DATA PROCESSING AGREEMENT

Last Updated: August 24, 2026

This Data Processing Agreement, including its Annexes ("**DPA**" or "**Addendum"**), is entered into as of the last date executed below by Wispr AI, Inc., a Delaware corporation ("**Wispr**"), and Customer (as set forth in the applicable terms between Wispr and Customer regarding use of the Service (the "**Agreement**").

Wispr provides its proprietary voice-to-text software-as-a-service platform (the "**Service**") to Customers. The provision of the Service involves the Processing of Personal Data subject to the Data Protection Laws, and the purpose of this DPA is to set forth the terms under which Wispr Processes the Personal Data.

THIS DPA APPLIES BETWEEN THE PARTIES WHERE A REPRESENTATIVE OF CUSTOMER CLICKS A BOX INDICATING ACCEPTANCE, TRANSFERS PERSONAL DATA TO WISPR FOR PROCESSING BY MEANS OF THE SERVICE, OR OTHERWISE AFFIRMATIVELY INDICATES ACCEPTANCE OF THIS DPA. BY DOING SO, YOU: (A) AGREE TO THIS DPA ON BEHALF OF THE ORGANIZATION, COMPANY, OR OTHER LEGAL ENTITY FOR WHICH YOU ACT ("**CUSTOMER**"); AND (B) REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND CUSTOMER AND ITS AFFILIATES TO THIS DPA. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT AGREE WITH THIS DPA, YOU MAY NOT DIRECTLY OR INDIRECTLY TRANSFER PERSONAL DATA TO WISPR. WISPR RESERVES THE RIGHT TO MODIFY OR UPDATE THE TERMS OF THIS DPA IN ITS DISCRETION, THE EFFECTIVE DATE OF WHICH WILL BE THE EARLIER OF (I) 30 DAYS FROM THE DATE OF SUCH UPDATE OR MODIFICATION AND (II) CUSTOMER'S CONTINUED TRANSFER OF PERSONAL DATA.

Wispr reserves the right to modify or update this DPA in its sole discretion. If Customer and Wispr have executed a written data processing agreement governing the processing of personal data by means of the Service, then the terms of such signed data processing agreement between the parties will supersede this DPA.

This DPA is incorporated into and made part of the Agreement.

The parties agree as follows:

1) **Definitions**. Unless otherwise defined in the Agreement, all capitalized terms used in this DPA will have the meanings given to them herein or in applicable Data Protection Laws.

   "**Controller**" means the entity or Business which solely or jointly with other entities determines the purposes and means of the Processing of Personal Data and for the purposes of this Addendum means Customer.

   "**Data Breach**" has the meaning given to it in the Data Protection Laws and for the purpose of this Addendum relates to the personal data Processed by Wispr on behalf of Customer.

   "**Data Protection Laws**" means to the extent applicable to Customer's use of the Service, all applicable data protection and privacy laws, their implementing regulations, regulatory guidance, and secondary legislation, each as updated or replaced from time to time, including, as they may apply: (i) the General Data Protection Regulation ((EU) 2016/679) (the "**GDPR**"), and any applicable national implementing laws; (ii) the UK General Data Protection Regulation ("**UK GDPR**") and the UK Data Protection Act 2018; (iii) U.S. legislation (e.g., the California Consumer Privacy Act and the California Privacy Rights Act); and (iv) any other laws that may be applicable.

   "**Data Subject**" means the identified or identifiable person to whom the Personal Data relates, as defined in applicable Data Protection Laws.

"**EEA**" means the European Economic Area.

"**EU Standard Contractual Clauses"** or **"EU SCCs"** or **"Clauses"** means the standard contractual clauses for the transfer of Personal Data to third countries, as described in Article 46 of the EU GDPR, approved by the European Commission's Implementing Decision (EU) 2021/914 of 4 June 2021, as may be amended, updated, or replaced from time to time.

"**Personal Data**" has the meaning given to it in the Data Protection Laws and for the purpose of this Addendum relates to the personal data Processed by Wispr on behalf of Customer as described in Section 3.

"**Processing**" has the meaning given to it in the Data Protection Laws and "process", "processes" and "processed" will be construed accordingly.

"**Processor**" means the entity or Service Provider which Processes Personal Data on behalf of the Controller, as defined in applicable Data Protection Laws and for the purposes of this Addendum means Wispr.

2) Compliance with Laws. Each party will comply with the Data Protection Laws as applicable to it. In particular, Customer will comply with its obligations as Controller (or on behalf of Controller) and Wispr will comply with its obligations as Processor.

3) Data Processing

a) Roles of the Parties. The Parties acknowledge and agree that with regard to the Processing of Personal Data, where such terms are used by applicable Data Protection Laws, (i) the Customer is the Controller, (ii) Wispr is the Processor or Service Provider and that (iii) the Processor may engage sub-Processors or other Service Providers pursuant to the requirements set forth in Section 10 below.

b) Customer Obligations. Customer as Controller undertakes that all instructions for the Processing of Personal Data under the Agreement or this Addendum or as otherwise agreed will comply with the Data Protection Laws, and such instructions will not in any way cause Wispr to be in breach of any Data Protection Laws. The Customer will have sole responsibility for the means by which the Customer acquired the Personal Data.

c) Wispr's Processing of Personal Data

i) Wispr will Process Personal Data only in accordance with Customer's (i) instructions as outlined in the Agreement and this Addendum or (ii) as otherwise documented by Customer, in either event only as permitted by applicable Data Protection Laws and for purpose of providing the Service to Customer in accordance with the terms of the Agreement.

ii) Unless prohibited by applicable law, Wispr will notify Customer if in its opinion, an instruction infringes any Data Protection Law to which it is subject, in which case Wispr will be entitled to suspend performance of such instruction without any kind of liability towards the Customer, until Customer confirms in writing that such instruction is valid under such Data Protection Law. Any additional instructions regarding the manner in which Wispr Processes the Personal Data will require prior written agreement between Wispr and Customer.

iii) Wispr will not disclose Personal Data to any government, except as necessary to comply with applicable law or a valid and binding order of a law enforcement agency (such as a subpoena or court order). If Wispr receives a binding order from a law enforcement agency for Personal

Data, Wispr will notify Customer of the request it has received so long as Wispr is not legally prohibited from doing so.

iv) Where Wispr acts as Customer's Service Provider, Wispr shall not: (i) sell Personal Data; (ii) collect, retain, use, or disclose Personal Data (a) for any purpose other than providing the Service as specified in the Agreement and this Addendum or (b) outside of the direct business relationship between Wispr and Customer; or (iii) combine this Personal Data with Personal Data that Wispr obtains from other sources except as permitted by applicable Data Protection Laws. Wispr certifies that it understands the prohibitions outlined in this Section 3(c)(iv) and will comply with them.

v) Wispr will take reasonable steps to ensure that individuals with access to or involved in the Processing of Personal Data are subject to appropriate confidentiality obligations and/or are bound by related obligations under Data Protection Laws or other applicable laws.

d) Duration; Purposes. The duration of the Processing, the nature and specific purposes of the Processing, the types of Personal Data Processed, and categories of Data Subjects under this Addendum are further specified in the Annexes to this Addendum and, on a more general level, in the Agreement.

4) Transfers of Personal Data. Wispr shall transfer Personal Data between jurisdictions as a Data Processor in accordance with applicable Data Protection Laws, including, as relevant, provisions of this Section 4.

a) Transfers of Personal Data Outside the EEA

i) Transfers to countries that offer adequate level of data protection. Personal Data may be transferred from EEA to other jurisdictions where such jurisdictions are deemed to provide an adequate level of data protection under applicable Data Protection Laws.

ii) Transfers to other third countries. If the Processing of Personal Data includes transfers from EEA/EU Member States to countries outside the EEA/EU which have not been deemed adequate under applicable Data Protection Laws, the parties' EU Standard Contractual Clauses are hereby incorporated into and form part of this Addendum. The Parties agree to include the optional Clause 7 (Docking clause) to the EU SCCs incorporated into this Addendum. With regards to clauses 8 to 18 of the EU SCCs, the different modules and options will apply as follows:

(1) Module Two shall apply.

(2) The Option within Clause 11(a) of the EU SCCs, providing for the optional use of an independent dispute resolution body, is not selected.

(3) The Options and information required for Clauses 17 and 18 of the EU SCCs, covering governing law and jurisdiction, are outlined in Section 14 of this Addendum.

(4) Option 2 within Clause 9(a) of the EU SCCs, covering authorization for sub-processors, is selected, as discussed within Section 10 of this Addendum.

b) Transfers of Personal Data Outside Switzerland. If Personal Data is transferred from Switzerland in a manner that would trigger obligations under the Federal Act on Data Protection of Switzerland ("FADP"), the EU SCCs shall apply to such transfers and shall be deemed to be modified in a manner that incorporates relevant references and definitions that would render such EU SCCs an

adequate tool for such transfers under the FADP.

c) Transfers of Personal Data Outside the UK. If Personal Data is transferred in a manner that would trigger obligations under UK GDPR, the parties agree that Annex IV shall apply.

d) Annexes. This Addendum and its Annexes, together with the Agreement, including as relevant applicable Clauses, serve as a binding contract that sets out the subject matter, duration, nature, and purpose of the Processing, the type of Personal Data and categories of data subjects as well as the obligations and rights of the Controller. Wispr may execute relevant contractual addenda, including as relevant the EU SCCs (Module 3) with any relevant Subprocessor (as hereinafter defined, including Affiliates). Unless Wispr notifies Customer to the contrary, if the European Commission subsequently amends the EU SCCs at a later date, such amended terms will supersede and replace any EU SCCs executed between the parties.

e) Alternative Data Export Solution. The parties agree that the data export solutions identified in this Section 4 will not apply if and to the extent that Customer adopts an alternative data export solution for the lawful transfer of Personal Data (as recognized under applicable Data Protection Laws), in which event, Customer shall reasonably cooperate with Wispr to implement such solution and such alternative data export solution will apply instead (but solely to the extent such alternative data export solution extends to the territories to which Personal Data is transferred under this Addendum).

f) Responsibilities of Controller. Customer shall be responsible for obligations corresponding to Data Controllers under Data Protection Laws.

5) Technical and organizational measures. Wispr will in relation to the Personal Data implement appropriate technical and organisational measures designed to ensure a level of security of Personal Data appropriate to the risk, as further described on Annex II of this Addendum. In assessing the appropriate level of security, Wispr will take into account the risks that are presented by Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise Processed.

6) Data Subjects rights. Wispr will assist Customer in responding to Data Subjects' requests exercising their rights under the Data Protection Laws. To that effect, Wispr will (i) to the extent permitted by applicable law, promptly notify Customer of any request received directly from Data Subjects to access, correct or delete its Personal Data without responding to that request, and (ii) upon written request from Customer, provide Customer with information that Wispr has available to reasonably assist Customer in fulfilling its obligations to respond to Data Subjects exercising their rights under the Data Protection Laws.

7) Data Protection Impact Assessments. If Customer is required under the Data Protection Laws to conduct a Data Protection Impact Assessment, then upon written request from Customer, Wispr will assist where reasonably possible in the fulfilment of the Customer's obligation as related to its use of the Service, to the extent Customer does not otherwise have access to the relevant information. If required under Data Protection Laws Wispr will provide reasonable assistance to Customer in the cooperation or prior consultation with Data Protection Authorities in relation to any applicable Data Protection Impact Assessment.

8) Audit of Technical and Organizational Measures. Wispr agrees to make available all information necessary to demonstrate its compliance with data protection policies and procedures implemented as part of the Service (i.e. third party audit report). To this end, upon written request (not more than once annually) Customer may, at its sole cost and expense, verify Wispr's compliance with its data protection obligations as specified in this Addendum by: (i) submitting a security assessment questionnaire to Wispr; and (ii) if Customer is not satisfied with Wispr's responses to the questionnaire,

then Customer may conduct an audit in the form of meetings with Wispr's information security experts upon a mutually agreeable date. Such interviews will be conducted with a minimum of disruption to Wispr's normal business operations and subject always to Wispr's agreement on scope and timings. The Customer may perform the verification described above either by itself or through a mutually agreed upon third party auditor, provided that Customer or its authorized auditor executes a mutually agreed upon Non-Disclosure Agreement. Customer will be responsible for any actions taken by its authorized auditor. All information disclosed by Wispr under this Section 8 will be deemed Wispr Confidential Information, and Customer will not disclose any audit report to any third party except as obligated by law, court order or administrative order by a government agency. Wispr will remediate any mutually agreed, material deficiencies in its technical and organizational measures identified by the audit procedures described in this Section 8 within a mutually agreeable timeframe.

9) **Breach notification.** If Wispr becomes aware of a Data Breach that results in unlawful or unauthorized access to, or loss, disclosure, or alteration of the Personal Data, which is likely to cause a risk to the fundamental rights and freedoms of the Data Subjects', then Wispr will notify the Customer without undue delay (but in no event no later than 72 hours) after becoming aware of such Data Breach and will co-operate with the Customer and take such reasonable commercial steps as agreed with the Customer to assist in the investigation, mitigation and remediation of such Data Breach. Wispr will provide all reasonably required support and cooperation necessary to enable Customer to comply with its legal obligations in case of a Data Breach pursuant to applicable Data Protection Laws.

10) **Sub-processing.** Customer agrees that Wispr may engage either Wispr affiliated companies or third parties providers as sub-Processors under the Agreement and this Addendum ("**Subprocessors**") and hereby authorizes Wispr to engage such Subprocessors in the provision of the Service. Wispr will restrict the Processing activities performed by Subprocessors to only what is necessary to provide the Service to Customer pursuant to the Agreement and this Addendum. Wispr will impose appropriate contractual obligations in writing upon the Subprocessors that are no less protective than this Addendum.

    Wispr maintains a list of all Subprocessors used by Wispr in the provision of Service which is set forth on Annex III to this Addendum as well as available at https://trust.wispr.ai/. Wispr may amend the list of Subprocessors by adding or replacing Subprocessors at any time and will provide at least 10 days' prior written notice of any such changes if Customer subscribes to receive updates at trust.wispr.ai. Customer will be entitled to object to a new Subprocessor by notifying Wispr in writing the reasons of its reasonable objection. Wispr will work in good faith to address Customer's objections. If Wispr is unable or unwilling to adequately address Customer's objections to its reasonable satisfaction, then Customer may terminate this Addendum and the Agreement in accordance with terms of the Agreement.

11) **Return or Deletion of Personal Data**. Wispr will delete or return, in Customer's discretion and upon Customer's written request, Personal Data within ninety (90) days following the termination or expiration of the Agreement unless otherwise required by applicable Data Protection Laws.

12) **Entire Agreement; Conflict**. Except as amended by this Addendum, the Agreement will remain in full force and effect. If there is a conflict between the Agreement and this Addendum, the terms of this Addendum will control.

13) **Law and Jurisdiction**. This Addendum shall be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement, unless required otherwise by applicable Data Protection Laws. For the purposes of Clauses 17 and 18 of the EU SCCs, where applicable, to the extent that the governing law and jurisdiction provisions in the Agreement do not meet the requirements of the EU SCCs, the parties select Option 2 of Clause 17, and agree that the EU SCCs shall be governed by the law of the EU Member State in which the data exporter is established; where such law does not allow for third-party beneficiary rights, the EU SCCs shall be governed by the laws

of the country of Ireland. Pursuant to Clause 18, any dispute between the Parties arising from the EU SCCs shall be resolved by the courts of Ireland, and the Parties submit themselves to such jurisdiction. For the purposes of Clause 13 of the GDPR, the Supervisory Authority shall be the data exporter's applicable Supervisory Authority. Data exporter shall notify data importer of the applicable Supervisory Authority by email at support+privacy@wisprflow.ai and shall provide any necessary updates without undue delay.

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

Name: The Customer as defined above.

Role: Controller

Activities relevant to the data transferred under these Clauses: Purchase of access to and use of the Service under the Agreement

Data importer(s):

Name: Wispr AI, Inc.

Address: 444 Townsend Street San Francisco, CA, 94107

Contact details: support+privacy@wisprflow.ai

Activities relevant to the data transferred under these Clauses: Processing of personal data to provide the Service as set forth in the Agreement

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred:

Employees, contractors, and personnel of Customers, End-users of Customers' services

Categories of personal data transferred:

- *Identification Data: Name, date of birth, gender*
- *Contact Information: Address, phone numbers, email addresses*
- *Audio Data: Voice recordings or audio files submitted for transcription*
- *Transcription Data: Textual representations of audio inputs*
- *Usage Data: Interaction logs, preferences, and settings*
- *Device and Technical Data: IP addresses, device type, browser type, operating system*

- *Customer and its Users (as defined in the Agreement) will not intentionally provide Wispr with sensitive or special-category Personal Data. If you entered into a separate business associate agreement ("BAA"), the processing of such PHI will be governed by such BAA.*

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):

Continuous basis during the Term of the Agreement

Nature of the processing:

As specified under the Agreement (i.e., the provision of Services to Customer)

Purpose(s) of the data transfer and further processing:

For the provision of the specific business purpose and Service under the Agreement

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:

During the term of the Agreement and as provided therein.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:

During the Term of the Agreement for the purpose of providing the Service.

C. *COMPETENT SUPERVISORY AUTHORITY*

The competent supervisory authority/ies applicable to Data Exporter as notified to Data Importer in accordance with Section 14 of the Addendum.

ANNEX II –
TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Data Importer has taken and will maintain appropriate administrative, technical, physical and procedural security measures, for the protection of the Personal Data, with such measures located at https://trust.wispr.ai/.

ANNEX III – LIST OF SUB-PROCESSORS

Data Importer maintains a list of Sub-processors that process Personal Data located at https://trust.wispr.ai/.

ANNEX IV
UK ADDENDUM TO EU STANDARD CONTRACTUAL CLAUSES

PART 1: TABLES

Table 1: Parties

Start date	Effective the date of the execution of the Addendum	
The Parties	**Exporter (who sends the Restricted Transfer)** **As listed in Annex I**	**Importer (who receives the Restricted Transfer)** **As listed in Annex I**
Parties' Details	**As listed in Annex I**	**As listed in Annex I**
Key Contacts	**As listed in Annex I**	**As listed in Annex I**

Table 2: Selected SCCs, Modules and Selected Clauses

"Addendum EU SCCs	The version of the approved EU SCCs agreed to in the Addendum to which this UK Addendum is appended to, including the Appendix Information.

Table 3: Appendix Information

"Appendix Information" means the information which must be provided for the selected modules as set out in the Appendix of the Approved SCCs (other than the Parties), and which for this UK Addendum is set out in:

Annex 1A: List of Parties: See Annex I
Annex 1B: Description of Transfer: Annex I
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: Annex II
Annex III: List of Sub processors: Annex III

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum: ☐ Importer ☐ Exporter ☒ neither Party

PART 2: MANDATORY CLAUSES

"Mandatory Clauses"	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.