Wispr AI, Inc.
Data Processing Addendum

This Data Processing Addendum ("DPA") forms part of and is incorporated into the Wispr AI, Inc. ("Wispr" or "Vendor") Master Services Agreement ("Agreement") and any Order Forms entered into by and between Wispr and any customer using their products ("Customer") (together, the "Parties"). This DPA sets forth Customer's instructions for the processing of Personal Data in connection with the services described in the Agreement ("Services") and the rights and obligations of both Parties. Except as expressly set forth in this DPA, the Agreement shall remain unmodified and in full force and effect. In the event of any conflicts between this DPA and the Agreement, this DPA will govern to the extent of the conflict.

1. **Definitions.** For the purposes of this DPA, the following terms shall have the meanings set out below. Capitalized terms used but not defined in this DPA shall have the meanings given in the Agreement. All other terms in this DPA not otherwise defined in the Agreement shall have the corresponding meanings given to them in Privacy Laws.

a. "Controller to Processor Clauses" means (a) in respect of transfers of Personal Data subject to the GDPR, the standard contractual clauses for the transfer of Personal Data to third countries set out in Commission Decision 2021/914 of 4 June 2021, specifically including Module 2 (Controller to Processor) ("EU SCCs"); and (b) in respect of transfers of Personal Data subject to the UK GDPR, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (version B.1.0) issued by the UK Information Commissioner ("UK Addendum"), in each case as amended, updated or replaced from time to time.

b. "EU/UK Privacy Laws" means: (a) the General Data Protection Regulation 2016/679 (the "GDPR"); (b) the Privacy and Electronic Communications Directive 2002/58/EC; (c) the UK Data Protection Act 2018, the UK General Data Protection Regulation as defined by the UK Data Protection Act 2018 as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (together with the UK Data Protection Act 2018, the "UK GDPR"), and the Privacy and Electronic Communications Regulations 2003; and (d) any relevant law, directive, order, rule, regulation or other binding instrument which implements any of the above, in each case, as applicable and in force from time to time, and as amended, consolidated, re-enacted or replaced from time to time.

c. "Personal Data" means any information Vendor processes on behalf of Customer to provide the Services that is defined as "personal data" or "personal information" under any Privacy Laws.

d. "Privacy Laws" means, as applicable, EU/UK Privacy Laws, US Privacy Laws and any similar law of any other jurisdiction which relates to data protection, privacy or the use of Personal Data, in each case, as applicable and in force from time to time, and as amended, consolidated, re-enacted or replaced from time to time.

e. "Processor to Processor Clauses" means (a) in respect of transfers of Personal Data subject to the GDPR, the standard contractual clauses for the transfer of personal data to third countries set out in Commission Decision 2021/914 of 4 June 2021, specifically including Module 3 (Processor to Processor); and (b) in respect of transfers of Personal Data subject to the UK GDPR, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (version B.1.0) issued by the UK Information Commissioner, in each case as amended, updated or replaced from time to time.

f. "Third Country" means any country or territory outside of the scope of the data protection laws of the

European Economic Area or the UK, as relevant, excluding countries or territories approved as providing adequate protection for Personal Data by the relevant competent authority from time to time.

g. "US Privacy Laws" means, as applicable, the California Consumer Privacy Act, as amended by the California Privacy Rights Act, the Virginia Consumer Data Protection Act, the Colorado Privacy Act, Connecticut Data Privacy Act, Utah Consumer Privacy Act, and any similar law of any other state which relates to data protection, privacy or the use of Personal Data.

2. **Amendments.** The Parties agree to negotiate in good faith modifications to this DPA if changes are required for Vendor to continue to process the Personal Data as contemplated by the Agreement or this DPA in compliance with Privacy Laws, or to address the legal interpretation of the Privacy Laws. Vendor reserves the right to update this DPA as necessary to comply with Privacy Laws or evolving legal requirements, provided that any such updates do not materially diminish Customer's rights or materially increase Customer's obligations under this DPA. Vendor shall notify Customer of any such updates in writing at least thirty (30) days prior to their effective date, unless a shorter notice period is required by law.

3. **Roles of the Parties.** The Parties acknowledge that for purposes of Privacy Laws, Customer is the "service recipient," "controller," "business," or any similar term provided under Privacy Laws, and Vendor is the "service provider," "processor," "contractor," or any similar term provided under Privacy Laws.

4. **Details of Processing.** The Parties agree that the details of processing are as described in **Annex 1** attached hereto.

5. **Customer Obligations.** Customer shall comply with all Privacy Laws in providing Personal Data to Vendor in connection with the Services. Customer represents and warrants that: (a) the Privacy Laws applicable to Customer do not prevent Vendor from fulfilling the instructions received from Customer and performing Vendor's obligations under this DPA; (b) all Personal Data was collected and at all times processed and maintained by or on behalf of Customer in compliance with all Privacy Laws, including with respect to any obligations to provide notice to and/or obtain consent from individuals; and (c) Customer has a lawful basis for disclosing the Personal Data to Vendor and enabling Vendor to process the Personal Data as set out in this DPA. Customer shall notify Vendor without undue delay if Customer makes a determination that the processing of Personal Data under the Agreement does not or will not comply with Privacy Laws, in which case, Vendor shall not be required to continue processing such Personal Data.

6. Processing of Personal Data.

a. Customer retains ownership of all Personal Data processed under this DPA.

b. Vendor shall only process Personal Data (i) to perform the Services as further described in **Annex 1**, and in accordance with and for the purposes set out in the documented instructions from Customer from time to time, (ii) to develop, improve and enhance the Services, provided that such processing is limited to deidentified, aggregated or anonymized data; (iii) for compliance with legal obligations applicable to Vendor; and (iv) as otherwise instructed by Customer in writing.

c. Vendor shall notify Customer without undue delay if it makes a determination that it can no longer meet its obligations under applicable Privacy Laws or cannot comply with any instruction from Customer with respect to the use of Personal Data;

d. to the extent required by Privacy Laws, and upon reasonable written notice that Customer reasonably believes Vendor is using Personal Data in violation of Privacy Laws or this DPA, Vendor shall grant Customer the right to take reasonable and appropriate steps to help ensure that Vendor uses the Personal Data in a manner consistent with Customer's obligations under Privacy Laws, and stop and remediate any unauthorized use of the Personal Data; and

e. Vendor shall require that each employee or other person processing Personal Data is subject to an appropriate duty of confidentiality with respect to such Personal Data in accordance with the provisions of this Agreement.

7. **Prohibitions.** To the extent required by applicable Privacy Laws, Vendor is prohibited from:

a. selling the Personal Data, except in deidentified, aggregated or anonymized form;

b. sharing the Personal Data for cross-context behavioral advertising purposes, except in deidentified, aggregated or anonymized form;

c. retaining, using, or disclosing the Personal Data for any purpose other than (i) for the specific purpose of performing the Services, (ii) to develop, improve, or enhance the Services through the use of deidentified, aggregated or anonymized data, or (iii) as as otherwise permitted under Privacy Laws;

d. retaining, using, or disclosing the Personal Data outside of the direct business relationship between Vendor and Customer, except as described above; and

e. combining the Personal Data received from, or on behalf of, Customer with any Personal Data that may be collected from Vendor's separate interactions with the individual(s) to whom the Personal Data relates or from any other sources, except to perform a business purpose or as otherwise permitted by Privacy Laws.

8. **Use of Subcontractors.** To the extent Vendor engages any subcontractors to process Personal Data on its behalf:

a. Customer hereby grants Vendor general written authorization to engage the subcontractors set out in **Annex 2**, subject to the requirements of this Section 8.

b. If Vendor appoints a new subcontractor or intends to make any changes concerning the addition or replacement of any subcontractor, it shall provide Customer with thirty (30) business days' prior written notice by posting updates to our Privacy Policy, during which Customer can object to the appointment or replacement on reasonable and documented grounds related to the confidentiality or security of Personal Data or the subcontractor's compliance with Privacy Laws (and if Customer does not so object, Vendor may proceed with the appointment or replacement). In urgent circumstances requiring immediate subprocessor changes (e.g., security incidents, service disruptions), Vendor may proceed with changes and provide notice within ten (10) business days thereafter.

c. Vendor shall engage subcontractors only pursuant to a written agreement that contains obligations on the subcontractor which are no less onerous on the relevant subcontractor than the obligations on Vendor under this DPA.

9. **Assistance.** To the extent required by Privacy Laws, and taking into account the nature of the processing, Vendor shall, in relation to the processing of Personal Data and to enable Customer to

comply with its obligations which arise as a result thereof, provide reasonable assistance to Customer, through appropriate technical and organizational measures, in:

a. responding to requests from individuals pursuant to their rights under Privacy Laws, including by providing, deleting or correcting the relevant Personal Data, or by enabling Customer to do the same, insofar as this is possible;

b. implementing reasonable security procedures and practices appropriate to the nature of the Personal Data to protect the Personal Data from unauthorized or illegal access, destruction, use, modification, or disclosure;

c. notifying relevant competent authorities and/or affected individuals of Personal Data breaches;

d. conducting data protection impact assessments and, if required, prior consultation with relevant competent authorities; and

e. entering into this DPA.

10. **Security Measures.** Vendor shall, taking into account the state-of-the-art, the costs of implementation and the nature, scope, context and purpose of the processing, implement, and ensure that its authorized personnel comply with, appropriate technical and organizational measures designed to provide a level of security appropriate to the risk, as set out in **Annex 3**, or otherwise agreed and documented between Customer and Vendor from time to time. To the extent required by Privacy Laws, Vendor shall without undue delay, and in any event within seventy-two (72) hours, notify Customer in writing of any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data, with further information about the breach provided in phases as more details become available.

11. **Access and Audits.** Upon reasonable request of Customer, Vendor shall make available to Customer such information in its possession as is reasonably necessary to demonstrate Vendor's compliance with its obligations under this DPA, and allow for and contribute to audits, including inspections, conducted by Customer or another auditor mandated by Customer and reasonably accepted by Vendor, at Customer's sole expense unless a material violation is discovered. Customer shall be permitted to conduct such an assessment no more than once every twelve (12) months, upon thirty (30) days' advance written notice to Vendor, and only after the Parties come to agreement on the scope of the audit and the auditor is bound by a duty of confidentiality. As an alternative to an audit performed by or at the direction of Customer, to the extent permitted by Privacy Laws, Vendor may arrange for a qualified and independent auditor to conduct, at Vendor's expense, an assessment of Vendor's policies and technical and organizational measures in support of its obligations under Privacy Laws using an appropriate and accepted control standard or framework and assessment procedure for such assessment, and will provide a report of such assessment to Customer upon reasonable request. Notwithstanding the foregoing, in no event shall Vendor be required to give Customer access to information, facilities or systems to the extent doing so would cause Vendor to be in violation of confidentiality obligations owed to other customers or its legal obligations.

12. **Deletion of Personal Data.** At Customer's written direction, Vendor shall delete or return all Personal Data to Customer as requested at the end of the provision of the Services, unless retention of the Personal Data is required by law.

13. **Data Transfers.** To the extent Vendor processes Personal Data subject to EU/UK Privacy Laws in a Third Country, and it is acting as data importer, Vendor shall comply with the data importer's obligations and Customer shall comply with the data exporter's obligations set out in the Controller

to Processor Clauses, which are hereby incorporated into and form part of this DPA, and:

a. for the purposes of Annex I or Part 1 (as relevant) of such Controller to Processor Clauses, Customer is a controller and Vendor is a processor, and the parties, contact person's details and processing details set out in the Agreement, this DPA and **Annex 1** shall apply and the Start Date is the effective date of the Agreement, and the signature(s) (in any form) given in connection with the execution of this Agreement by a party and the dates of such signature(s) shall apply as the dated signature required from that party;

b. if applicable, for the purposes of Part 1 of the UK Addendum, the relevant Addendum EU SCCs (as such term is defined in the UK Addendum) are the EU SCCs as incorporated into this DPA by virtue of this Section 13;

c. for the purposes of Annex II or Part 1 (as relevant) of such Controller to Processor Clauses, the technical and organizational security measures, and the technical and organizational measures taken by Vendor to assist Customer, as each are set out in **Annex 3**, shall apply; and

d. if applicable, for the purposes of Annex III or Part 1 (as relevant) of such Controller to Processor Clauses, the list of authorized sub-contractors set out in Schedule 4 (Authorized Sub-contractors) shall apply; and

e. if applicable, for the purposes of: (i) Clause 9, Option 2 ("General written authorization") is deemed to be selected and the notice period specified in Section 8 shall apply; (ii) Clause 11(a), the optional wording in relation to independent dispute resolution is deemed to be omitted; (iii) Clause 13 and Annex I.C, the competent supervisory authority shall be the Ireland Data Protection Commission; (iv) Clauses 17 and 18, Option 1 is deemed to be selected and the governing law and the competent courts shall be The Republic of Ireland; (vi) Part 1, Vendor as importer may terminate the UK Addendum pursuant to Section 19 of such UK Addendum.

Additionally, Vendor may rely on an adequacy decision, the EU-US Data Privacy Framework, derogations for specific situations under Privacy Laws, or any other lawful mechanism for data transfers to ensure compliance with Privacy Laws.

Any disputes regarding cross-border transfers or compliance with applicable Privacy Laws related to such transfers shall be resolved in accordance with the governing law and jurisdiction specified in the Agreement.

Customer acknowledges and agrees that Vendor may appoint an affiliate or third-party subcontractor to process the Personal Data in a Third Country, in which case, Vendor shall execute the Processor to Processor Clauses with any relevant subcontractor (including affiliates) it appoints on behalf of Customer.

14. **Limitation of Liability.**

a. Vendor shall not be liable for any indirect, consequential, incidental, special, exemplary, or punitive damages, or for loss of profits, revenue, data, or business opportunities, even if Vendor has been advised of the possibility of such damages. To the fullest extent permitted by law, Vendor's total aggregate liability arising out of or in connection with this DPA, whether in contract, tort (including negligence), breach of statutory duty, or otherwise, shall not exceed the total fees paid or payable by Customer to Vendor for the Services under the Agreement in the twelve (12) months immediately preceding the date of the event giving rise to the claim.

b. Exclusions from Liability Cap. The limitations of liability set forth in Section 14(a) shall not apply to:

i. Vendor’s gross negligence, willful misconduct, or fraud;

ii. Vendor’s liability for death or personal injury caused by its negligence; or

iii. Any liability that cannot be lawfully limited under applicable Privacy Laws.

c. Data Breaches. In the event of a data breach caused by Vendor’s breach of this DPA or Privacy Laws, Vendor’s liability shall be limited to the reasonable and direct costs incurred by Customer in responding to the breach, subject to the aggregate liability cap in Section 14.1.

d. Exclusive Remedies. The remedies set forth in this DPA are Customer’s sole and exclusive remedies with respect to any claim arising out of Vendor’s processing of Personal Data or compliance with this DPA.

e. Limitation on Claims. No action or proceeding arising under or in connection with this DPA may be brought by Customer more than one (1) year after the occurrence of the event giving rise to the claim, except where prohibited by law.

ANNEX 1

Details of Processing

1. Nature of the processing

- Access, use, disclosure, storage, deletion and/ or other processing of Personal Data by Vendor in connection with providing Vendor's Services to Customer as set out in the Agreement.

2. Purpose(s) of the processing

- Providing the Services by Vendor to Customer as set out in the Agreement.

3. Categories of individuals whose Personal Data is processed

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

4. Categories of Personal Data processed

- 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

5. Types of Personal Data subject to the processing that are considered "sensitive" or "special category" under Privacy Laws

- Customer, and/or its personnel shall not provide any sensitive or special category data under this Agreement, and Vendor is not liable for processing sensitive data provided by Customer. Vendor does not intentionally collect or Process any special categories of Personal Data.

6. Frequency (e.g. one-off or continuous) and duration of the processing

- Relevant Personal Data is processed on a continuous basis, for the duration of the term of the Agreement and any post-termination retention period as set out in the Agreement.

7. The subject matter, nature and duration of processing carried out by any sub-processors authorized pursuant to Section 8

- As set out in this **Annex 1** and in **Annex 2**.

ANNEX 2

Authorized Sub-Processors

Supabase, Inc.	Authentication Provider	USA
Anthropic PBC	AI Features / Natural Language Processing	USA
Cerebras Systems Inc.	Natural Language Processing	USA
OpenAI Inc.	Natural Language Processing	USA
OpenPipe Inc.	Natural Language Processing	USA
Cloudflare, Inc.	Cloud Infrastructure	USA
Fireworks AI, Inc.	Cloud Infrastructure	USA
Google LLC	Cloud Infrastructure, Natural Language Processing, AI Features, Firebase	USA
Foundry Technologies, Inc. (Mithril.ai)	Cloud Infrastructure	USA
Vercel Inc.	Cloud Infrastructure	USA
BaseTen Labs, Inc.	Cloud Infrastructure	USA
Modal Labs, Inc.	Cloud Infrastructure	USA
Amazon Web Services, Inc.	Cloud Infrastructure	USA
Redis Inc.	Data Caching	USA
Functional Software, Inc. (Sentry)	Error Management	USA
Clickhouse, Inc.	Site and Product Analytics	USA
Segment.io, Inc.	Site and Product Analytics	USA
PostHog, Inc.	Site and Product Analytics	USA
Metabase, Inc.	Site and Product Analytics	USA
Dub Technologies, Inc.	Site and Product Analytics	USA
HEX Technologies, Inc.	Site and Product Analytics	USA
Slack Technologies, LLC	Customer Support	USA
Peaberry Software, Inc. (CustomerIO)	Email Marketing	USA
Eleven Labs Inc.	Text-to-Speech	USA
Pylon Labs Inc.	Customer Support	USA

Baremetrics Inc.	Revenue Analytics	USA
RevenueCat Inc.	Payment Processing	USA
Apple Inc.	Payment Processing	USA
Attio Inc.	Customer Relationship Management	USA
Enterpret Inc.	Customer Insights & Analytics	USA
Twilio Inc.	SMS Messaging	USA
Better Stack, Inc. (Logtail)	Logging & Observability	USA
WorkOS, Inc.	Enterprise SSO & Directory Sync	USA
Stripe, Inc.	Payment Processing	USA

ANNEX 3

Technical and Organizational Measures

This Annex 3 sets forth the following technical and organizational security measures implemented by Wispr AI, Inc. ("Wispr") under the Data Processing Agreement ("DPA"):

1. **Access Control:** Access to personal data is restricted to authorized personnel only, with role-based access controls and strong authentication mechanisms such as multi-factor authentication (MFA) to help secure access.
2. **Employee Training and Awareness:** Employees undergo regular training on data protection, privacy, and security best practices.
3. **Data Encryption:** Wispr employs industry-standard encryption protocols to ensure that personal data is encrypted at rest and in transit. Encryption keys are managed securely and are regularly rotated.
4. **Network Security:** Network security is maintained through the deployment of firewalls, intrusion detection, and prevention systems (IDPS), and regular vulnerability assessments and penetration testing are conducted.
5. **Application Security:** Secure software development practices, including code reviews and security testing, are followed, and web application firewalls (WAF) are used to protect against common web exploits.
6. **Data Backup and Recovery:** Regular backups of personal data are performed and stored securely, with disaster recovery and business continuity plans in place and tested periodically.
7. **Data Center Security:** Data centers are protected by physical security controls, including access controls, surveillance systems, and security personnel. Access to data centers is restricted to authorized personnel only.
8. **Office Security:** Office premises are secured with access controls, alarm systems, and surveillance cameras, and visitors are required to sign in and are escorted by authorized personnel.
9. **Security Monitoring:** Wispr conducts continuous monitoring of systems and networks to detect and respond to security incidents. Security information and event management (SIEM) systems are used to correlate and analyze security events.
10. **Incident Response:** An incident response plan is in place to handle security incidents promptly and effectively, and data breach notification procedures comply with applicable laws and regulations.
11. **Privacy by Design:** Data protection principles are integrated into the design and development of systems and processes through the implementation of Privacy by Design. Regular privacy impact assessments are conducted to identify and mitigate risks.
12. **Data Minimization:** Personal data collection and processing are limited to what is necessary for the specified purposes, and data anonymization and pseudonymization techniques are used where appropriate.
13. **Continuous Monitoring and Improvement**: Wispr continuously monitors its data privacy and security policies, implementing improvements and updates as needed to ensure the highest level of protection for our users' data. We strive to stay at the forefront of industry best practices and evolving legal requirements to maintain the trust and confidence of our clients.

By implementing these measures, Wispr is dedicated to upholding high standards of data privacy and security, enabling our users to benefit from the Services.