DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**Addendum**") entered into by and between the Customer (as defined in the Agreement) and Krisp Technologies, Inc. ("**Krisp**"), supplements the Krisp Master Subscription Agreement available at https://krisp.ai/master-subscription-agreement/, as updated from time to time, or other written agreement between Customer and Krisp, governing Customer's use of the Services ("**Agreement**"). Any terms not defined in this Addendum shall have the meaning set forth in the Agreement. In the event of a conflict between the terms and conditions of this Addendum and the Agreement, the terms of this Addendum shall supersede and control. Customer and Krisp are hereinafter jointly referred to as the "**Parties**", and each of the Parties individually also as a "**Party**".

Recitals

In the course of its business activities and under the Agreement, Krisp may receive from Customer access to certain Personal Data collected and/or controlled by Customer, which Krisp shall Process pursuant to the Instructions provided in writing by Customer. This Addendum is concluded in order to ensure that Customer and Krisp may meet their respective data protection obligations with respect to the Commissioned Processing under Data Protection Legislation. The Parties shall ensure that they Process any and all Personal Data subject hereto solely for the purposes contemplated in the Agreement, or as otherwise agreed to in writing by the Parties, including pursuant to Customer's written Instructions, and in compliance with the terms hereof. This Addendum also applies where the Customer is itself acting as a "Processor" or "Service Provider" on behalf of one or more of its clients and in that case Krisp will, respectively, act as a data "Sub-Processor" under the GDPR or as a "Sub-Service Provider" (under the California Consumer Privacy Act and California Privacy Rights Act (together "**CCPA**"). Customer's clients act as a "Data Controller" under the GDPR and a "Business" under the CCPA.

1. Definitions.

1.1. The following definitions shall apply in this Addendum:

a) **"Authorized Subprocessor"** means a third-party who has a need to know or otherwise access Personal Data to enable Krisp to perform its obligations under this DPA or the Agreement, and who is authorized under Section 5.2 of this DPA.

b) "**Commissioned Processing**" means Processing of Personal Data that is carried out by Krisp on behalf of Customer, in accordance with the Agreement, Instructions of Customer and the terms of this Addendum.

c) "**Data Protection Legislation**" means (i) all laws and regulations applicable to the Processing of Personal Data, including those of the EU, the EEA and their member states, Switzerland, the United Kingdom, the United States and its states, and (ii) any judicial or administrative interpretation of any of the above, any guidance, guidelines, codes of practice, or approved certification mechanisms issued by any relevant supervisory authority and binding under applicable law.

d) "**Data Subject**" means an identified or identifiable person to whom Personal Data relates, including as may be defined in applicable Data Protection Legislation.

e) "**EU**" and "**EEA**" shall respectively mean the European Union and the European Economic Area.

f) "**GDPR**" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), including as implemented or adopted under the laws of the United Kingdom.

g) "**Instruction(s)**" means directions, either in writing (including by e-mail) or by using a software or online tool that logs or generates written records, issued by Customer (acting as either controller or processor) to Krisp and directing Krisp to Process Personal Data. Oral directions shall not constitute Instructions hereunder.

h) "**Personal Data**" means any personal data, as such term and similar terms (including personal information) are defined under applicable Data Protection Legislation, which Krisp may Process on behalf of Customer for the purposes of providing the Services.

i) "**Process**" or "**Processing**" means any operation or set of operations performed upon the Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction.

j) "**Security and Fraud Prevention**" shall mean any and all measures taken by Krisp with respect to Personal Data in order to ensure its security and prevent any fraud in connection therewith.

k) "**Security Incident**" means the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data, transmitted, stored, or otherwise Processed by Krisp or its Subprocessors.

l) "**Services"** means the services performed by Krisp and identified in the Agreement.

m) "**Standard Contractual Clauses**" or "**SCCs**" means the model clauses for the transfer of Personal Data to third countries pursuant to GDPR, approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, as currently set out at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj.

n) "**U.S. State Privacy Laws**" means the CCPA and any regulations promulgated thereunder; the Colorado Privacy Act of 2021; the Virginia Consumer Data Protection Act of 2021; the Utah Consumer Privacy Act of 2022, as amended; the Connecticut Data Privacy Act of 2022, and any other US state law that may be enacted that adheres to the same or substantially the same requirements of the aforementioned laws in this definition.

o) "**UK Addendum**" means the SCCs as amended by the International Data Transfer Addendum, Version B1.0 (21 March 2022) issued under S1198A(1) Data Protection Act 2018, as currently set out at https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf.

1.2. All other terms used in this Addendum shall have the meanings given to them in the Agreement.

2. Details of Processing.

2.1. This Addendum applies when Personal Data is Processed by Krisp. In this context, Krisp will act as processor to Customer, who may act either as controller or as processor of Personal Data on behalf of a third-party controller. Where Customer is a processor, Customer warrants that (i) it has obtained all necessary authorizations from the relevant data controller to appoint Krisp as a sub-processor, and (ii) it has imposed data protection obligations on the relevant data controller that are at least as protective as those set out in this Addendum.

2.2. The subject matter, nature, purpose, and duration of the Processing, as well as the types of Personal Data collected and categories of Data Subjects, are described in Exhibit A to this Addendum.

2.3. The Commissioned Processing of the Personal Data by Krisp is solely carried out within the framework of the Agreement, this Addendum and the specific individual Instructions provided by Customer. Krisp shall comply with all documented Instructions regarding the type, extent and procedure of Commissioned Processing; provided, however, that if any Instructions (or Processing thereunder) may cause Krisp to breach its obligations under Data Protection Legislation, Krisp shall promptly notify Customer in writing as set forth in Section 4.3 hereof.

2.4. Krisp shall not use the Personal Data for any purposes other than to perform the Services. Notwithstanding the foregoing, Krisp may use Personal Data, including Services usage data solely in an anonymized (or de-identified) and aggregated form, such that the data no longer constitutes Personal Data under applicable Data Protection Legislation, solely for (i) internal purposes of developing anonymized and aggregated Services usage and performance metrics for reporting or statistical purposes, (ii) Security and Fraud Prevention, and/or (iii) compliance with Krisp's legal and regulatory obligations, in any event only to the extent permitted under applicable Data Protection Legislation.

2.5. Where Krisp Processes Personal Information (as defined under applicable U.S. State Privacy Laws) subject to U.S. state consumer privacy laws, the terms of Schedule B (U.S. State Privacy Law Addendum) shall apply.

3. Obligations of Customer.

Customer is solely responsible for (i) the accuracy, quality, and legality of the Personal Data provided to Krisp by (or on behalf) of Customer, (ii) the means by which Customer acquires any such Personal Data, including establishing all required legal bases (and obtaining and recording consent where consent is required) for the Processing contemplated hereunder, (iii) informing Data Subjects of the Processing of their Personal Data by Krisp (as applicable), and (iv) the Instructions it provides to Krisp regarding the Processing of such Personal Data. Customer shall not provide or make available to Krisp any Personal Data in violation of the Agreement, this Addendum or Data Protection Legislation, or that is otherwise inappropriate for the nature of the Services to be provided by Krisp, and shall promptly notify Krisp where Personal Data that is Processed by Krisp must no longer be Processed by reason of a Data Subject's request for deletion or withdrawal of consent, or any other legally valid obligation under Data Protection Legislation that mandates the cessation of Processing by Krisp. If Customer is itself a processor, Customer warrants to Krisp that: (i) Customer has been duly authorized by the relevant data controller to appoint Krisp as a sub-processor; (ii) Customer has entered into a binding agreement with the relevant data controller that complies with Data Protection Legislation, including Article 28 of the GDPR; and (iii) Customer shall pass on relevant instructions and information from the relevant data controller to Krisp in a timely manner.

4. Obligations of Krisp.

4.1. Unless otherwise requested by Customer, upon termination or expiration of the Agreement, Krisp shall immediately cease Processing Personal Data and securely destroy all Personal Data in Krisp's possession, custody or control, including copies thereof. Further, at any time upon Customer's written request, Krisp shall promptly delete a particular individual's Personal Data from Krisp's records unless it is required to retain such Personal Data under Data Protection Legislation. Krisp will certify to Customer that Personal Data have been securely destroyed or returned if previously requested by Customer.

4.2. Krisp shall ensure that all of its employees who have a need to know or otherwise access Personal Data to enable Krisp to perform its obligations under this Addendum or the Agreement are made aware of the confidential nature of Personal Data and have executed confidentiality agreements that prevent them from disclosing or otherwise Processing, both during and after their engagement with Krisp, any Personal Data except in accordance with their obligations in connection with the Services.

4.3. To the extent that Customer provides or materially modifies the Instructions within the framework of the Agreement such that Krisp is not able to comply with such Instructions or modifications without incurring material additional costs, Krisp shall: (i) immediately inform Customer and provide sufficient information to enable Customer to determine a possible resolution; and (ii) cease all Processing of the affected Personal Data (other than securely storing such Personal Data) until revised Instructions are received and accepted in writing by Krisp. The Parties agree that any material changes to Customer's Instructions that affect the pricing structure or commercial relationship of the Parties must be addressed under the Agreement or supplemental written instrument agreed upon by both Parties.

4.4. When acting as a sub-processor, Krisp shall (i) comply with the obligations set forth in Article 28(3) of the GDPR (or equivalent obligations under applicable Data Protection Legislation); (ii) provide reasonable assistance to Customer in enabling the relevant data controller to comply with its obligations under applicable Data Protection Legislation; and (iii) forward any requests, complaints, or other communications from the relevant data controller to Customer without undue delay.

5. Authorized Subprocessors

5.1. Customer acknowledges and agrees that Krisp may (1) engage its affiliates and Authorized Subprocessors referenced in Section 5.2 below to access and process Personal Data in connection with the Services and (2) from time to time engage additional third parties for the purpose of providing the Services, including without limitation the processing of Personal Data. By way of this DPA, Customer provides general written authorization to Krisp to engage subprocessors as necessary to perform the Services.

5.2. A list of Krisp's current Authorized Subprocessors is currently available at https://trust.krisp.ai/subprocessors or such other URL as Krisp may designate (the "**Subprocessor List**"). The Subprocessor List may be updated by Krisp from time to time. Krisp may provide a mechanism to subscribe to notifications of new Authorized Subprocessors and Customer agrees to subscribe to such notifications where available. At least fifteen (15) days before enabling any third party other than existing Authorized Subprocessors to access or participate in the processing of Personal Data, Krisp will add such third party to the Subprocessir List and notify Customer. Customer may object to such an engagement by informing Krisp within fifteen (15) days of receipt of the aforementioned notice to Customer, provided such objection is in writing and based on reasonable grounds relating to data protection. Customer acknowledges that certain subprocessors are essential to providing the Services and that objecting to the use of a subprocessor may prevent Krisp from offering the Services to Customer.

5.3. If Customer reasonably objects to an engagement in accordance with Section 5.2, and Krisp cannot provide a commercially reasonable alternative within a reasonable period of time, Customer may discontinue the use of the affected Service by providing written notice to Krisp. Discontinuation shall not relieve Customer of any fees owed to Krisp under the Agreement.

5.4. If Customer does not object to the engagement of a third party in accordance with Section 5.2 within fifteen (15) days of notice by Krisp, that third party will be deemed an Authorized Subprocessor for the purposes of this DPA.

5.5. If Customer and Krisp have entered into Standard Contractual Clauses as described in Section 7 (Transfers of Personal Data), (i) the above authorizations will constitute Customer's prior written consent to the subcontracting by Krisp of the processing of Personal Data if such consent is required under the Standard Contractual Clauses, and (ii) the parties agree that the copies of the agreements with Authorized Subprocessors that must be provided by Krisp to Customer pursuant to Clause 9(c) of the EU SCCs may have commercial information, or information unrelated to the Standard Contractual Clauses or their equivalent, removed by Krisp beforehand, and that such copies will be provided by Krisp only upon request by Customer.

6. Security Incident Management and Notification.

6.1. If Krisp becomes aware of a Security Incident, Krisp will promptly and without undue delay, but in any case, within 48 hours of discovery of Security Incident (i) notify Customer of the Security Incident; (ii) investigate the Security Incident and provide Customer with detailed information about the Security Incident; (iii) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident. The obligations herein shall not apply to incidents that are caused by Customer.

6.2. Notification(s) of Security Incidents will be delivered to Customer by any means Krisp selects, including via email. It is Customer's sole responsibility to ensure Customer maintains accurate contact information with Krisp for the Services. Customer is solely responsible for complying with its obligations under Data Processing Legislation applicable to Customer and fulfilling any third-party notification obligations related to any Security Incident. Without limiting the generality of the foregoing, Krisp shall make reasonable efforts to assist Customer in fulfilling Customer's obligation under applicable Data Protection Legislation to notify the relevant supervisory authority and data subjects about such Security Incident.

6.3. Krisp's notification of or response to a Security Incident under this section is not an acknowledgement by Krisp of any fault or liability with respect to the Security Incident.

6.4. Customer must notify Krisp promptly about any possible misuse of its accounts or authentication credentials or any Security Incident related to the Services.

7. <u>Transfers of Personal Data.</u>

7.1. To protect transfers of Personal Data out of the EU/EEA and its member states, the United Kingdom, and/or Switzerland, Customer authorizes Krisp to make international transfers of the Personal Data in accordance with Standard Contractual Clauses and the UK Addendum, as appropriate. By entering into this Addendum, the parties are deemed to be signing the Standard Contractual Clauses and the UK Addendum.

7.2. To the extent required under the GDPR, the Standard Contractual Clauses form part of this Addendum and take precedence over the rest of this Addendum for such transfer to the extent of any conflict, and they will be deemed completed as follows:

a) Where Customer is acting as a controller, Module 2 (Controller to Processor) of the SCCs applies. Where Customer is acting as a processor on behalf of a third-party controller, Module 3 (Processor to Processor) of the SCCs applies.

b) Clause 7 (the optional docking clause) does not apply unless expressly agreed by the Parties in writing.

c) If the Customer wishes to exercise its rights under Clause 8.9 (Documentation and compliance), applicable under either Module 2 or Module 3, depending on the role of Customer, the Customer shall first request a copy of the annual third-party audit report of Krisp's facilities and data processing ("Audit Report") subject to any reasonable confidentiality assurances (up to and including a non-disclosure agreement) that Krisp may seek. It is only where Customer reasonably considers that the Audit Report does not provide Customer with reasonable reassurances about Krisp's compliance with the SCCs that Customer shall request to conduct an audit by itself or mandate an independent auditor as permitted under Clause 8.9.

d) Audits in accordance with Clause 8.9 (Documentation and compliance) shall: (i) be on no less than ten (10) working days' prior written notice to Krisp (ii) be conducted during normal business hours; (iii) not unreasonably interfere with Krisp's business activities; (iv) be limited to once a calendar year unless required by law; (v) be subject to Krisp's reasonable security restrictions (e.g., sign-in requirements, badge requirements, escort requirements); (vi) be subject to a non-disclosure agreement between the auditor and Krisp, where requested by Krisp; and (vii) be at Customer's cost (including reimbursing Krisp for its reasonable costs associated with the audit) unless the parties agree otherwise.

e) Under Clause 9 (Use of subprocessors), the parties select Option 2 (General written authorization).

f) Under Clause 11 (Redress), the optional requirement that data subjects be permitted to lodge a complaint with an independent dispute resolution body does not apply.

g) Under Clause 17 (Governing law), the parties choose Option 1 (the law of an EU Member State that allows for third-party beneficiary rights). The parties select the law of Ireland.

h) Under Clause 18 (Choice of forum and jurisdiction), the parties select the courts of Ireland.

i) Annexes I and II of the Standard Contractual Clauses are set forth in Schedule A of this Addendum. Annex III of the Standard Contractual Clauses is set forth in Section 5.2 of this Addendum.

j) Any assistance provided by Krisp to Controller under Clause 8.6 (Security of processing), Clause 8.9 (Documentation and compliance) and Clause 10 (Data Subject Rights) shall be at Customer's sole cost and expense except for those circumstances where Krisp is not complying with its obligations under the Standard Contractual Clauses.

7.3. To the extent required under Data Protection Legislation of the United Kingdom, the UK Addendum forms part of this Addendum and takes precedence over the rest of this Addendum for such transfer to the extent of any conflict, and the annex information for the UK SCCs shall be the same as that for the EU SCCs save that English law shall apply, English courts shall be the relevant forum and the competent authority shall be the Information Commissioner's Office.

7.4. To the extent required under Data Protection Legislation of Switzerland, the Standard Contractual Clauses form part of this Addendum and take precedence over the rest of this Addendum for such transfer to the extent of any conflict, and they will be deemed completed in accordance with Section 7.2 above, except that:

a) Switzerland's Federal Data Protection and Information Commissioner shall be the competent supervisory authority in accordance with Clause 13 of the Standard Contractual Clauses to the extent the transfer is governed by the Swiss Federal Act on Data Protection.

b) References to "Member State" refer to Switzerland, and data subjects may exercise and enforce their rights under the SCCs in Switzerland.

c) References to GDPR refer to the Swiss Federal Act on Data Protection (as amended and replaced).

d) The term "data subjects" shall be interpreted as including data subjects in Switzerland.

e) Data subjects with their regular place of residence in Switzerland may bring a lawsuit in Switzerland against either the data exporter or the data importer in accordance with Clause 18(c) of the SCCs.

8. Final Provisions.

8.1. If one or more stipulations of this Addendum are deemed void, this shall not affect validity of the other stipulations of this Addendum. In the event of invalidity of one or more stipulations of this Addendum, the Parties shall negotiate a legally effective provision commercially close to the invalid stipulation. The same shall apply in the event of a regulatory gap. In case a change in applicable law makes an amendment of this Addendum necessary, the Parties shall discuss and agree such required change in good faith.

8.2. Without prejudice to any requirements under the GDPR, or clauses 17 (Governing Law) and 18 (Choice of Forum and Jurisdiction) of the Standard Contractual Clause Agreement, the Parties hereby submit to the choice of venue and jurisdiction stipulated in the Agreement with respect to any disputes or claims howsoever arising under this Addendum, including disputes regarding its existence, validity or termination or the consequences of its nullity; provided, however, that the Parties agree that this Addendum shall be governed by the laws of the State of California, without reference to its choice of law rules.

8.3. The total liability of each of Customer and Krisp (and their respective employees, directors, officers, affiliates, successors, and assigns) towards each other, arising out of or related to this Addendum, the SCCs, the UK Addendum, the U.S. State Privacy Law Addendum, and any other data protection agreements or security addenda signed by the parties in connection with the Agreement (if any), whether in contract, tort, or other theory of liability, shall not, when taken together in the aggregate, exceed the limitation of liability for aggregate or direct damages set forth in the Agreement.

krisp

SCHEDULE A

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

Name: Purchaser - as listed in the Agreement
Address: as listed in the Agreement
Contact person's name, position and contact details: as listed in the Agreement
Activities relevant to the data transferred under this Addendum: as listed in the Agreement
Signature and date: Please refer to the signature and date of the Agreement.
Role: Controller or processor

Data importer(s):

Name: Krisp Technologies, Inc.
Address: 2150 Shattuck Ave, Penthouse 1300, Berkeley, CA 94704, USA
Contact person's name, position and contact details:
Name: as listed in the Agreement
Position: as listed in the Agreement
Email: dpo@krisp.ai
Activities relevant to the data transferred under this Addendum: as listed in the Agreement
Signature and date: Please refer to the signature and date of the Agreement.
Role: Processor or sub-processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

- End users authorized by Customer to use the Services; and
- Other categories of data subjects whose personal information may be shared with the data importer for the purposes of providing the Services.

Categories of personal data transferred

Personal Data uploaded to the Services, which may include the following:

- Contact information, such as business email address;
- Localization data;
- Analytics data;
- Audio data containing the voice and speech content of data subjects, processed transiently for real-time AI-powered voice translation, if applicable;
- System log data; and
- other Personal Data contained in business related communications and interactions.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

Not applicable (except for AI Voice Translation). For AI Voice Translation, Krisp does not intentionally collect or require sensitive personal data. However, such information may be incidentally included in a user's speech during real-time translation. All audio data is processed in transit only, is not stored or retained by Krisp unless instructed by

Customer, and is immediately discarded once the translation is completed. Processing is fully automated, encrypted in transit, and no human access or review occurs.

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

The Personal Data is transferred on a continuous basis.

Nature of the processing

The Personal Data (except the Personal Data processed through the Krisp AI Voice Translation service) processed may be subject to the following processing activities: collect, record, organize, store, adapt, alter, retrieve, redact, and consult**.** The Personal Data processed through the Krisp AI Voice Translation service is subject to limited, real-time processing activities necessary to provide translation functionality. Specifically, Personal Data (such as speech audio) is collected and transmitted in real time, temporarily processed to enable transcription and translation, and immediately discarded once the translated output is delivered. No Personal Data is stored unless instructed by Customer, indexed, profiled, or analyzed after processing.

Purpose(s) of the data transfer and further processing

Processing of Personal Data for the purposes described in 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

The Personal Data may be processed during the Term of the Agreement, unless otherwise agreed upon in writing or required by applicable Data Protection Legislation.

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

The subject matter, nature and duration of the processing are set forth in Section 5 of the DPA.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

Supervisory authority of the EU Member State as identified in Clause 13 based on the Data Exporter’s place of establishment respective to the EU.

krisp

ANNEX II

DESCRIPTION OF THE TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES IMPLEMENTED BY THE DATA IMPORTER IN ACCORDANCE WITH THE STANDARD CONTRACTUAL CLAUSES

A. RELEVANT CERTIFICATIONS

SOC 2 Type II Report for Service Organizations: Trust Services Criteria

Krisp has undergone a SOC 2 for Service Organizations: Trust Services Criteria Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy examination by an independent third party. The SOC 2 Type II Report details the management's description of Krisp's system and the suitability of the design and operating effectiveness of controls.

Krisp's SOC 2 Type II Report provides assurance to Krisp and its customers that Krisp has designed an effective system of security, availability, and confidentiality controls. It also includes a mapping of security, availability, and confidentiality trust services criteria to applicable requirements of GDPR.

PCI-DSS Compliance

Krisp ensures full compliance with the Payment Card Industry Data Security Standard (PCI-DSS) when Krisp's services involve the processing or storage of payment cardholder data. Krisp's PCI-DSS compliance has been independently validated by a qualified security assessor (QSA), and Krisp maintains an Attestation of Compliance as evidence of its adherence to these rigorous industry standards.

B. TECHNICAL AND ORGANIZATIONAL MEASURES

Krisp has organized and implemented technical and organizational measures for personal data protection to support its data protection program. The measures include the following types of controls:

Information Security Policies

Provides management direction and support for information security in accordance with business requirements, and relevant laws and regulations.

Organization of Information Security

Establishes a framework for initiating and controlling information security implementation and operations at Krisp.

Enterprise Risk Management

Defines the methodology for the assessment and treatment of risks associated with the loss of confidentiality, integrity, and availability of information, and defines the acceptable risk level.

Human Resource Security

- Ensures that all workforce members are well suited for, and understand, their roles and responsibilities.
- Ensures that potential workforce hires undergo background checks.
- Ensures that workforce members sign non-disclosure agreements and commit to acceptable use policies.
- Ensures that all workforce members are aware of, and that they fulfill, their information security responsibilities and obligations, such as adhering to Krisp's infosec policies.
- Ensures that the organization's interests are protected throughout the employment process, from pre-employment to termination.

Asset Management

- Identifies and classifies Krisp's information assets, defines and assigns appropriate responsibilities for ensuring their protection, and sets their retention schedules.
- Ensures an appropriate level of protection for information assets in accordance with their sensitivity level and importance to the organization.

- Prevents the unauthorized disclosure, modification, removal, or destruction of information stored on media.

Access Control

- Sets forth management principles governing information security and cybersecurity to secure information in any form.
- Establishes governing principles for the protection of all Krisp's information and to reduce the risk of unauthorized access to Krisp's information.
- Provides the framework for user, system and application access control and management, and user responsibilities.
- Limits access to information and information processing facilities.
- Ensures authorized user access and prevents unauthorized access to systems and services.
- Makes users accountable for safeguarding their authentication information.
- Prevents unauthorized access to systems and applications.

Cryptography

- Ensures proper and effective use of cryptography in order to protect the confidentiality, authenticity, and integrity of information.
- Provides guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively.
- Establishes procedures on proper encryption for data in motion encryption, data at rest encryption and key management.

Physical and Environmental Security

Establishes procedures for properly defining secure areas, entry, threat protection, equipment security, secure disposal, clear desk and clear screen policies, and visitor access in order to prevent (1) unauthorized physical access, damage, and interference with Krisp's information and information processing facilities; and (2) loss, damage, theft, or compromise of Krisp's assets, and interruption of its operations.

Operations Security

- Establishes procedures on the proper management of IT systems, including change management, capacity management, malware, backup, logging, monitoring, installation, vulnerabilities, and audit controls
- Ensures that information and information processing facilities are operated securely and protected from malware and loss of data.
- Ensures that security events are recorded appropriately.
- Maintains operational system integrity and avoids exploitation of technical vulnerabilities.

Communications Security

Establishes controls related to network security, network segregation, network services, transfer of information internally and externally, messaging, and more.

Information Security Incident Management

- Establishes policies to reduce the impact of security incidents to the confidentiality, integrity, and availability of Krisp's technology resources, services and information.
- Enables Krisp to provide consistent, repeatable and measurable guidance that reduces or eliminates the ambiguity and questions that would otherwise commonly appear and result in inconsistent processes.

Information Security Aspects of Business Continuity Management

- Establishes a business continuity framework and defines how Krisp should recover its IT architecture and IT services within set deadlines in the event of a disaster or other disruptive incident.
- Ensures data backup for cloud-hosted implementations.
- Maintains a business continuity plan and ensures annual technical and tabletop tests.

Compliance

Ensures Krisp's compliance with respect to the organization's internal policies and procedures and contractual obligations related to information privacy and security, and applicable privacy, information security, and data protection laws and regulations.

Other Industry Standard Security Controls

- Penetration Testing
- Vulnerability Management
- Application Architecture Security
- OAuth-based Authorization
- API Security
- Privacy by Design

C. SUPPLEMENTARY MEASURES

In addition to the personal data protection controls described above, Krisp has implemented, and maintains, the following supplementary measures based on the European Data Protection Board's nonbinding guidance.

Additional Technical Measures

- Krisp uses end-to-end encryption.
- Krisp encrypts data in transit and at rest.

Additional Contractual Measures

Transparency

- Upon request, Krisp can, based on its best efforts and to the best of its knowledge, provide information on the access to data by public authorities.
- Krisp certifies that:
  (1) it has not built, and will not purposefully build, backdoors or similar programming that public authorities could use to access its personal data or information systems;
  (2) it has not changed, and will not purposefully change, its processes in a manner that facilitates public authorities' access to data; and
  (3) national law or government policy does not require Krisp to create or maintain back doors or to facilitate access to personal data or systems or for it to be in possession or to hand over the encryption key (subject to change based on legislative developments).
- Krisp will notify the Customer if Krisp is unable to comply with the legal obligations and/or contractual commitments related to international transfers and as a result with the required standard of "essentially equivalent level of data protection."

Specific Actions

- Krisp will review the legality of any public authority's data request and, upon assessing the request, Krisp will challenge the request where legitimate lawful grounds exist for doing so and where appropriate under the circumstances.
- Similarly, Krisp will review the legality of any public authority's data request and, upon assessing the request, Krisp, where appropriate and lawful, will inform the requesting public authority of the incompatibility of the order with the safeguards contained in the Article 46 GDPR transfer tool and the resulting conflict of obligations for Krisp.

Additional Organizational Measures

Adoption and Review of Internal Policies

Krisp monitors legal and regulatory developments related to cross-border transfers of personal data outside the EU, EEA, UK, or Switzerland to ensure that the data continues to enjoy an essentially equivalent level of data protection. Krisp also regularly reviews internal policies to assess the appropriateness/effectiveness of supplementary measures and to identify and implement additional or alternative solutions when necessary. Where applicable and appropriate, Krisp will work diligently to implement any required technical, organizational, and/or contractual measures.

Organizational Methods and Data Minimization Measures

- Krisp has adopted organizational controls to comply with the accountability principle, including adoption of strict and granular data access and confidentiality policies and best practices, based on a strict need-to-know principle, monitored with regular audits and enforced through disciplinary measures may also be useful measures in a transfer context.
- Krisp also practices data minimization to only process the minimum amount of personal data necessary for providing the Services and to limit the exposure of personal data to unauthorized access.
- Krisp has adopted best practices to appropriately and timely involve and provide access to information to the data protection officer, and to the legal services on matters related to international transfers of personal data transfers.

Data Security/Privacy Standards/Best practices

Krisp has adopted strict data security and data privacy policies, based on international best practices with due regard to the state of the art, in accordance with the risk of the categories of data processed and the likelihood of attempts from public authorities to access it.

Other Organizational Measures

- Krisp has adopted, and regularly reviews, internal policies to assess the suitability of the implemented supplementary measures and to identify and implement additional or alternative solutions, when necessary, to ensure that an equivalent level of protection to that guaranteed within the EU, EEA, UK or Switzerland of the personal data transferred, is maintained.
- Krisp regularly reviews and monitors Subprocessors to ensure that they maintain appropriate technical and organizational measures, which effectively meet the GDPR requirements and protect the rights of data subjects.
- Krisp and its Subprocessors enter into a legally binding data protection agreement (DPA) to ensure that the Subprocessors are subject to the data protection obligations as set forth in Article 28 GDPR and provides sufficient guarantees to implement appropriate technical and organizational measures in a manner to satisfies that GDPR requirements. The DPA also stipulates, among other things, Krisp's rights and Subprocessor's contractual obligations.
- Krisp relies on the SCCs as its lawful transfer mechanism under Article 46 of the GDPR.
- Krisp and its subprocessors enter into legally binding Standard Contractual Clauses for personal data transfers outside of the EU, EEA, UK, or Switzerland.
- Pursuant to the SCCs, Krisp’s subprocessors have contractual obligations to implement technical and organizational measures and, where appropriate, to assist Krisp so that Krisp may assist the Customer in fulfilling its data protection obligations.

krisp

SCHEDULE B

U.S. STATE PRIVACY LAW ADDENDUM

This U.S. State Privacy Law Addendum ("**State Law Addendum**") supplements the terms of the DPA to which it is attached and sets forth certain data privacy rights and obligations in connection with U.S. State Privacy Laws. Capitalized terms used in this State Law Addendum but not otherwise defined herein have the meaning ascribed to them in the DPA or the Agreement.

1. Roles and Scope

1.1. For purposes of the U.S. State Privacy Laws, Customer is the "Business" or "Controller", or may act as a "Service Provider" or "Processor," as applicable, and Krisp is the "Service Provider" or "Processor," or may act as a "Sub-Service Provider" or "Subprocessor" as applicable.

1.2. This State Law Addendum applies to Krisp's provision of Services to Customer and governs the extent to which Krisp Processes Personal Information or Personal Data of residents of U.S. states subject to the U.S. State Privacy Laws in the course of providing the Services.

2. Krisp's Restrictions and Obligations

Krisp agrees that it shall:

2.1. Process Personal Information only on behalf of and at the direction of Customer, for the purpose of providing the Services and in accordance with the DPA and Agreement.

2.2. Not Sell or Share Personal Information as defined under the CCPA, including for behavioral advertising.

2.3. Not retain, use, or disclose Personal Information (i) for any purpose other than the specific purpose of performing the Services, or (ii) outside of the direct business relationship between Krisp and Customer, except as permitted under applicable U.S. State Privacy Laws.

2.4. Not combine Personal Information received from Customer with Personal Information collected independently or from another source, except to the extent permitted under applicable U.S. State Privacy Laws for purposes such as (i) creating anonymized or de-identified data for internal analytics, as described in Section 2.4 of the DPA, or (ii) complying with legal or regulatory obligations, provided such combination does not result in the re-identification of individuals or use of Personal Information outside the direct business relationship with Customer.

2.5. To the extent it has access to the requested Personal Information and its systems are reasonably capable of fulfilling such requests, assist Customer in responding to verifiable consumer requests within a reasonable timeframe, including (i) requests to access, delete, correct, or opt-out of the sale or sharing of Personal Information, (ii) requests to limit the use of Sensitive Personal Information under applicable U.S. State Privacy Laws, and (iii) other rights as required by applicable U.S. State Privacy Laws. Customer shall be responsible for Krisp's reasonable costs and expenses arising from such assistance, including but not limited to personnel time and system modifications, unless such assistance is required due to Krisp's non-compliance with this State Law Addendum or applicable U.S. State Privacy Laws, in which case Krisp shall bear its own costs. Krisp shall promptly notify Customer if its systems lack the functionality to fulfill a specific request, and the Parties shall cooperate in good faith to identify an alternative solution.

3. Security Measures

Krisp shall maintain reasonable administrative, technical, and physical security procedures and practices appropriate to the nature of the Personal Information, to protect it from unauthorized or illegal access, destruction, use, modification, or disclosure, in accordance with the DPA, including the technical and organizational measures described in Annex II of Schedule A, and applicable U.S. State Privacy Laws.

4. Use of Subprocessors

Customer authorizes Krisp to engage subprocessors consistent with the Authorized Subprocessors listed in Section 5 of the DPA. Krisp shall (i) enter into contracts requiring each subprocessor to adhere to the same data protection obligations as set forth in this Addendum; (ii) provide Customer with a reasonable notice of new subprocessors via a public list, email notification, or dashboard update, with a right to object on reasonable privacy-related grounds within fifteen (15) days of such notice; and (iii) remain liable for subprocessors' actions in accordance with the DPA. Where Customer is acting as a Service Provider or Processor, this Section satisfies Customer's obligation to flow down equivalent requirements to subprocessors under U.S. State Privacy Laws. Customer agrees to subscribe to Krisp's

notification mechanism for subprocessor updates, where available, and to maintain accurate contact information to receive such notices.

5. Audits and Assessments

5.1. Upon reasonable written request and no more than once annually, unless required by law or in response to a Security Incident, Krisp shall provide documentation necessary to demonstrate compliance with this State Law Addendum and applicable U.S. State Privacy Laws.

5.2. Customer may also request a copy of Krisp's most recent audit reports or certifications (e.g., SOC 2 Type II) as evidence of appropriate data protection practices. Any audit reports or certifications provided by Krisp shall be subject to a non-disclosure agreement between Krisp and Customer to protect Krisp's confidential information.

6. Data Minimization

Krisp shall Process Personal Information only to the extent necessary to provide the Services and fulfill its obligations under the Agreement, this DPA, and this State Law Addendum, in accordance with applicable U.S. State Privacy Laws. Krisp shall not collect, retain, or Process Personal Information beyond what is reasonably required for the specified purposes, except as permitted under Section 2.4 of the DPA for anonymized or de-identified data. Customer shall ensure that Personal Information provided to Krisp is limited to what is necessary for the Services and complies with data minimization requirements under applicable U.S. State Privacy Laws, including where Customer acts as a Service Provider or Processor and provides Personal Information on behalf of a third-party controller. Upon Customer's written request, Krisp shall promptly delete or return any Personal Information that is no longer necessary for the Services, unless Krisp is required to retain such data under applicable law or for legitimate business purposes as permitted by the DPA.

7. Certification

Krisp certifies that it understands and will comply with the restrictions and obligations set forth in this State Law Addendum and in the applicable U.S. State Privacy Laws, including but not limited to those found in Cal. Civ. Code § 1798.140(v) and § 1798.100(d), as well as any analogous requirements under other U.S. State Privacy Laws in effect during the term of the Agreement.

8. Dispute Resolution

In the event of a dispute arising out of or relating to this State Law Addendum or Krisp's compliance with applicable U.S. State Privacy Laws, the Parties shall first attempt to resolve the dispute in good faith through informal discussions between designated representatives within thirty (30) days of written notice of the dispute. If the dispute remains unresolved, the Parties may pursue remedies in accordance with Section 8.2 of the DPA, provided that any such dispute shall be governed by the laws of the State of California, unless otherwise required by applicable U.S. State Privacy Laws. Nothing in this Section shall limit either Party's right to seek injunctive relief or other equitable remedies in a court of competent jurisdiction to prevent or mitigate harm arising from a breach of this State Law Addendum.

9. Miscellaneous

9.1. This State Law Addendum will terminate automatically upon the expiration or termination of the Agreement or DPA.

In the event of any conflict between the DPA and this State Law Addendum, this State Law Addendum shall prevail solely with respect to matters under the U.S. State Privacy Laws.