sub-processors for the specific Processing requested, such as transcription, translation, summarization, or speaker diarization); (b) to diagnose and resolve operational issues affecting the Services, on an as-needed basis and subject to the confidentiality and security obligations of this DPA; and (c) to generate aggregated and de-identified statistics that do not identify Customer or any Data Subject, and from which re-identification is not reasonably possible.

15.3 **Sub-processor commitments.** Provider relies on contractual commitments made by its AI Sub-processors, through their applicable API, business, or enterprise terms, that content submitted via API will not be used to train their general-purpose models. Customer acknowledges that the specific commitments vary by Sub-processor and are governed by each Sub-processor's own data processing terms, which are referenced in Annex 3.

1.16 16. Liability and Indemnity

16.1 Each Party's liability arising out of or related to this DPA, whether in contract, tort, or under any other theory of liability, is subject to the exclusions and limitations of liability set out in the Agreement.

16.2 For the avoidance of doubt, the SCCs, where applicable, create direct rights for Data Subjects that are not subject to such limitations.

1.17 17. Order of Precedence

In the event of any conflict or inconsistency between the documents governing the Processing of Customer Personal Data, the following order of precedence applies:

1. the SCCs and UK Addendum (with respect to Restricted Transfers governed by them);
2. this DPA;
3. the Agreement.

To the extent Provider's Privacy Policy describes Processing of Customer Personal Data covered by this DPA, this DPA controls in the event of conflict.

This DPA replaces any prior data processing addendum or similar instrument between the Parties with respect to the subject matter described herein.

1.18 Annex 1 — Processing Details

1.18.1 A. List of Parties

Data Exporter (Controller): Customer, as identified in the Agreement.

Data Importer (Processor): WhisperAI Technology Inc., PO Box 572551, Tarzana, CA 91357, United States. Contact: support@whisperai.com.

1.18.2 B. Description of Processing

Item	Detail
Subject matter	Provision of cloud-based audio transcription, translation, summarization, speaker diarization, and related collaboration features (the Services).
Duration	For the term of the Agreement, plus the retention periods described in Section 12 of this DPA.
Nature and purpose	Receiving audio recordings and related content uploaded or recorded by Customer or its end users; converting, storing, transcribing, translating, summarizing, and diarizing such content; making the resulting transcripts, translations, summaries, and exports available to Customer; and providing organization, sharing, billing, support, and security functions in connection with the Services.
Categories of Data Subjects	(a) Customer's authorized users (administrators, end users, organization members); (b) individuals whose voices, names, or other personal data appear in audio recordings, transcripts, or related content uploaded or recorded via the Services; (c) recipients of shared transcripts or exports designated by Customer.
Categories of Personal Data	(a) Account identifiers: email address, name, hashed password, profile preferences, authentication tokens, organization membership and role; (b) Billing data: subscription tier, billing frequency, billing-cycle metadata; payment-card details are collected and processed directly by Stripe and are not stored by Provider; (c) Content data: audio recordings; derived transcripts, translations, summaries, and speaker labels; metadata such as duration, language, file name, and timestamps; user-supplied prompts and edits; (d) Collaboration data: folder and tag organization, sharing relationships, organization audit log entries; (e) Usage and operational data: API and request logs, diagnostic identifiers for uploads and transcriptions, error logs, monthly minutes and dictation seconds counters.

Item	Detail
Special Categories of Personal Data	The Services are not designed for, and Customer should not use the Services to Process, Special Categories of Personal Data except where Customer has determined it has a lawful basis to do so. To the extent Customer chooses to upload content that contains Special Categories (for example, audio of medical, legal, or other sensitive consultations), such Processing is performed at Customer's instruction and risk. Unless Provider has separately entered into a Business Associate Agreement with Customer, Customer must not use the Services to create, receive, maintain, transmit, or otherwise Process Protected Health Information subject to HIPAA (see Section 4.6).
Frequency of transfer	Continuous, on an as-needed basis driven by Customer's use of the Services.
Retention	As set out in Section 12 of this DPA and in Provider's Privacy Policy.
Permitted Business Purposes (CCPA/CPRA)	Providing, securing, maintaining, debugging, supporting, billing, fraud prevention, abuse prevention, account administration, and improving the Services solely for Customer and only as permitted by Applicable Data Protection Laws and this DPA. The Permitted Business Purposes do not include broad product improvement, advertising, profiling, Selling or Sharing Personal Information, unrelated analytics, or training of general-purpose AI or ML models.

1.18.3 C. Competent Supervisory Authority (for SCC purposes)

Where the EU GDPR applies, the competent Supervisory Authority is determined in accordance with Clause 13 of the SCCs. For SCC governing-law and forum purposes (Sections 11.2(f) and 11.2(g) of this DPA), Ireland is selected.

1.19 Annex 2 — Technical and Organizational Measures

Provider implements the following technical and organizational measures. References to specific technologies reflect Provider's current implementation and may be replaced with measures providing an equivalent or higher level of protection.

1.19.1 A. Pseudonymization and Encryption

- **In transit:** All connections between Customer's browsers/clients and the Services, and between the Services and external Sub-processor APIs, are protected using TLS 1.2 or higher.
- **At rest:** Customer Personal Data is stored in managed services (Neon Postgres and Google Cloud Storage) that provide encryption at rest by default using industry-standard symmetric encryption.

1.19.2 B. Confidentiality, Integrity, Availability, and Resilience of Processing Systems

- **Access control:** Authentication to the Services is via email-and-password (with bcrypt-hashed credentials) or Google OAuth 2.0. Session state is stored server-side in the application database with session tokens transmitted via secure, HTTP-only cookies.
- **Authorization:** Role-based access within the Services (free, basic, premium, pro, enterprise tiers; organization member, admin, owner roles) is enforced server-side.
- **Network:** The Services are served exclusively over HTTPS; HTTP traffic to the canonical production domain is redirected to HTTPS.
- **Multi-tenancy isolation:** Personal Data is segregated by user and organization identifiers in the application database and storage layer, and queries are scoped to the authenticated principal.
- **Background processing:** Long-running jobs (transcription, summary generation) use durable queues with leader-election to prevent concurrent corruption.

1.19.3 C. Resilience and Recovery

- **Database backups:** The managed Postgres provider performs automated backups and point-in-time recovery as part of its managed service.
- **Object storage durability:** Audio and derived files are stored in a managed object storage service with provider-managed redundancy.

1.19.4 D. Logging and Monitoring

- **Operational logging:** Provider maintains application and infrastructure logs covering authentication events, API calls, upload diagnostics (per-request correlation IDs), and error events.
- **Error alerting:** Critical error events trigger internal notifications to Provider's operations contact.

1.19.5 E. Personnel and Access Management

- **Confidentiality:** Personnel with access to Customer Personal Data are bound by written confidentiality obligations.
- **Least privilege:** Production-system access is limited to personnel with a need to know.
- **Multi-factor authentication:** Multi-factor authentication is required for production administrative access to systems that Provider directly controls and that support it (including cloud-provider consoles, the production code repository, and managed-service dashboards).
- **Secret management:** Production secrets and credentials are stored in environment variables or a managed secret system and are not committed to source control.
- **Access lifecycle:** Production access is removed when personnel no longer require it.
- **Patching:** Security patches and dependency updates are applied within a commercially reasonable timeframe based on severity and exploitability.
- **Audit logging:** Administrative access to managed services is logged where the underlying platform supports such logging.

1.19.6 F. Sub-processor Management

- Sub-processors are bound by data protection terms consistent with Section 8 of this DPA and are listed in Annex 3.

1.19.7 G. Security Incident Response

- Provider maintains an internal security-incident response process that includes investigation, containment, customer notification within seventy-two (72) hours of awareness, and post-incident review.

1.19.8 H. Items Intentionally Not Claimed

The following are **not** claimed by Provider as of the Effective Date and will be added only if and when validly attained:

- SOC 2 Type I or Type II attestation.
- ISO/IEC 27001 certification.
- HIPAA Business Associate Agreement availability.
- Periodic third-party penetration testing on a defined cadence.
- Customer-managed encryption keys (BYOK / HYOK).

1.20 Annex 3 — Sub-processors

As of the Effective Date, Provider engages the following Sub-processors to Process Customer Personal Data in connection with the Services:

Sub-processor	Service Provided	Categories of Personal Data Processed	Processing Location	Website
AssemblyAI, Inc.	AI-based audio transcription and speaker diarization.	Audio recordings, derived transcripts, speaker labels, language identifiers.	United States	assemblyai.com
OpenAI, L.L.C.	AI-based summarization and translation of transcript text; HTML cleanup for export rendering.	Transcript text, user-supplied prompts and edits.	United States	openai.com
PyannoteAI	AI-based speaker diarization (used where engaged).	Audio recordings, derived speaker segmentation.	United States	pyannote.ai
Stripe, Inc.	Payment processing, subscription billing, invoicing. Certain payment processing activities may be governed by Stripe's own terms, privacy notices, and data processing terms; Provider does not store full payment-card numbers.	Billing contact details, subscription metadata; payment-card data is collected and stored directly by Stripe.	United States	stripe.com
Twilio Inc. (SendGrid)	Transactional and notification email delivery (account, billing, sharing, security incident notices, transcript-related emails).	Email address, name, email body content (which may include transcript excerpts where Customer enables email delivery).	United States	sendgrid.com
Neon, Inc.	Managed PostgreSQL database hosting application and Customer Personal Data.	All categories of Customer Personal Data described in Annex 1 except raw audio files.	United States	neon.tech

Sub-processor	Service Provided	Categories of Personal Data Processed	Processing Location	Website
Google LLC (Google Cloud Storage)	Object storage for raw audio files, converted audio, and chunked-upload parts.	Audio recordings and derived audio.	United States	cloud.google.com/storag
Google LLC (Cloud Run)	Application hosting, request routing, and TLS termination.	Transient request data including all categories described in Annex 1 in the course of request handling.	United States	cloud.google.com/run

Optional integrations. Optional integrations are engaged only when enabled by Customer or an authorized user. Depending on the integration and user configuration, these providers may act as independent controllers, processors, service providers, or third-party providers under their own terms. They are disclosed here for transparency:

Integration	Service Provided	Data Involved	Website
Google LLC (Google Drive)	Import of user-selected audio files into the Services.	Only the file(s) the user explicitly selects.	google.com/drive

Updates. This Annex 3 will be maintained and updated by Provider in accordance with Section 8.4 of this DPA. The current version is available on request from support@whisperai.com.

1.21 Annex 4 — Standard Contractual Clauses and UK Addendum

1.21.1 A. EU Standard Contractual Clauses

The Standard Contractual Clauses approved by Commission Implementing Decision (EU) 2021/914 of 4 June 2021 are incorporated into this DPA by reference, with the following selections (as set out in Section 11.2 of this DPA):

- **Modules:** Module Two (Controller-to-Processor) applies where Customer is a Controller. Module Three (Processor-to-Sub-processor) applies where Customer is itself a Processor on behalf of a third-party controller.
- **Clause 7 (Docking clause):** Included.
- **Clause 9 (Use of sub-processors):** Option 2 — General written authorization, with thirty (30) days' prior notice of changes.
- **Clause 11 (Redress):** The optional independent-dispute-resolution language is not included.
- **Clause 17 (Governing law):** Irish law.
- **Clause 18 (Choice of forum and jurisdiction):** The courts of Ireland.
- **Annex I.A (List of Parties):** Annex 1, Section A of this DPA.
- **Annex I.B (Description of transfer):** Annex 1, Section B of this DPA.
- **Annex I.C (Competent Supervisory Authority):** Annex 1, Section C of this DPA.
- **Annex II (Technical and Organizational Measures):** Annex 2 of this DPA.
- **Annex III (List of Sub-processors):** Annex 3 of this DPA.

The current authoritative text of the SCCs is available at: https://eur-lex.europa.eu/eli/dec_impl/2021/914.

1.21.2 B. UK International Data Transfer Addendum

The UK International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (Version B1.0, issued by the UK Information Commissioner's Office and laid before Parliament on 2 February 2022) is incorporated into this DPA by reference for Restricted Transfers subject to the UK GDPR, and completed as follows:

- **Table 1 (Parties):** As set out in Annex 1, Section A.
- **Table 2 (Selected SCCs, Modules and Selected Clauses):** As set out in Section A above.
- **Table 3 (Appendix Information):** As set out in Annexes 1, 2, and 3 of this DPA.
- **Table 4 (Ending the Addendum when the Approved Addendum Changes):** Neither Party may end the Addendum under Section 19 of the Addendum.

The current authoritative text of the UK Addendum is available from the UK Information Commissioner's Office.

1.21.3 C. Swiss FADP

For Restricted Transfers subject to the Swiss FADP, the SCCs apply with the modifications set out in Section 11.4 of this DPA.

End of Data Processing Agreement v2 — April 30, 2026.