WhisperAI Data Processing Agreement

Version 3. Effective October 26, 2026. Replaces Version 2.

This Data Processing Agreement ("DPA") forms part of the WhisperAI Terms of Service or other written agreement (the "Agreement") between WhisperAI Technology Inc., a Delaware corporation ("Provider"), and the customer that accepts the Agreement ("Customer"). It applies automatically when Customer accepts the Agreement.

1. Definitions

"Applicable Data Protection Laws" means all data protection and privacy laws that apply to a party's Processing of Personal Data under the Agreement. Where applicable, they include:

- (a) the EU General Data Protection Regulation 2016/679 ("EU GDPR")
- (b) the UK GDPR and Data Protection Act 2018 ("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")
- (e) other US state privacy laws
- (f) for PHI, HIPAA

"BAA" means the WhisperAI Business Associate Agreement that Customer accepts in its account settings, or signs, as updated under its terms.

"Controller", "Processor", "Data Subject", "Personal Data", "Processing", "Supervisory Authority", "Sub-processor" and "Special Categories of Personal Data" have the meanings given in the EU GDPR, or the equivalent terms in other Applicable Data Protection Laws.

"Customer Content" means audio and video files, live recordings, dictation, transcripts, translations, summaries, AI chat messages, speaker labels, prompts, custom vocabulary, file names and exports submitted to or created through the Services on Customer's instructions.

"Customer Personal Data" means Personal Data in Customer Content, or otherwise Processed by Provider on Customer's behalf, as described in Annex 1.

"Customer-Enabled Integration" means a third-party service that Customer or its users choose to connect to the Services. Examples are Google Drive (Cloud Sync) and AI assistants connected through the WhisperAI MCP connector, such as Claude or ChatGPT.

"HIPAA" means the Health Insurance Portability and Accountability Act of 1996, the HITECH Act and their regulations at 45 C.F.R. Parts 160 and 164.

"HIPAA Account" means a workspace or Developer API account on the Business Pro, Enterprise or Developer API plan. Customer must have accepted the BAA for it, and Provider must have confirmed in the Services that HIPAA mode is enabled.

"HIPAA-Eligible Services" means the services listed in Exhibit A of the BAA.

"PHI" means protected health information as defined at 45 C.F.R. § 160.103.

"Restricted Transfer" means a transfer of Personal Data from the EEA, the United Kingdom or Switzerland to a country without an adequacy decision from the relevant authority.

"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 transmitted, stored or otherwise Processed by Provider or a Sub-processor, as described in Article 4(12) EU GDPR. It does not include unsuccessful attempts or events that do not compromise the security of Customer Personal Data, such as pings, port scans, blocked log-in attempts or denial-of-service attacks.

"Services" means the WhisperAI services described in the Agreement. They include the web application, file transcription, live recording and Meeting Assistant, the Developer API, the Chrome extension and the mobile apps, together with any Customer-Enabled Integrations Customer chooses to use.

"SCCs" means the standard contractual clauses approved by Commission Implementing Decision (EU) 2021/914, as set out in Annex 4. "UK Addendum" means the International Data Transfer Addendum issued by the UK Information Commissioner's Office, in force from March 21, 2022.

2. Scope and Roles

2.1 **Scope.** This DPA applies to Provider's Processing of Customer Personal Data in providing the Services.

2.2 **Roles.** For Customer Personal Data, Customer is the Controller (or a Processor acting for a third-party controller), and Provider is the Processor (or Sub-processor). For CCPA/CPRA purposes, Customer is a "Business" and Provider is a "Service Provider" (Section 14). For PHI in a HIPAA Account, Customer is a Covered Entity or Business Associate, and Provider is its Business Associate or Subcontractor under the BAA.

2.3 **Provider as independent controller.** Provider acts as an independent Controller when it Processes Personal Data for its own purposes, and that Processing is governed by its Privacy Policy, not this DPA. These purposes are:

- managing the customer relationship
- billing and payments, including Stripe and Apple/RevenueCat
- product analytics (Mixpanel)
- fraud and abuse prevention
- permitted marketing
- the public marketing website and its consent-gated analytics and advertising
- meeting its own legal obligations

Where Provider Processes Personal Data solely to deliver the Services on Customer's documented instructions, Provider acts as Processor under this DPA.

2.4 **Compliance.** Each party will comply with its own obligations under Applicable Data Protection Laws.

3. Details of Processing

The subject matter, nature, purpose and duration of the Processing, and the categories of Data Subjects and Personal Data, are set out in Annex 1.

4. Instructions and Customer Responsibilities

4.1 **Documented instructions.** Provider will Process Customer Personal Data, including any transfer to a third country, only on Customer's documented instructions, or as required by law. Those instructions include the Agreement, this DPA, the BAA where it applies, and Customer's choice of features, settings and Customer-Enabled Integrations. Where required by law and permitted, Provider will tell Customer about a legal requirement before Processing under it.

4.2 **Unlawful instructions.** Provider will tell Customer if, in its opinion, an instruction infringes Applicable Data Protection Laws. It may suspend that instruction until Customer confirms, amends or withdraws it.

4.3 **Customer responsibilities.** Customer is responsible for the lawfulness of its instructions and of the Customer Content it submits. That includes giving all required notices and obtaining all consents and lawful bases needed for Provider and its Sub-processors to Process it.

4.4 **Recording consent.** Customer is responsible for complying with all recording, wiretapping, consent, employment, biometric and communications laws when it records, uploads or transcribes calls, meetings or other audio. This includes all-party-consent laws.

4.5 **Sensitive information.** Recordings may lawfully contain sensitive information, such as legal interviews, health or religious topics, or other Special Categories of Personal Data. Customer may submit such information where it has a lawful basis and has determined that the safeguards in this DPA are appropriate. Customer must not submit:

- (a) PHI, except in a HIPAA Account under Section 4.6
- (b) payment card numbers or authentication credentials
- (c) other information whose Processing legally requires a certification, contract or control that Provider does not offer

4.6 **HIPAA and PHI.**

(a) **HIPAA Accounts.** Provider offers HIPAA Accounts on the Business Pro, Enterprise and Developer API plans. For PHI in a HIPAA Account, Provider acts as a Business Associate under the BAA and complies with the HIPAA requirements that apply to business associates.

(b) **Conditions.** Customer may create, receive, maintain or transmit PHI using the Services only if all of the following are true:

- (i) Customer has accepted the BAA for that account
- (ii) Provider has confirmed in the Services that HIPAA mode is enabled
- (iii) the PHI is submitted only through the HIPAA-Eligible Services in that HIPAA Account

(c) **Outside a HIPAA Account.** PHI submitted anywhere else is not covered by the BAA, and Customer must not submit it there. That includes other plans or accounts, the mobile apps, YouTube import, Customer-Enabled Integrations, support requests, email, and account, billing or payment details.

(d) **Precedence.** For PHI, the BAA controls over this DPA.

4.7 **Unauthorized PHI and restricted content.** Customer is responsible for ensuring that its users comply with Sections 4.5 and 4.6, and shall notify Provider promptly if it learns that PHI or other prohibited content has been submitted outside a HIPAA Account. If Provider becomes aware of such content, it may suspend further Processing of it, restrict access, and coordinate with Customer on its deletion or return. Provider does not undertake to inspect Customer Content.

5. Confidentiality

Provider will ensure that persons authorized to Process Customer Personal Data are bound by confidentiality obligations.

6. Security Measures

6.1 **Measures.** Provider will implement appropriate technical and organizational measures to protect Customer Personal Data, as required by Article 32 EU GDPR and other Applicable Data Protection Laws. The current measures are described in Annex 2.

6.2 **Changes.** Provider may update the measures from time to time, subject to Section 6.1.

7. Security Incident Notification

7.1 **Notice.** Provider will notify Customer without undue delay after becoming aware of a Security Incident affecting Customer Personal Data. Provider does not need to complete its investigation before notifying Customer. Unsuccessful attempts and other security events that are not Security Incidents do not require notice.

7.2 **Content.** To the extent known, the notice will describe:

- the nature of the incident, including the categories and approximate number of Data Subjects and records
- its likely consequences
- the measures taken or proposed to address it and mitigate its effects
- a contact person

Provider may give the information in phases, without further undue delay.

7.3 **Customer notices.** Customer is responsible for notifications it must make to Supervisory Authorities, regulators and Data Subjects. Provider will assist as required by Article 28(3)(f) EU GDPR.

7.4 **Method.** Notices go to the security or administrative contact designated in Customer's account, or otherwise to the account owner's email address.

7.5 **No admission.** Notifying Customer of a Security Incident is not an admission of fault or liability.

7.6 **PHI.** For PHI in a HIPAA Account, the reporting terms of the BAA apply instead of this Section 7.

8. Sub-processors and Integrations

8.1 **Authorization.** Customer gives Provider general written authorization to engage Sub-processors, subject to this Section. The current Sub-processors are listed in Annex 3.

8.2 **Sub-processor terms.** Provider will impose on each Sub-processor, by written contract, data protection obligations no less protective than those in this DPA, to the extent relevant to the service it provides. Each Sub-processor that receives PHI from a HIPAA Account is bound by a business associate agreement with Provider.

8.3 **Changes and objection.** Provider will inform Customer of any intended addition or replacement of a Sub-processor at least 14 days before it starts Processing Customer Personal Data, by updating the published list. Customer may object on reasonable data-protection grounds within that period.

8.4 **Liability.** Provider remains liable to Customer for each Sub-processor's performance of its data protection obligations.

8.5 **Customer-Enabled Integrations.** A Customer-Enabled Integration is not a Provider Sub-processor. When Customer or its user connects one:

- data flows to or from that service on Customer's instruction, under the terms between Customer and that service
- for the WhisperAI MCP connector, the connected AI assistant receives the transcripts, summaries, titles and download links needed for each request, within the scopes the user approves
- to the extent permitted by Applicable Data Protection Laws, Provider is not responsible for that service's independent Processing, storage, retention or use of data after it has been transmitted on Customer's instructions

Customer-Enabled Integrations are not HIPAA-Eligible Services and must not be used with PHI.

9. Data Subject Requests

9.1 **Self-service.** The Services let Customer export, correct and delete Customer Content and account data. Customer can use these tools to answer most Data Subject requests.

9.2 **Assistance.** Where the tools are not enough, Provider will assist Customer, by appropriate technical and organizational measures and insofar as possible, in responding to requests to exercise Data Subject rights.

10. Compliance Assistance

10.1 Provider will assist Customer, at Customer's reasonable cost, with its obligations under Articles 32 to 36 of the EU GDPR and equivalent laws, taking into account the nature of the Processing and the information available to Provider.

10.2 Provider will make available the information necessary to demonstrate compliance with this DPA, as set out in Section 13.

11. International Transfers

11.1 **Locations.** Provider and its Sub-processors Process Customer Personal Data in the United States and Germany, as shown in Annex 3.

11.2 **EEA transfers.** For Restricted Transfers from the EEA, the SCCs in Annex 4 are incorporated: Module Two where Customer is a Controller, and Module Three where Customer is a Processor.

11.3 **UK and Swiss transfers.** For Restricted Transfers from the UK, the UK Addendum in Annex 4 applies. For Restricted Transfers from Switzerland, the SCCs apply with the Swiss modifications in Annex 4.

11.4 **Conflict.** If this DPA conflicts with the SCCs or the UK Addendum, the SCCs or the UK Addendum prevail.

12. Return and Deletion

12.1 **During the term.** Customer can export or delete Customer Content at any time through the Services. Provider does not delete Customer Content automatically.

12.2 **End of the Services.** At the end of the Services, Provider will, at Customer's choice, delete or return Customer Personal Data, unless the law requires Provider to keep it. Customer makes that choice by exporting its content, deleting it in the Services, deleting its account, or asking Provider in writing to delete it. For a HIPAA Account, the return and destruction terms of the BAA apply instead.

12.3 **Backups and exceptions.** Customer Personal Data in backups is deleted as those backups expire. Provider may keep data the law requires it to keep, and aggregated or de-identified data that is no longer Personal Data.

12.4 **Copies outside the Services.** Deletion in the Services does not remove copies that Customer has exported or sent to a Customer-Enabled Integration.

13. Audit and Records

13.1 **Records.** Provider will keep records of its Processing activities as required by Article 30(2) EU GDPR and equivalent laws.

13.2 **Information.** Once in any 12-month period, on written request, Provider will make available, subject to confidentiality, the information necessary to demonstrate compliance with Article 28 EU GDPR, including its current security documentation.

13.3 **Audits.** If that information is not enough to show compliance, Customer may request an audit. The audit must meet these conditions, and Customer bears its cost:

- at least 30 days' notice, except on a regulator's order
- during business hours
- by an independent auditor who is bound by confidentiality and is not a Provider competitor
- without compromising other customers' data

13.4 **Mandatory rights.** Nothing in this Section limits a Supervisory Authority's audit rights, the rights of the Secretary of Health and Human Services under the BAA, Customer's audit rights under Clause 8.9 of the SCCs, or any other audit right that cannot lawfully be restricted.

14. CCPA/CPRA Service Provider Terms

14.1 Provider Processes Personal Information as a Service Provider for the business purposes in Annex 1. Provider will not:

- (a) sell or share it
- (b) retain, use or disclose it for any other purpose, including any commercial purpose, or outside the direct business relationship with Customer
- (c) combine it with Personal Information from other sources, except as the CCPA/CPRA permits

14.2 Provider will provide the same level of privacy protection the CCPA/CPRA requires of Businesses, and will notify Customer if it can no longer meet these obligations. Customer may then take reasonable steps to stop and remediate unauthorized use.

14.3 Customer may take reasonable steps to ensure Provider uses Personal Information consistently with Customer's CCPA/CPRA obligations, including through Section 13.

14.4 Provider certifies that it understands and will comply with this Section, and will impose equivalent obligations on Sub-processors.

15. AI Processing

15.1 **No training on PHI.** Provider will not use PHI from a HIPAA Account to train, fine-tune or improve any machine-learning or artificial-intelligence model.

15.2 **Accuracy.** AI-generated transcripts, summaries and translations may contain errors. Customer is responsible for reviewing outputs before relying on them, and must not present them as human-generated.

16. Liability

16.1 **Cap.** To the extent permitted by law, each party's total liability arising out of this DPA is limited to the fees Customer paid Provider under the Agreement in the 12 months before the event giving rise to the claim. Neither party is liable under this DPA for indirect, incidental, special, consequential or punitive damages, or for lost profits, revenue or goodwill.

16.2 **Exceptions.** These limits do not apply to liability that cannot lawfully be limited, to a party's fraud or willful misconduct, or to Customer's payment obligations. The SCCs, where they apply, give Data Subjects direct rights that are not subject to these limits.

Liability for PHI is governed by the BAA.

17. Precedence and General Terms

17.1 **Order of precedence.** For the Processing of Customer Personal Data, the following apply in this order. This DPA prevails over the Privacy Policy where they conflict.

1. the SCCs and UK Addendum, for Restricted Transfers
2. the BAA, for PHI
3. this DPA
4. the Agreement

17.2 **Replacement.** This DPA replaces Version 2 and any other earlier standard WhisperAI data processing agreement, without affecting claims that arose earlier.

17.3 **Updates.** Provider may update this DPA to reflect changes in law or the Services by publishing an updated version.

17.4 **Governing law.** This DPA is governed by the laws of the State of Delaware, without regard to conflict-of-law rules, and the state and federal courts located in Delaware have exclusive jurisdiction, as in the Terms of Service. This does not apply where the SCCs or the UK Addendum require a different law or forum.

17.5 **General.** If any provision is invalid, the rest remains in effect. Electronic signatures and counterparts are valid.

Annex 1 — Processing Details

A. Parties.

Data exporter. Customer, as identified in the Agreement or its account.

- Contact: the account owner's email address, or the privacy contact Customer designates
- Role: Controller, or Processor acting for a third-party controller. For PHI, a Covered Entity or Business Associate.
- Activities: use of the Services

Data importer. WhisperAI Technology Inc., PO Box 572551, Tarzana, CA 91357, United States.

- Contact: support@whisperai.com

- Role: Processor. For PHI, a Business Associate.
- Activities: providing the Services

Signature. Customer's acceptance of the Agreement is treated as signature of the SCCs and the UK Addendum, including their annexes.

B. Description of Processing

Item	Detail
Subject matter	Hosted transcription, real-time transcription and dictation, live recording and Meeting Assistant, speaker labeling, translation, AI summaries and chat, editing, search, export, collaboration and the Developer API
Nature and purpose	Receiving audio and video that Customer uploads, records, dictates, imports from YouTube or submits through the Developer API; converting, storing, transcribing, translating, summarizing and labeling it; making the results available to Customer, including through notifications to its devices; user authentication, support and security of the Services
Duration	The term of the Agreement, and afterwards until the data is deleted under Section 12
Data Subjects	Customer's authorized users; people whose voices, names or information appear in Customer Content; recipients of content Customer shares
Account data	Name, email, hashed password or Google/Microsoft sign-in identifiers, organization membership and role, session and OAuth tokens, API keys
Content data	Audio and video, transcripts, translations, summaries, AI chat messages, speaker labels, prompts, custom vocabulary, file names, duration, language and timestamps
Collaboration data	Folders, tags, sharing settings, organization audit-log entries

Item	Detail
Usage and operational data	Request and error logs, usage counters, Developer API request records
Not covered	Billing, payment, product-analytics and marketing data, which Provider Processes as a Controller (Section 2.3)
Sensitive data	May be included where Customer has a lawful basis (Section 4.5). PHI is permitted only in a HIPAA Account under the BAA. Safeguards: the measures in Annex 2, and for PHI, the BAA
Frequency	Continuous, as Customer uses the Services
Retention	Until Customer deletes it, as set out in Section 12
Transfers to Sub-processors	Same subject matter, nature and duration as above, limited to each Sub-processor's service in Annex 3
CCPA/CPRA business purposes	Providing, securing, maintaining, debugging and supporting the Services

C. Competent Supervisory Authority. Determined under Clause 13 of the SCCs.

Annex 2 — Technical and Organizational Measures

The Services run on Google Cloud and Neon managed PostgreSQL in the United States.

Area	Measures
Encryption	TLS 1.2 or higher for data in transit; AES-256 encryption at rest in Google Cloud Storage and Neon
Authentication	Email and password stored as bcrypt hashes, with email-code verification at sign-up, or Google or Microsoft sign-in; server-side sessions in secure, HTTP-only cookies; OAuth 2.0 for the MCP connector; scoped API keys for the Developer API

Area	Measures
Authorization and isolation	Role-based access enforced server-side; data scoped to the authenticated user and organization; short-lived signed links for file uploads and downloads
Availability and resilience	Managed database backups with point-in-time recovery (Neon); redundant object storage (Google Cloud Storage)
Logging and monitoring	Application and request logging; error monitoring (Sentry)
Personnel	Confidentiality obligations; production access limited to personnel who need it
Sub-processors	Written data protection terms with each Sub-processor, and business associate agreements with Sub-processors that receive PHI
Incident response	A process for investigating, containing and notifying Security Incidents
HIPAA Accounts	The administrative, physical and technical safeguards required by the HIPAA Security Rule

Not claimed: SOC 2 attestation, ISO/IEC 27001 certification or HITRUST certification. No government body certifies HIPAA compliance.

Annex 3 — Sub-processors and Integrations

Sub-processor	Service	Customer Personal Data	Location	HIPAA Accounts
Google LLC (Google Cloud)	Cloud infrastructure for hosting, storing and processing the Services	All categories	United States	Yes, under BAA

Sub-processor	Service	Customer Personal Data	Location	HIPAA Accounts
Neon, Inc.	Managed PostgreSQL database	All persisted data except raw audio files	United States	Yes, under BAA
AssemblyAI, Inc.	Transcription, real-time transcription and dictation, speaker labeling, translation	Audio, transcripts, speaker labels, language	United States	Yes, under BAA
OpenAI, L.L.C.	Speech-to-text, AI summaries, AI chat, translation and export formatting	Audio, transcript text, prompts and chat messages	United States	Yes, under BAA
Functional Software, Inc. (Sentry)	Error and performance monitoring	Error reports, request metadata, user ID, IP address, device and browser details	United States	Yes, under BAA
Twilio Inc. (SendGrid)	Transactional email	Email address, name, notification content	United States	No
Dumpling Software UG (Supadata)	Import of YouTube transcripts	YouTube video links and the transcripts returned	Germany; United States	No
650 Industries, Inc. (Expo)	Push notifications to the mobile apps	Device push tokens and notification content, including recording names	United States	No

Customer-Enabled Integrations (not Provider Sub-processors; see Section 8.5)

Integration	What it does	Data involved
Google Drive (Cloud Sync)	Imports files from the folder the user selects, and saves transcripts back to it	Selected files; generated transcripts and exports
AI assistants via the WhisperAI MCP connector (for example Claude, ChatGPT)	Lets the user transcribe, search, summarize and export from inside the assistant	Results the user requests
Google and Microsoft sign-in	Authentication	Name, email, account identifier

Outside this DPA. Provider uses the following as an independent Controller under Section 2.3 and its Privacy Policy, not as Sub-processors: Stripe; Apple and RevenueCat; Mixpanel; Google Analytics, Google Ads and OpenAI Ads.

Annex 4 — International Transfer Terms

A. EU Standard Contractual Clauses. The SCCs (official text) are incorporated by reference with these selections:

Clause	Selection
Modules	Module Two (Controller to Processor) where Customer is a Controller; Module Three (Processor to Processor) where Customer is a Processor
Clause 7 (docking)	Included
Clause 9(a) (sub-processors)	Option 2, general written authorization, with the 14-day notice in Section 8.3
Clause 11(a) (redress)	Optional independent dispute resolution not included
Clause 13 (supervision)	The supervisory authority determined under Clause 13(a)
Clause 17 (governing law)	Law of Ireland

Clause	Selection
Clause 18 (forum)	Courts of Ireland
Annex I.A, I.B, I.C	Annex 1, Sections A, B and C of this DPA
Annex II	Annex 2 of this DPA
Annex III	Annex 3 of this DPA

B. UK Addendum. For Restricted Transfers from the UK, the UK Addendum (version B1.0) is incorporated. Table 1 is completed with Annex 1, Section A; Table 2 with Part A above; and Table 3 with Annexes 1 to 3. For Table 4, neither party may end the Addendum under its Section 19.

C. Switzerland. For Restricted Transfers from Switzerland, the SCCs apply with these changes:

- references to the EU GDPR include the FADP
- the competent authority is the Swiss Federal Data Protection and Information Commissioner
- "Member State" does not prevent Data Subjects in Switzerland from bringing claims where they habitually reside