DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") supplements the Krisp Terms of Use, available at https://krisp.ai/terms-of-use/, as updated from time to time between the Customer (as defined in the Agreement) ("**Customer**") and Krisp Technologies, Inc. ("**Krisp**"), or other agreement between Customer and Krisp governing Customer's use of the Services ("**Agreement**"). Any terms not defined in this DPA shall have the meaning set forth in the Agreement. In the event of a conflict between the terms and conditions of this DPA and the Agreement, the terms of this DPA 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**".

1. Definitions.

1.1. **"Authorized Subprocessor"** means a third-party who has a need to know or otherwise access Customer's Personal Data to enable Krisp to perform its obligations under this DPA or the Agreement, and who is either (1) listed in Annex III of Schedule A or (2) subsequently authorized under Section 6.2 of this DPA.

1.2. "**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 DPA.

1.3. "**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) judicial or administrative interpretations 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.

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

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

1.6. "**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.

1.7. "**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 to Krisp and directing Krisp to Process Personal Data. Oral directions shall not constitute Instructions hereunder. Customer's Instructions shall be complete, clear, and in compliance with Data Protection Legislation. Krisp may, at its discretion, request clarification of any unclear or incomplete Instructions and may refuse to act on Instructions that it reasonably believes are unlawful or non-compliant with Data Protection Legislation, without liability. Customer acknowledges that Krisp has no obligation to monitor the compliance of Instructions with applicable Data Protection Legislation.

1.8. "**Personal Data**" means any information relating to a Data Subject that Krisp Processes on behalf of Customer in connection with the provision of the Services. This definition encompasses all information that qualifies as personal data, personal information, or similar terms under applicable Data Protection Legislation.

1.9. "**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.

1.10. "**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.

1.11. "**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 Authorized Subprocessors.

1.12. "**Services"** means the AI Meeting Assistant services performed by Krisp and identified in the Agreement.

1.13. "**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, and as may be amended from time to time.

1.14. "**US State Privacy Laws**" means the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020, and any regulations promulgated thereunder (collectively, "**CCPA**"); 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.

1.15. "**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, and as may be amended from time to time.

2. Details of Processing.

2.1. This DPA applies when Personal Data is Processed by Processor. In this context, Processor will act as processor to Customer, who acts as controller of Personal Data.

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 DPA.

2.3. The Commissioned Processing of the Personal Data by Krisp is solely carried out within the framework of the Agreement, this DPA 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 5.2 hereof.

2.4. Except as otherwise provided herein, Krisp shall not use the Personal Data for any purposes other than to perform the Services. Notwithstanding the foregoing, Krisp may use Personal 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. Krisp will ensure that any such anonymized data meets the standards for anonymization set forth in applicable Data Protection Legislation and relevant regulatory guidance on anonymization techniques. Krisp shall periodically review its anonymization techniques to ensure ongoing compliance with 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. Confidentiality.

Krisp shall ensure that any person it authorizes to process Personal Data has agreed to protect Personal Data in accordance with Krisp's confidentiality obligations in the Agreement. Customer agrees that Krisp may disclose Personal Data to its advisers, auditors or other third parties as reasonably required in connection with the performance of its obligations under this DPA, the Agreement, or the provision of Services to Customer.

4. Obligations of Customer.

Customer shall, in its use of the Services, at all times process Personal Data, and provide Instructions for the processing of Personal Data, in compliance with Data Protection Legislation. 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 DPA 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 Customer's Instructions and actions with respect to that Customer Personal Data, including its appointment of Krisp as another processor, have been authorized by the relevant data controller. Customer shall ensure that the processing of Personal Data in accordance with Customer's Instructions will not cause Krisp to be in breach of the Data Protection Legislation. Customer shall not provide or make available to Krisp any Personal Data in violation of this DPA, the Agreement or otherwise inappropriate for the nature of the Services, and shall indemnify Krisp from all claims and losses in connection therewith.

5. Obligations of Krisp.

5.1 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, except for Personal Data that Krisp is required to retain under applicable law, for legitimate business purposes such as billing or dispute resolution, or as necessary to demonstrate compliance with its legal obligations. 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.

5.2 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.

6. Authorized Subprocessors.

6.1. Customer acknowledges and agrees that Krisp may (1) engage its Affiliates and Authorized Subprocessors referenced in Annex III of Schedule A to this DPA 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.

6.2. 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 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.

6.3. If Customer reasonably objects to an engagement in accordance with Section 6.2, 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.

6.4. If Customer does not object to the engagement of a third party in accordance with Section 6.2 within fifteen (15) days of notice by Krisp, that third party will be deemed an Authorized Subprocessor for the purposes of this DPA.

6.5. If Customer and Krisp have entered into Standard Contractual Clauses as described in Section 9 (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.

7. Security of Personal Data.

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Krisp shall maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk of processing Personal Data, as described at https://trust.krisp.ai or such other URL as Krisp may designate.

8. Security Incident Management and Notification.

8.1. If Krisp becomes aware of a Security Incident, Krisp will promptly and without undue delay, but in no event later than 48 hours after discovery of the 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 or Customer's Authorized Users, or to attempts to compromise Krisp systems that do not result in actual unauthorized access to Personal Data.

8.2. 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.

8.3. 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.

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

9. Transfers of Personal Data.

9.1. The Parties agree that Krisp may transfer Personal Data processed under this DPA outside the EEA, the UK, or Switzerland as necessary to provide the Services. Customer acknowledges that Krisp's primary processing operations take place in the United States, and that the transfer of Customer's Personal Data to the United States is necessary for the provision of the Services to Customer. If Krisp transfers Personal Data protected under this DPA to a jurisdiction for which the European Commission has not issued an adequacy decision, Krisp will ensure that appropriate safeguards have been implemented for the transfer of Personal Data in accordance with Data Protection Legislation.

9.2. 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 DPA, the parties hereby execute and agree to be bound by the Standard Contractual Clauses and the UK Addendum, each as fully incorporated herein by reference.

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

9.3.1. Customer acts as data exporter and Krisp acts as data importer with respect to the Personal Data subject to the Standard Contractual Clauses, and its Module 2 (Controller to Processor) applies.

9.3.2. Clause 7 (the optional docking clause) does not apply.

9.3.3. If the Customer wishes to exercise its rights under Clause 8.9 (Documentation and compliance), 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. Krisp shall provide such Audit Report within fifteen (15) business days of Customer's request. 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, or where Customer is required by a data protection authority to conduct an audit, that Customer shall request to conduct an audit by itself or mandate an independent auditor as permitted under Clause 8.9.

9.3.4. Audits in accordance with Clause 8.9 (Documentation and compliance) shall: (i) be on no less than twenty (20) 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 or in response to a Security Incident; (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; and (vii) be at Customer's cost (including reimbursing Krisp for its reasonable costs associated with the audit) unless the parties agree otherwise.

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

9.3.6. 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.

9.3.7. 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.

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

9.3.9. Annexes I, II and III of the Standard Contractual Clauses are set forth in Schedule A of this DPA.

9.3.10. Any assistance provided by Krisp to Customer 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.

9.4. To the extent required under Data Protection Legislation of the United Kingdom, the UK Addendum forms part of this DPA and takes precedence over the rest of this DPA for such transfer to the extent of any conflict, and it will be deemed completed as follows:

9.4.1. The "exporter" is the Customer, and the exporter's contact information is set forth in Schedule A.
9.4.2. The "importer" is Krisp, and Krisp's contact information is set forth in Schedule A.
9.4.3. The Approved EU SCCs described in Table 2 of the UK Addendum shall be the Standard Contractual Clauses as completed in Section 9.3 above.
9.4.4. Annex 1A and 1B of the UK Addendum are set forth in Schedule A.
9.4.5. Annex II of the UK Addendum is set forth in Annex II of Schedule A.
9.4.6. Annex III of the UK Addendum is set forth in Annex III Schedule A.
9.4.7. Exporter and importer may end the UK Addendum as described in Table 4 of the UK Addendum.
9.5. To the extent required under Data Protection Legislation of Switzerland, the Standard Contractual Clauses form part of this DPA and take precedence over the rest of this DPA for such transfer to the extent of any conflict, and they will be deemed completed in accordance with Section 9.3 above, except that:
9.5.1. 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.
9.5.2. References to "Member State" refer to Switzerland, and data subjects may exercise and enforce their rights under the SCCs in Switzerland.
9.5.3. References to GDPR refer to the Swiss Federal Act on Data Protection, including its requirements for transparency, data subject rights, and data minimization.
9.5.4. The term "data subjects" shall be interpreted as including data subjects in Switzerland.
9.5.5. 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.
9.5.6. Krisp shall ensure that its Processing activities comply with the enhanced obligations of the revised Swiss Federal Act on Data Protection, including but not limited to providing clear and accessible information to data subjects about the Processing of their Personal Data and facilitating the exercise of their rights.

10. Rights of Data Subjects.

10.1 Krisp shall, to the extent permitted by law, notify Customer upon receipt of a request by a Data Subject to exercise the Data Subject's right of: access, rectification, erasure, data portability, restriction or cessation of processing, withdrawal of consent to processing, and/or objection to being subject to processing that constitutes automated decision-making (such requests individually and collectively "**Data Subject Request(s)**"). If Krisp receives a Data Subject Request in relation to Customer's data, Krisp will advise the Data Subject to submit their request to Customer and Customer will be responsible for responding to such request, including, where necessary, by using the functionality of the Services. Customer is solely responsible for ensuring that Data Subject Requests for erasure, restriction or cessation of processing, or withdrawal of consent to processing of any Personal Data are communicated to Krisp, and, if applicable, for ensuring that a record of consent to processing is maintained with respect to each Data Subject.
10.2 Krisp shall, at the request of Customer, and taking into account the nature of the processing applicable to any Data Subject Request, apply appropriate technical and organizational measures to assist Customer in complying with Customer's obligation to respond to such Data Subject Request and/or in demonstrating such compliance, where possible, provided that (i) Customer is itself unable to respond without Krisp's assistance and (ii) Krisp is able to do so in accordance with all applicable laws, rules, and regulations. 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 DPA or applicable Data Protection Legislation, in which case Krisp shall bear its own costs.

11. Final Provisions.

11.1 If one or more stipulations of this DPA are deemed void, this shall not affect validity of the other stipulations of this DPA. In the event of invalidity of one or more stipulations of this DPA, 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 DPA necessary, the Parties shall discuss and agree such required change in good faith.
11.2 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 DPA, including disputes regarding its existence, validity or termination or the consequences of its nullity; provided, however, that the Parties agree that this DPA shall be governed by the laws of the Republic of Ireland.

11.3 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 DPA, 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, shall not exceed the total fees paid or payable by Customer to Krisp under the Agreement in the twelve (12) months preceding the event giving rise to liability. This cap shall not apply to liability that cannot be limited under applicable Data Protection Legislation.

11.4 If any provision of this DPA is impacted by a change in applicable Data Protection Legislation, the Parties agree to negotiate in good faith any necessary revisions.

11.5 This DPA shall be effective as of the Effective Date of the Agreement and shall remain in force for the duration of the Agreement, unless terminated earlier upon mutual written agreement of the Parties.

SCHEDULE A

Annexes I, II and III of the Standard Contractual Clauses and UK Addendum.

ANNEX I

A. LIST OF PARTIES

Data Exporter: Customer
Contact details: as designated by Customer in the applicable Order Form in connection with the Agreement.
Activities relevant to the data transferred under this DPA: as listed in the Agreement
Signature and date: By entering into the Agreement, data exporter is deemed to have signed these Standard Contractual Clauses incorporated herein, as of the Effective Date of the Agreement.
Role (controller/processor): Controller

Data Importer: Krisp
Contact details: As designated by Krisp in the applicable Order Form in connection with the Agreement.
Activities relevant to the data transferred under this DPA: as listed in the Agreement
Signature and date: By entering into the Agreement, data importer is deemed to have signed these Standard Contractual Clauses incorporated herein, as of the Effective Date of the Agreement.
Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Duration of Processing
Krisp will process Customer's Personal Data as long as required (i) to provide the Services to Customer under the Agreement; (ii) for Krisp's legitimate business needs; or (iii) by applicable law or regulation.

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, as detailed below:
- Email addresses
- Team names
- Payment history and invoices
- Analytics data
- Call metadata
- Calendar data *
- Meeting transcription *
- Meeting recordings *
- Collaboration data *
- Integrations data *
- Other Personal Data contained in Customer's or its end users' communications, disclosed while using Krisp AI Meeting Assistant

* Each of these categories is transferred only where Customer or its end users enable the Service feature that requires it.

Further details are available at: https://krisp.ai/security-for-ai-meeting-assistant/#customer-data

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.

Where Controller uses Krisp AI Meeting Assistant, Krisp Processes Personal Data on Controller's documented Instructions and in accordance with Controller's configuration, which may include the recording, transcription, and storage of meeting content and related data described in the applicable documentation. Krisp does not intentionally collect other special categories of personal data; however, Controller or Controller's other meeting participants may disclose such information while using Krisp AI Meeting Assistant. Controller is responsible for providing all notices and obtaining all consents required for such processing. Krisp applies the technical and organizational measures described in Annex II, including encryption in transit and at rest and access restrictions on a need-to-know basis.

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
Krisp will process Customer's Personal Data as necessary to provide the Services under the Agreement, for the purposes specified in the Agreement and this DPA, and in accordance with Customer's Instructions as set forth in this DPA. The nature of processing includes, without limitation:

- Receiving data, including collection, accessing, retrieval, recording, and data entry
- Holding data, including storage, organization and structuring
- Using data, including automated processing using artificial intelligence models, analysis, testing, generation of voice embeddings for speaker identification
- Updating data, including correcting, adaptation, alteration, alignment and combination
- Protecting data, including restricting, encrypting, and security testing
- Sharing data, including disclosure, dissemination, allowing access or otherwise making available
- Returning data to the data exporter or data subject
- Erasing data, including destruction and deletion
- Anonymizing or pseudonymizing data, where applicable, for service improvement, analytics, or diagnostics

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 described in Annex III.

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. The supervisory authority for the purposes of the UK Addendum shall be the UK Information Commissioner's Officer.

ANNEX II

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

A. RELEVANT CERTIFICATIONS

1. 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.

2. 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:

1. Information Security Policies

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

2. Organization of Information Security

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

3. 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.

4. 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.

5. 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.

6. 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.

7. 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.

8. 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.

9. 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.

10. Communications Security

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

11. 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.

12. 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.

13. 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.

14. 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.

1. Additional Technical Measures

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

2. Additional Contractual Measures

(i) 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."

(ii) 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 Article 46 GDPR transfer tool and the resulting conflict of obligations for Krisp.

3. Additional Organizational Measures

(i) 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.

(ii) 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.

(iii) 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.

(iv) 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 Authorized 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 Authorized Subprocessors enter into a legally binding data protection agreements ("**Subprocessor DPAs**") to ensure that the Authorized 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 that satisfies that GDPR requirements. The Subprocessor DPAs also stipulates, among other things, Krisp's rights and Authorized Subprocessor's contractual obligations.
- Krisp relies on the SCCs as its lawful transfer mechanism under Article 46 GDPR.
- Krisp and its Authorized Subprocessors enter into legally binding Standard Contractual Clauses for personal data transfers outside of the EU, EEA, UK, or Switzerland.
- Authorized 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.

ANNEX III

AUTHORIZED SUBPROCESSORS

The Customer hereby authorizes the use of the Authorized Subprocessors listed at: https://trust.krisp.ai/subprocessors

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" and Krisp is the "Service Provider" or "Processor," 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 or service improvement, 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 Annex III of Schedule A 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. 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. 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 11.2 of the DPA, provided that any such dispute shall be governed by the laws of the Republic of Ireland, 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.
9.2. 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.