Zoom Video Communications, Inc.
Global Data Processing Addendum

This Data Processing Addendum ("**Addendum**") forms part of the Master Subscription Agreement, Terms of Service, Terms of Use, or any other agreement about the delivery of services (the "**Agreement**") between Zoom Video Communications, Inc. ("**Zoom**") and the Customer named in such Agreement or identified below to reflect the parties' agreement about the Processing of Personal Data (as those terms are defined below).

In providing the Services to Customer according to the Agreement, Zoom may Process Personal Data on behalf of Customer, and the parties agree to comply with the following provisions concerning any Personal Data, each acting reasonably and in good faith.

In the event of a conflict between the terms and conditions of this Addendum, or the Agreement, the terms and conditions of this Addendum shall prevail with respect to the subject matter of Processing of Personal Data. All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

1. Definitions

1.1. **"Affiliate"** means, with respect to a party, any entity that directly or indirectly controls, is controlled by, or is under common control with that party. For purposes of this Addendum, "control" means an economic or voting interest of at least fifty percent (50%) or, in the absence of such economic or voting interest, the power to direct or cause the direction of the management and set the policies of such entity.

1.2. "**Applicable Data Protection Law**" means any applicable legislative or regulatory regime enacted by a recognized government, or governmental or administrative entity with the purpose of protecting the privacy rights of natural persons or households consisting of natural persons, in particular the General Data Protection Regulation 2016/679 ("**GDPR**") and supplementing data protection law of the European Union Member States, the United Kingdom's Data Protection Act 2018 and the GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 ("**UK GDPR**"), the Swiss Federal Data Protection Act ("**Swiss DPA**"), Canada's Personal Information Protection and Electronic Documents Act ("**PIPEDA**") S.C. 2000, ch. 5, and any provincial legislation deemed substantially similar to PIPEDA under the procedures set forth therein, and the California Consumer Privacy Act ("**CCPA**") of 2018 and, the Brazilian Law No. 13,709/2018 – Brazilian General Data Protection Law ("**LGPD**").

1.3. "**Authorized Subprocessor**" means a subprocessor engaged by Zoom and Processes Personal Data to provide Services to Customer per the Customer's Instructions under the terms of this Agreement and this Addendum. Authorized Subprocessor may include Zoom Affiliates but shall exclude Zoom employees, contractors and consultants.

1.4. "**Controller**" means the entity that determines as a legal person alone or jointly with others the purposes and means of the Processing of Personal Data. Unless otherwise specified, Controller or "data exporter" refers to Customer.

1.5. "**Data Subject**" means the identified or identifiable person to whom Personal Data relates.

1.6. "**Instruction**" means direction issued by Customer to Zoom directing Zoom to Process Personal Data.

1.7. "**Personal Data**" means any information relating to an identified or identifiable natural person, including information that could be linked, directly or indirectly, with a particular Data Subject.

1.8. "**Personal Data Breach**" means a breach of security which results in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data Processed by Zoom or Zoom's Authorized Subprocessor.

1.9. "**Process**" or "**Processing**" means any operation or set of operations which is performed upon Personal Data or sets of 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, restriction, erasure, or destruction.

1.10. "**Processor**" means an entity which processes Personal Data on behalf of the Controller. Processor or "data importer" in this Addendum refers to Zoom.

1.11. "**Services**" means Zoom's Services as set forth in the Agreement.

1.12. "**Standard Contractual Clauses**" means: (i) where the GDPR applies the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (the "**EU SCCs**"); (ii) where the UK GDPR applies, the applicable standard data protection clauses adopted pursuant to Article 46(2)(c) or (d) of the UK GDPR (the "**UK SCCs**"); and (iii) where the Swiss DPA applies, the applicable standard data protection clauses issued, approved or otherwise recognized by the Swiss Federal Data Protection and Information Commissioner ("**FDPIC**")(the "**Swiss SCCs**").

1.13. "**Supervisory Authority**" means an independent public authority responsible for monitoring the application of Applicable Data Protection Law, including the Processing of Personal Data covered by this Addendum.

2. Roles of the Parties

Where Applicable Data Protection law provides for the roles of "controller," "processor," and "subprocessor":

2.1. Where Customer is a Controller of the Personal Data covered by this Addendum, Zoom shall be a Processor Processing Personal Data on behalf of the Customer and this Addendum shall apply accordingly.

2.2. Where Customer is a Processor of the Personal Data covered by this Addendum, Zoom shall be a subprocessor of the Personal Data and this Addendum shall apply accordingly.

2.3. Where and to the extent Zoom Processes Personal Data as a data controller, Zoom will Process such Personal Data in compliance with Applicable Data Protection Laws and the "Security Measures" set out in Exhibit B and Section 7 of this Addendum to the extent applicable.

3. Processing of Personal Data

3.1. Customer shall, in its use of the Services, at all times Process Personal Data, and provide documented Instructions for the Processing of Personal Data, in compliance with Applicable Data Protection Laws. Customer shall ensure that its instructions comply with all laws, rules and regulations applicable to the Personal Data, and that the Processing of Personal Data per Customer's instructions will not cause Zoom to be in breach of Applicable Data Protection Law. Customer is solely responsible for the accuracy, quality, and legality of (i) the Personal Data provided to Zoom by or on behalf of Customer; (ii) how Customer acquired any such Personal

Data; and (iii) the Instructions it provides to Zoom regarding the Processing of such Personal Data. Customer shall not provide or make available to Zoom any Personal Data in violation of the Agreement, this Addendum, or otherwise inappropriate for the nature of the Services and shall indemnify Zoom from all claims and losses in connection therewith.

3.2. Zoom shall Process Customer's Personal Data on behalf of the Customer only (i) to perform the Agreement and as set out in EXHIBIT A.2; (ii) under the terms and conditions outlined in this Addendum, and (iii) any other documented Instructions provided by Customer (which may be provided to Zoom from time to time, including for example by way of letter of instruction or through the Customer's use of Zoom settings, controls or other user preference functionality within the Services); including concerning transfers of Customer's Personal Data to a third country or an international organization, unless Zoom is required to do otherwise by applicable law to which Zoom is subject, in such a case Zoom shall inform the Customer of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest. Customer hereby instructs Zoom to Process Personal Data following the preceding and as part of any Processing initiated by Customer in its use of the Services, using means of Processing that are reasonably necessary and proportionate to providing the Services. For the avoidance of doubt, Zoom shall not engage in the sale of Customer's Personal Data within the meaning of the CCPA.

3.3. Zoom shall immediately notify the Customer, if, in Zoom's opinion, an Instruction of the Customer infringes Applicable Data Protection Law and request that Customer withdraw, amend or confirm the relevant Instruction. Pending the decision on the withdrawal, amendment, or confirmation of the relevant Instruction, Zoom shall be entitled to suspend the implementation of the relevant Instruction.

3.4. The subject matter, nature, purpose, and duration of this Processing, as well as the types of Personal Data collected and categories of Data Subjects, are described in EXHIBIT A.2 to this Addendum. Following the completion of the Services, at Customer's choice, Zoom shall either enable Customer to delete all of Customer's Personal Data, shall return to Customer all Personal Data, or shall delete all Personal Data, and delete any existing copies in compliance with its data retention and deletion policy, except to the extent that further storage by Zoom is required by applicable law. If return or destruction is impracticable or prohibited by law, rule or regulation, Zoom shall take measures to block such Customer's Personal Data from any further Processing (except to the extent necessary for its continued hosting or Processing required by applicable law) and shall continue to appropriately protect the Personal Data remaining in its possession, custody, or control and, where any Authorized Subprocessor continues to possess Customer's Personal Data, require the Authorized Subprocessor to take the same measures that would be required of Zoom.

4. Authorized Persons

Zoom shall ensure that all persons authorized to Process Customer's Personal Data are made aware of the confidential nature of Personal Data and have committed themselves to confidentiality (e.g., by confidentiality agreements) or are under an appropriate statutory obligation of confidentiality.

5. Authorized Subprocessors

5.1. The Customer hereby generally authorizes Zoom to engage subprocessors in accordance with this Section 5.

5.2. Customer approves the third-party subprocessors currently listed at zoom.us/subprocessors.

5.3. Zoom may remove, replace or appoint suitable and reliable further subprocessors in accordance with this Section 5.3:

5.3.1. Zoom shall at least fifteen (15) days before engaging any new subprocessors to access or participate in the Processing of Customer's Personal Data notify Customer of that update. The Customer may object to such an engagement in writing within ten (10) days of receipt of the aforementioned notice by the Customer. To enable such notifications, Customer shall visit zoom.us/subprocessors and enter the email address to which Zoom shall send such notifications into the submission field at the bottom of the page.

5.3.2. If the Customer reasonably objects to the engagement of a new subprocessor, Zoom shall have the right to cure the objection through one of the following options (to be selected at Zoom's sole discretion):

a) Zoom cancels its plans to use the subprocessor with regard to Customer's Personal Data.

b) Zoom will take the corrective steps requested by Customer in its objection (which remove Customer's objection) and proceed to use the subprocessor with regard to Customer's Personal Data.

c) Zoom may cease to provide or Customer may agree not to use (temporarily or permanently) the particular aspect of the Service that would involve the use of such subprocessor with regard to Controller's personal data.

d) Zoom provides Customer with a written description of commercially reasonable alternative(s), if any, to such engagement, including without limitation modification to the Services. If Zoom, in its sole discretion, cannot provide any such alternative(s), or if Customer does not agree to any such alternative(s) if provided, Zoom and Customer may terminate this Addendum with prior written notice. Termination shall not relieve Customer of any fees or charges owed to Zoom for Services provided up to the effective date of the termination under the Agreement.

5.3.3. If Customer does not object to a new subprocessor's engagement within ten (10) days of notice by Zoom, that new subprocessor shall be deemed accepted.

5.4. Zoom shall ensure that all Authorized Subprocessors have executed confidentiality agreements that prevent them from unauthorized Processing of Customer's Personal Data both during and after their engagement by Zoom.

5.5. Zoom shall, e.g., by way of contract or other legal act impose on the Authorized Subprocessor the equivalent data protection obligations as set out in this Addendum. Zoom shall exercise reasonable care and evaluate a potential subprocessor's data protection practices before allowing the subprocessor to act as an Authorized Subprocessor.

5.6. Zoom shall be fully liable to Customer where that Authorized Subprocessor fails to fulfil its data protection obligations for the performance of that Authorized Subprocessor's obligations to the

same extent that Zoom would itself be liable under this Addendum had it conducted such acts or omissions.

5.7. If Customer and Zoom have entered into Standard Contractual Clauses as described in Section 7 (International Transfers of Personal Data), the above authorizations will constitute Customer's prior written consent to the subcontracting by Zoom of the Processing of Customer's 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 Zoom to Customer pursuant to Clause 5(j) of the Standard Contractual Clauses may have commercial information, or information unrelated to the Standard Contractual Clauses or their equivalent, removed by the Zoom beforehand, and that Zoom will provide such copies only upon request by Customer.

6. Security of Personal Data

6.1. 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, Zoom shall maintain appropriate technical and organizational measures with regard to Customer's Personal Data and to ensure a level of security appropriate to the risk, including, but not limited to, the "**Security Measures**" set out in EXHIBIT B. Customer acknowledges that the Security Measures are subject to technical progress and development and that Zoom may update or modify the Security Measures from time to time, provided that such updates and modifications do not degrade or diminish the overall security of the Services.

6.2. Zoom shall implement such measures to ensure a level of security appropriate to the risk involved, including as appropriate:

6.2.1. the pseudonymization (as defined in Art. 4(5) of the GDPR) and encryption of Personal Data;

6.2.2. the ability to ensure the ongoing confidentiality, integrity, availability, and resilience of Processing systems and services;

6.2.3. the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and

6.2.4. a process for regularly testing, assessing, and evaluating the effectiveness of security measures.

7. International Transfers of Personal Data

7.1. Customer acknowledges and agrees that Zoom may transfer and process Customer's Personal Data to and in the United States and anywhere else in the world where Zoom, its Affiliates, or its Authorized Subprocessors maintain data processing operations. Zoom shall ensure that such transfers are made in compliance with Applicable Data Protection Law and this Addendum.

7.2. Any transfer of Customer's Personal Data made subject to this Addendum from member states of the European Union, the European Economic Area (Iceland, Liechtenstein, Norway), Switzerland or the United Kingdom to any countries where the European Commission, the FDIPC or the UK Information Commissioner's Office has not decided that this third country or more specified sectors within that third country in question ensures an adequate level of protection, shall be

undertaken, in particular, through the Standard Contractual Clauses, in connection with which the Parties agree the following:

7.2.1 EU SCCs (Controller to Controller Transfers). In relation to Personal Data that is protected by the EU GDPR and processed in accordance with Section 2.3 of this Addendum, the EU SCCs shall apply, completed as follows:

(a) Module One will apply;
(b) in Clause 7, the optional docking clause will apply;
(c) in Clause 11, the optional language will not apply;
(d) in Clause 17, Option 1 will apply, and the New EU SCCs will be governed by Irish law;
(e) in Clause 18(b), disputes shall be resolved before the courts of Ireland;
(f) Annex I of the New EU SCCs shall be deemed completed with the information set out in **EXHIBIT A.1** to this Addendum; and
(g) Subject to Section 6.1 of this Addendum, Annex II of the New EU SCCs shall be deemed completed with the information set out in **EXHIBIT B** to this Addendum;

7.2.2 **EU SCCs (Processor to Processor Transfers).** In relation to Personal Data that is protected by the EU GDPR and processed in accordance with Sections 2.1 or 2.2 of this Addendum, the EU SCCs shall apply, completed as follows:

(a) Module Two or Module Three will apply (as applicable);
(b) in Clause 7, the optional docking clause will apply;
(c) in Clause 9, Option 2 will apply, and the time period for prior notice of Sub-processor changes shall be as set out in Section 5.3 of this DPA;
(d) in Clause 11, the optional language will not apply;
(e) in Clause 17, Option 1 will apply, and the New EU SCCs will be governed by Irish law;
(f) in Clause 18(b), disputes shall be resolved before the courts of Ireland;
(g) Annex I of the New EU SCCs shall be deemed completed with the information set out in EXHIBIT A.2 to this Addendum; and
(h) Subject to Section 6.1 of this Addendum, Annex II of the New EU SCCs shall be deemed completed with the information set out in EXHIBIT B to this Addendum;

7.2.3 **Transfers from the UK.** In relation to Personal Data that is protected by the UK GDPR, the EU SCCs will apply in accordance with Sections 7.2.1 and 7.2.2 above, with the following modifications:

(a) any references in the EU SCCs to "Directive 95/46/EC" or "Regulation (EU) 2016/679" shall be interpreted as references to the UK GDPR; references to specific Articles of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK GDPR;
(b) references to "EU", "Union" and "Member State law" are all replaced with "UK"; Clause 13(a) and Part C of Annex I of the EU SCCs are not used; references to the "competent supervisory authority" and "competent courts" shall be interpreted as references to the Information Commissioner and the courts of England and Wales;
(c) Clause 17 of the EU SCCs is replaced to state that "The Clauses are governed by the laws of England and Wales" and Clause 18 of the EU SCCs is replaced to state

"Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may bring legal proceeding against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts", unless the EU SCCs as implemented above cannot be used to lawfully transfer such Personal Data in compliance with the UK GDPR, in which event the UK SCCs shall instead be incorporated by reference and form an integral part of this Addendum and shall apply to such transfers. Where this is the case, the relevant Annexes of the UK SCCs shall be populated using the information contained in EXHIBITS A.1, A.2 and B to this Addendum (as applicable);

7.2.4 **Transfers from Switzerland.** In relation to Personal Data that is protected by the Swiss DPA, the EU SCCs will apply in accordance with Sections 7.2.1 and 7.2.2, with the following modifications:

(a) any references in the EU SCCs to "Directive 95/46/EC" or "Regulation (EU) 2016/679" shall be interpreted as references to the Swiss DPA;

(b) references to "EU", "Union", "Member State" and "Member State law" shall be interpreted as references to Switzerland and Swiss law, as the case may be; and

(c) references to the "competent supervisory authority" and "competent courts" shall be interpreted as references to the FDIPC and competent courts in Switzerland, unless the EU SCCs as implemented above cannot be used to lawfully transfer such Personal Data in compliance with the Swiss DPA, in which event the Swiss SCCS shall instead be incorporated by reference and form an integral part of this Addendum and shall apply to such transfers. Where this is the case, the relevant Annexes of the Swiss SCCs shall be populated using the information contained in **EXHIBITS A.1, A.2** and **B** to this Addendum (as applicable);

7.2.5 **No Conflict.** It is not the intention of either party to contradict or restrict any of the provisions set forth in the Standard Contractual Clauses and, accordingly, if and to the extent the Standard Contractual Clauses conflict with any provision of the Agreement (including this Addendum) the Standard Contractual Clauses shall prevail to the extent of such conflict.

7.3. Zoom may adopt a replacement data export mechanism (including any new version of or successor to the Standard Contractual Clauses or alternative mechanisms adopted pursuant to Applicable Data Protection Law) ("**Alternative Transfer Mechanism**"). So long as the Alternative Transfer Mechanism complies with Applicable Data Protection Law and extends to the territories to which Customer's Personal Data is transferred on behalf of the Customer, Customer agrees to execute documents and take other reasonably necessary actions to give legal effect to such Alternative Transfer Mechanism.

7.4. In the event the Supervisory Authority of a Controller's country begins regulation of the transfer of Personal Data from the Controller's country to any other country, including the approval of Brazil standard contractual clauses, then Zoom shall amend this Addendum and adopt all the necessary measures as may be required to carry out such international transfer, or if the measures imposed by the Supervisory Authority of the Controller's country cannot be adopted, immediately suspend such international transfer.

8. Rights of Data Subjects

8.1. To the extent required by Applicable Data Protection Law, Zoom shall promptly notify Customer upon receipt of a request by a Data Subject to exercise Data Subject rights under Applicable Data Protection Law. Zoom 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.

8.2. Zoom shall, taking into account the nature of the Processing, assist the Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Customer's obligation to respond to requests for exercising the Data Subject's rights (regarding information, access, rectification and erasure, restriction of Processing, notification, data portability, objection and automated decision-making) under Applicable Data Protection Law.

9. Impact Assessment, Personal Data Breach and Audits

9.1. Zoom shall, taking into account the nature of the Processing and the information available to Zoom, assist Customer in ensuring compliance with its obligations under Applicable Data Protection Law to conduct a data protection impact assessment and, with prior notice, to assist with consultations with the supervisory authority, where required.

9.2. Zoom shall maintain records sufficient to demonstrate its compliance with its obligations under this Addendum.

9.3. Zoom makes available to the Customer all information reasonably necessary to demonstrate compliance with the obligations laid down in Art. 28 GDPR and allows for and contributes to audits, including inspections, reasonably requested by the Customer.

9.4. Upon Customer's request, Zoom shall, no more than once per calendar year make available for Customer's review, copies of certifications or reports demonstrating Zoom's compliance with prevailing data security standards applicable to the Processing of Customer's Personal Data. If the Customer and Zoom have entered into Standard Contractual Clauses, the Customer's right to audit Zoom's activities under the Standard Contractual Clauses shall be interpreted in line with this Addendum, so as to be satisfied by the audit rights provided to the Customer as set out in this Section 9.3 and 9.4.

9.5. In the event of a confirmed Personal Data Breach, Zoom shall, without undue delay after becoming aware of a breach of personal data, inform Customer of the Personal Data Breach and take such steps as Zoom in its sole discretion deems necessary and reasonable to remediate such violation.

9.6. In the event of such a Personal Data Breach, Zoom shall, taking into account the nature of the Processing and the information available to Zoom, provide Customer with reasonable cooperation and assistance necessary for Customer to comply with its obligations under Applicable Data Protection Law with respect to notifying (i) the relevant Supervisory Authority and/or (ii) Data Subjects affected by such Personal Data Breach without undue delay.

9.7. The obligations described in Sections 9.5 and 9.6 shall not apply in the event that a Personal Data Breach results from the actions or omissions of Customer, except where required by

Applicable Data Protection Law. Zoom's obligation to report or respond to a Personal Data Breach under Sections 9.5 and 9.6 will not be construed as an acknowledgement by Zoom of any fault or liability with respect to the Personal Data Breach.

10. General

10.1. This Addendum may be executed in counterparts, each of which will be deemed an original, but all of which together will constitute one and the same instrument.

10.2. Customer and Zoom acknowledge that the other party may disclose the Standard Contractual Clauses, this Addendum and any privacy-related provisions in the Agreement to any UK, Swiss, European, US or Brazilian regulator upon request.

10.3. Except for the changes made by this Addendum, the Agreement remains unchanged and in full force and effect. If there is any conflict between this Addendum and the Agreement with regard to the subject matter of this Addendum, this Addendum shall prevail to the extent of that conflict.

10.4. In the event of a change in Applicable Data Protection Law or a determination or order by a supervisory authority or competent court affecting this Addendum or the lawfulness of any Processing activities under this Addendum, Zoom may (in its sole discretion) make any amendments to this Addendum as are reasonably necessary to ensure continued compliance with Applicable Data Protection Law and/or the Processing instructions herein.

10.5. The provisions of this Addendum are severable. If any phrase, clause or provision or Exhibit (including the Standard Contractual Clauses) is invalid or unenforceable in whole or in part, such invalidity or unenforceability shall affect only such phrase, clause or provision, and the rest of this Addendum or the remainder of the Exhibit, shall remain in full force and effect.

10.6. This Addendum shall be governed by and construed in accordance with the governing law and jurisdiction provisions in the Agreement, unless required otherwise by Applicable Data Protection Law.

[Signature page follows.]

"Customer"	**Zoom Video Communications, Inc.**
Signature: _____	Signature: DocuSigned by: Deborah Fay 3BA802462F4F44D... _____
Print Name: _____	Print Name: Deborah Fay _____
Customer Address: _____	Title: Deputy General Counsel _____
Title: _____	Date: Sep 22, 2021 _____
Date: _____	

EXHIBIT A.1 - Description of the Processing / Transfer

Controller to Controller

(A) List of Parties:

Data Exporter	**Data Importer**
Name:	Name: Zoom Video Communications, Inc.
Address:	Address: 55 Almaden Blvd. Suite 600, San Jose, CA 95113
Contact Person's Name, position and contact details: Name: Position: Address:	Contact Person's Name, position and contact details: Name: Deborah Fay Position: Data Protection Officer Address: 55 Almaden Blvd., Suite 600, San Jose, CA95113
Activities relevant to the transfer: See Schedule 1(B) below	Activities relevant to the transfer: See Schedule 1(B) below
Role: Controller	Role: Controller

(B) Description of Transfer

Categories Data Subjects	
The personal data transferred concern the following categories of data subjects	Individual Zoom Service users
Purposes of the transfer(s)	
The transfer is made for the following purposes:	Zoom processes the personal data to provide the Services, for product research and development, marketing and promotions, authentication, integrity, security and safety; and for legal reasons
Categories of Personal Data	
The personal data transferred concern the following categories of data:	• account information • product and website usage information • device information

	• settings information
Frequency of the transfer	
Whether continuous or one-off.	The transfer of account information is one off, otherwise continuous when using the Service
Special categories of personal data (if appropriate)	
The personal data transferred concern the following categories of sensitive data:	Not applicable
Duration of processing:	The term of the Agreement plus the period until Zoom deletes all Customer's Personal Data processed on behalf of Customer in accordance with the Agreement.
Nature and Subject Matter of the Processing:	The personal data transferred may be subject to the following processing activities: Managing contracts with account owners, including billing, compliance with contractual obligations, and related administration Authenticating accounts and activity, detecting, investigating, and preventing malicious conduct or unsafe experiences, addressing security threats, protecting public safety, and securing the Services. Developing, testing, and improving the Services. Marketing, advertising, and promoting the Services Compliance with applicable law, investigating or participating in civil discovery, litigation, or other adversarial legal proceedings, and enforcing or investigating potential violations of our Terms of Service or policies.
Retention period (or, if not possible to determine, the criteria used to determine that period):	Zoom retains personal data for as long as required for the purposes for which it was collected unless a longer retention period is required by applicable law. The criteria used to determine our retention periods include the following:

	• The length of time of our relationship with Service users (for example, the duration of a Zoom account) • Whether account owners modify or their users delete information through their accounts • Whether we have a legal obligation to keep the data (for example, certain laws require us to keep records of your transactions for a certain period of time before we can delete them) • Whether retention is advisable in light of our legal position (such as in regard to the enforcement of our agreements, the resolution of disputes, and applicable statutes of limitations, litigation, or regulatory investigation)

(C): Competent supervisory authority

The competent supervisory authority, in accordance with Clause 13 of the New EU SCCs, must be (i) the supervisory authority applicable to the data exporter in its EEA country of establishment or, (ii) where the data exporter is not established in the EEA, the supervisory authority applicable in the EEA country where the data exporter's EU representative has been appointed pursuant to Article 27(1) of the GDPR, or (iii) where the data exporter is not obliged to appoint a representative, the supervisory authority applicable to the EEA country where the data subjects relevant to the transfer are located. With respect to Personal Data to which the UK GDPR applies, the competent supervisory authority is the Information Commissioners Office (the "ICO"). With respect to Personal Data to which the Swiss DPA applies, the competent supervisory authority is the Swiss Federal Data Protection and Information Commissioner.

EXHIBIT A.2 - Description of the Processing / Transfer

Controller to Processor / Processor to Processor

(A) List of Parties:

Data Exporter	**Data Importer**
Name:	Name: Zoom Video Communications, Inc.
Address:	Address: 55 Almaden Blvd. Suite 600, San Jose, CA 95113
Contact Person's Name, position and contact details: Name: Position: Address:	Contact Person's Name, position and contact details: Name: Deborah Fay Position: Data Protection Officer Address: 55 Almaden Blvd., Suite 600, San Jose, CA95113
Activities relevant to the transfer: See Schedule 1(B) below	Activities relevant to the transfer: See Schedule 1(B) below
Role: Controller or Processor	Role: Processor

(B) Description of Transfer

Categories Data Subjects	
The personal data transferred concern the following categories of data subjects	Individuals about whom Personal Data is provided to Zoom via the Services by (or at the direction of) Customer or Customer's end-users, which may include without limitation Customer's or its Affiliates' employees, contractors, and end-users.
Purposes of the transfer(s)	
The transfer is made for the following purposes:	Zoom will Process Customer's Personal Data on behalf of Customer for the purposes of providing the Services in accordance with the Agreement, which may include providing access to Customer account data to third parties (including Zoom resellers or distributors through whom Customer has purchased

	Zoom services, where Zoom received Instructions from the customer to this effect).
Categories of Personal Data	
The personal data transferred concern the following categories of data:	Depending on Customer's use of the Services, Personal Data provided to Zoom via the Services by (or at the direction of) Customer or Customer's end users, including but not limited to the following: • Cloud Recordings (optional): Mp4 of all video, audio, whiteboard, captions and presentations, • M4A of all audio, text file of all in meeting chats, audio transcript file • Meeting notification content / text message alerts (optional): name and contact of message recipient and any free text meeting details input by the user that happen to contain Personal Data elements • Meeting and Webinar: title, date and time, polls, chat logs, attendee information (screen name, join/leave time) • Registration details (optional): name and contact details of meeting or webinar registration invitee and any data requested by Customer to be provided by registrant that may contain Personal Data elements • Webinar only: Questions & Answers, and survey information • Persistent Chat: messages and in-chat file transfer (including image sharing)
Frequency of the transfer	
Whether continuous of one off.	Continuous
Special categories of personal data (if appropriate)	
The personal data transferred concern the following categories of sensitive data:	Special categories of data are not required to use the service. The extent of any submission of such data is determined and controlled by the Customer / data exporter in its sole discretion. Such special categories of data include, but may not be limited to, Personal Data with information revealing racial or ethnic origins, political opinions, religious or philosophical beliefs, trade union membership, and

	the processing of data concerning an individual's health or sex life.
Duration of processing:	The term of the Agreement plus the period until Zoom deletes all Customer's Personal Data processed on behalf of Customer in accordance with the Agreement.
Nature and Subject Matter of the Processing:	The personal data transferred may be subject to the following processing activities: • account configuration and maintenance; • facilitating conferences and meetings between data subjects and third-party participants; • hosting and storing personal data arising from such conferences and meetings solely for the purposes of providing the services; • customer/ client technical and operational support.
Retention period (or, if not possible to determine, the criteria used to determine that period):	The term of the Agreement plus the period until Zoom deletes all Customer's Personal Data processed on behalf of Customer in accordance with the Agreement, subject to a longer period of retention where required by applicable law.

(C): Competent supervisory authority

The competent supervisory authority, in accordance with Clause 13 of the New EU SCCs, must be (i) the supervisory authority applicable to the data exporter in its EEA country of establishment or, (ii) where the data exporter is not established in the EEA, the supervisory authority applicable in the EEA country where the data exporter's EU representative has been appointed pursuant to Article 27(1) of the GDPR, or (iii) where the data exporter is not obliged to appoint a representative, the supervisory authority applicable to the EEA country where the data subjects relevant to the transfer are located. With respect to Personal Data to which the UK GDPR applies, the competent supervisory authority is the Information Commissioners Office (the "ICO"). With respect to Personal Data to which the Swiss DPA applies, the competent supervisory authority is the Swiss Federal Data Protection and Information Commissioner.

EXHIBIT B Technical and Organizational Security Measures

Zoom's technical and organizational security measures for Processing Customer Personal Data will meet the Minimum-Security Control Requirements set out in this Exhibit B ("**Security Measures**"). Customer recognizes that there may be multiple acceptable approaches to accomplish a particular minimum control requirement. Zoom must document in reasonable detail how a particular control meets the stated minimum control requirement. Zoom may revise the Security Measures from time to time. The term "should" in these Security Measures means that Zoom will use commercially reasonable efforts to accomplish the stated minimum control requirement and will document those efforts in reasonable detail, including the rationale, if any, for deviation.

As used in these Security Measures, (i) "including" and its derivatives mean "including but not limited to"; and (ii) any capitalized terms not defined in this Exhibit B shall have the same meaning as set forth in the Addendum.

1. Definitions

1.1. "**Systems**" means Zoom's production systems.
1.2. "**Assets**" means Zoom's production assets.
1.3. "**Facilities**" means Zoom's production facilities, whether owned or leased by Zoom (e.g., AWS, data centers).

2. Risk Management

2.1. Risk Assessment Program. The effectiveness of controls must be regularly validated through a documented risk assessment program and appropriately managed remediation efforts.
2.2. Risk Assessment. A risk assessment must be performed annually to verify the implementation of controls that protect business operations and Confidential Information.

3. Security Policy

A documented set of rules and procedures must regulate the Processing of information and associated services.

3.1. Security Policies and Exception Process. Security policies must be documented, reviewed, and approved, with management oversight, on a periodic basis, following industry best practices.
3.2. A risk-based exception management process must be in place for prioritization, approval, and remediation or risk acceptance of controls that have not been adopted or implemented.
3.3. Awareness and Education Program. Security policies and responsibilities must be communicated and socialized within the organization to Zoom personnel. Zoom personnel must receive security awareness training on an annual basis.

4. Organizational Security

A personnel security policy must be in place to establish organizational requirements to ensure proper training, competent performance, and an appropriate and accountable security organization.

4.1. *Organization.* Current organizational charts representing key management responsibilities for services provided must be maintained.
4.2. *Background Checks*. Where legally permissible, background checks (including criminal) must be performed on applicable Zoom personnel.
4.3. *Confidentiality Agreements*. Zoom personnel must be subject to written non-disclosure or confidentiality obligations.

5. Technology Asset Management

Controls must be in place to protect Zoom production assets, including mechanisms to maintain an accurate inventory of assets and handling standards for introduction and transfer, removal and disposal of assets.

5.1. *Accountability*. A process for maintaining an inventory of hardware and software assets and other information resources, such as databases and file structures, must be documented. Process for periodic asset inventory reviews must be documented. Identification of unauthorized or unsupported hardware/ software must be performed.

5.2. *Asset Disposal or Reuse*. If applicable, Zoom will use industry standards to wipe or carry out physical destruction as the minimum standard for disposing of assets. Zoom must have documented procedures for disposal or reuse of assets.

5.3. Procedures must be in place to remove data from production systems in which Customer's Personal Data are stored, processed, or transmitted.

6. Physical and Environmental

Controls must be in place to protect systems against physical penetration by malicious or unauthorized people, damage from environmental contaminants and electronic penetration through active or passive electronic emissions.

6.1. *Physical and Environmental Security Policy*. Physical and environmental security plans must exist for facilities and scenarios involving access or storage of Customer's Personal Data. Additional physical and environmental controls must be required and enforced for applicable facilities, including servers and datacenter locations.

6.2. *Physical Access.* Physical access, to include visitor access to facilities, must be restricted and all access periodically reviewed.

6.3. Policies must be in place to ensure that information is accessed on a need-to-know basis.

6.4. *Environmental Control*. Facilities, including data and processing centers, must maintain appropriate environmental controls, including fire detection and suppression, climate control and monitoring, power and back-up power solutions, and water damage detection. Environmental control components must be monitored and periodically tested.

7. Communication and Connectivity

Zoom must implement controls over its communication network to safeguard data. Controls must include securing the production network and implementation of encryption, logging and monitoring, and disabling communications where no business need exists.

7.1. *Network Identification*. A production network diagram, to include production devices, must be kept current to facilitate analysis and incident response.

7.2. *Data Flow Diagram.* A current data flow diagram must depict data from origination to endpoint (including data which may be shared with Subprocessors).

7.3. *Data Storage.* All of Customer's Personal Data, including Customer's Personal Data shared with subprocessors, must be stored and maintained in a manner that allows for its return or secure destruction upon request from Customer.

7.4. *Firewalls.* Firewalls must be used for the isolation of all environments, to include physical, virtual, network devices, production and non-production, and application/presentation layers. Firewall management must follow a process that includes restriction of administrative access, and that is documented, reviewed, and approved, with management oversight, on a periodic basis.

7.5. The production network must be either firewalled or physically isolated from the development and test environments. Multi-tier security architectures that segment application tiers (e.g., presentation layer, application and data) must be used.

7.6. Periodic network vulnerability scans must be performed, and any critical vulnerabilities identified must be remediated within a defined and reasonable timeframe.

7.7. *Clock Synchronization*. Production network devices must have internal clocks synchronized to reliable time sources.

7.8. *Remote Access.* The data flow in the remote connection must be encrypted and multi-factor authentication must be utilized during the login process.

7.9. Remote connection settings must limit the ability of remote users to access both initiating network and remote network simultaneously (i.e., no split tunneling).

7.10. Subprocessors' remote access, if any, must adhere to the same controls and must have a valid business justification.

7.11. *Wireless Access.* Wireless access to the Zoom corporate network must be configured to require authentication and be encrypted.

8. Change Management

Changes to the production systems, production network, applications, data files structures, other system components, and physical/environmental changes must be monitored and controlled through a formal change control process. Changes must be reviewed, approved, and monitored during postimplementation to ensure that expected changes and their desired result are accurate.

8.1. *Change Policy and Procedure.* A change management policy, including application, operating system, network infrastructure, and firewall changes must be documented, reviewed, and approved, with management oversight, on a periodic basis.

8.2. The change management policy must include clearly identified roles and responsibilities so as to support separation of duties (e.g., request, approve, implement). The approval process must include pre- and post-evaluation of change. Zoom posts service status and scheduled maintenance at https://status.zoom.us.

9. Operations

Documented operational procedures must ensure the correct and secure operation of Zoom's assets. Operational procedures must be documented and include monitoring of capacity, performance, service level agreements and key performance indicators.

10. Access Control

Authentication and authorization controls must be appropriately robust for the risk of the system, data, application, and platform; access rights must be granted based on the principle of least privilege and monitored to log access and security events, using tools that enable rapid analysis of user activities.

10.1. *Logical Access Control Policy*. Documented logical access policies and procedures must support role-based, "need-to-know" access (e.g., interdepartmental transfers, terminations) and ensure separation of duties during the approval and provisioning process. Each account provisioned must be uniquely identified. User access reviews must be conducted on a periodic basis.

10.2. *Privileged Access*. Management of privileged user accounts (e.g., those accounts that have the ability to override system controls), to include service accounts, must follow a documented process and be restricted. A periodic review and governance process must be maintained to ensure appropriate provisioning of privileged access.

10.3. *Authentication and Authorization*. A documented authentication and authorization policy must cover all applicable systems. That policy must include password provisioning requirements, password complexity requirements, password resets, thresholds for lockout attempts, thresholds for inactivity, and assurance that no shared accounts are utilized. Authentication credentials must be encrypted, including in transit to and from subprocessors' environments or when stored by subprocessors.

11. Data Integrity

Controls must ensure that any data stored, received, controlled, or otherwise accessed is accurate and reliable. Procedures must be in place to validate data integrity.

11.1. *Data Transmission Controls*. Processes, procedures, and controls must be documented, reviewed, and approved, with management oversight, on a periodic basis, to ensure data integrity during transmission and to validate that the data transmitted is the same as data received.

11.2. *Data Transaction Controls*. Controls must be in place to protect the integrity of data transactions at rest and in transit.

11.3. *Encryption*. Data must be protected and should be encrypted, both in transit and at rest, including when shared with subprocessors.

11.4. *Data Policies*. A policy must be in place to cover data classifications, encryption use, key and certificate lifecycle management, cryptographic algorithms and associated key lengths. This policy must be documented, reviewed, and approved with management oversight, on a periodic basis.

11.5. *Encryption Uses*. Customer Personal Data must be protected, and should be encrypted, while in transit and at rest. Confidential Information must be protected, and should be encrypted when stored and while in transit over any network; authentication credentials must be encrypted at all times, in transit or in storage.

12. Incident Response

A documented plan and associated procedures, to include the responsibilities of Zoom personnel and identification of parties to be notified in case of an information security incident, must be in place.

12.1. *Incident Response Process*. The information security incident management program must be documented, tested, updated as needed, reviewed, and approved, with management oversight, on a periodic basis. The incident management policy and procedures must include prioritization, roles and responsibilities, procedures for escalation (internal) and notification, tracking and reporting, containment and remediation, and preservation of data to maintain forensic integrity.

13. Business Continuity and Disaster Recovery

Zoom must have formal documented recovery plans to identify the resources and specify actions required to help minimize losses in the event of a disruption to the business unit, support group unit, application, or infrastructure component. Plans assure timely and orderly recovery of business, support processes, operations, and technology components within an agreed upon time frame and include orderly restoration of business activities when the primary work environment is unavailable.

13.1. *Business Recovery Plans*. Comprehensive business resiliency plans addressing business interruptions of key resources supporting services, including those provided by subprocessors, must be documented, tested, reviewed, and approved, with management oversight, on a

periodic basis. The business resiliency plan must have an acceptable alternative work location in place to ensure service level commitments are met.

13.2. *Technology Recovery*. Technology recovery plans to minimize service interruptions and ensure recovery of systems, infrastructure, databases, applications, etc. Must be documented, tested, reviewed, and approved with management oversight, on a periodic basis.

14. Back-ups

Zoom must have policies and procedures for back-ups of Customer's Personal Data. Backups must be protected using industry best practices.

14.1. *Back-up and Redundancy Processes*. Processes enabling full restoration of production systems, applications, and data must be documented, reviewed, and approved, with management oversight, on a periodic basis.

15. Third-Party Relationships

Subprocessors must be identified, assessed, managed, and monitored. Subprocessors that provide material services, or that support Zoom's provision of material services to Customers, must comply with control requirements no less stringent than those outlined in this document.

15.1. *Selection and Oversight*. Zoom must have a process to identify subprocessors providing services to Zoom; these subprocessors must be disclosed to Customer and approved to the extent required by this Agreement.

15.2. *Lifecycle Management*. Zoom must establish contracts with subprocessors providing material services; these contracts should incorporate security control requirements, including data protection controls and notification of security and privacy breaches must be included. Review processes must be in place to ensure subprocessors' fulfillment of contract terms and conditions.

16. Standard Builds

Production systems must be deployed with appropriate security configurations and reviewed periodically for compliance with Zoom's security policies and standards.

16.1. *Secure Configuration Availability*. Standard security configurations must be established and security hardening demonstrated. Process documentation must be developed, maintained, and under revision control, with management oversight, on a periodic basis. Configurations must include security patches, vulnerability management, default passwords, registry settings, file directory rights and permissions.

16.2. *System Patches*. Security patch process and procedures, to include requirements for timely patch application, must be documented.

16.3. *Operating System*. Versions of operating systems in use must be supported and respective security baselines documented.

16.4. *Desktop Controls*. Systems must be configured to provide only essential capabilities. The ability to write to removable media must be limited to documented exceptions.

17. Application Security

Zoom must have an established software development lifecycle for the purpose of defining, acquiring, developing, enhancing, modifying, testing, or implementing information systems. Zoom must ensure that web-based and mobile applications used to store, receive, send, control, or access Customer Personal Data are monitored, controlled, and protected.

17.1. *Functional Requirements*. Applications must implement controls that protect against known vulnerabilities and threats, including Open Web Application Security Project (OWASP) Top 10 Risks and denial of service (DDOS) attacks.
17.2. Application layer controls must provide the ability to filter the source of malicious traffic.
17.3. Restrictions must also be placed on or in front of web server resources to limit denial of service (DoS) attacks.
17.4. Zoom must monitor uptime on a hosted web or mobile application.
17.5. Software Development Life Cycle. A Software Development Life Cycle (SDLC) methodology, including release management procedures, must be documented, reviewed, approved, and version-controlled, with management oversight, on a periodic basis. These must include activities that foster the development of secure software.
17.6. Testing and Remediation. Software executables related to client/server architecture that are involved in handling Customer Personal Data must undergo vulnerability assessments (both the client and server components) prior to release and on an on-going basis, either internally or using external experts, and any gaps identified must be remediated in a timely manner.
17.6.1. Testing must be based on, at a minimum, the OWASP Top 10 risks (or the OWASP Mobile Top 10 risks, where applicable), or comparable replacement.
17.7. Zoom must conduct penetration testing on an annual basis.

18. Vulnerability Monitoring

Zoom must continuously gather information and analyze vulnerabilities in light of existing and emerging threats and actual attacks. Processes must include vulnerability scans, anti-malware, Intrusion Detection Systems (IDS)/Intrusion Prevention Systems (IPS), logging and security information and event management analysis and correlation.

18.1. *Vulnerability Scanning and Issue Resolution*. Vulnerability scans (authenticated and unauthenticated) and penetration tests must be performed against internal and external networks and applications periodically and prior to system provisioning for production systems that process, store or transmit Customer Data.
18.2. *Malware*. In production, Zoom must employ tools to detect, log, and disposition malware.
18.3. *Intrusion Detection/Advanced Threat Protection*. Network and host-based intrusion detection/advanced threat protection must be deployed with events generated fed into centralized systems for analysis. These systems must accommodate routine updates and realtime alerting. IDS/advanced threat protection signatures must be kept up to date to respond to threats.
18.4. *Logging and Event Correlation*. Monitoring and logging must support the centralization of security events for analysis and correlation. Organizational responsibility for responding to events must be defined. Retention schedule for various logs must be defined and followed.

19. Cloud Technology

Adequate safeguards must ensure the confidentiality, integrity, and availability of Customer Personal Data stored, processed or transmitted using cloud technology (either as a cloud customer or cloud provider, to include subprocessors), using industry standards.

19.1. *Audit Assurance and Compliance*. The cloud environment in which data is stored, processed or transmitted must be compliant with relevant industry standards and regulatory restrictions.
19.2. *Application and Interface Security*. Threat modeling should be conducted throughout the software development lifecycle, including vulnerability assessments, including Static/Dynamic

scanning and code review, to identify defects and complete remediations before hosting in cloud environments.

19.3. *Business Continuity Management and Operational Resiliency*. Business continuity plans to meet recovery time objectives (RTO) and recovery point objectives (RPO) must be in place.

19.4. *Data Security and Information Lifecycle Management*. Proper segmentation of data environments and segregation must be employed; segmentation/segregation must enable proper sanitization, per industry requirements.

19.5. *Encryption and Key Management*. All communications must be encrypted in-transit between environments.

19.6. *Governance and Risk Management*. Comprehensive risk assessment processes and centralized monitoring that enables incident response and forensic investigation must be used to ensure proper governance and oversight.

19.7. *Identity and Access Management.* Management of accounts, including accounts with privileged access, must prevent unauthorized access and mitigate the impacts thereof.

19.8. *Infrastructure and Virtualization Security*. Controls defending against cyberattacks, including the principle of least privilege, baseline management, intrusion detection, host/network-based firewalls, segmentation, isolation, perimeter security, access management, detailed data flow information, network, time, and a SIEM solution must be implemented.

19.9. *Supply Chain Management, Transparency and Accountability*. Zoom must be accountable for the confidentiality, availability and integrity of production data, to include data processed in cloud environments by subprocessors.

19.10. *Threat and Vulnerability Management*. Vulnerability scans (authenticated and unauthenticated) must be performed, both internally and externally, for production systems. Processes must be in place to ensure tracking and remediation.

20. Audits

At least annually, Zoom will conduct an independent third-party review of its security policies, standards, operations, and procedures related to the Services provided to Customer. Such review will be conducted in accordance with the AICPA's Statements on Standards for Attestation Engagements (SSAE), and Zoom will be issued a SOC 2 Type II report. Upon Customer's request, Zoom will provide Customer with a copy of the SOC 2 Type II report within thirty (30) days. If applicable, Zoom will provide a bridge letter to cover time frames not covered by the SOC 2 Type II audit period scope within 30 days, upon request by Customer. If exceptions are noted in the SOC 2 Type II audit, Zoom will document a plan to promptly address such exceptions and shall implement corrective measures within a reasonable and specific period. Upon Customer's reasonable request, Zoom will keep Customer informed of progress and completion of corrective measures.

20.1. Customer shall rely on the third-party audit SOC 2 Type II report for validation of proper information security practices and shall not have the right to audit, unless such right is granted under applicable law, except in the case of a Security Breach resulting in a material business impact to Customer. If Customer exercises the right to audit as a result of a Security Breach, such audit shall be within the scope of the Services. Customer will provide Zoom a minimum of thirty (30) days of notice prior to the audit. Zoom shall have the right to approve any third-party Customer may choose to conduct or be involved in the audit.

21. Specific Measures

Measure	Description
Measures of pseudonymisation and encryption of personal data	• *Optional End-to-End Encryption for Meetings:* Users may choose to enable end-to-end encryption for Zoom meetings. This provides a high level of security since no third party — including Zoom — has access to the meeting's private keys. • *Default Encryption:* The connection between a given device and Zoom is encrypted by default, using a mixture of TLS 1.2+ (Transport Layer Security), Advanced Encryption Standard (AES) 256-bit encryption, and SRTP (Secure Real-time Transport Protocol). The precise methods used depend on whether a user uses the Zoom client, a web browser, a third-party device or service, or the Zoom phone product. For further information, please see our Encryption Whitepaper.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	Zoom utilizes security measures to ensure the ongoing confidentiality, integrity, availability, and resilience of our processing systems and services.
Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	Zoom takes measures to facilitate the restoration of availability and access to our processing systems and services promptly in the event of a physical or technical incident.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing	Zoom implements a process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures to ensure the security of the data we process.

Measures for user identification and authorisation	• *Protections against unauthorised meeting participants:* Zoom has implemented numerous safeguards and controls to prohibit unauthorized participants from joining meetings:
	  • Eleven (11) digit unique meeting IDs
	  • Complex passwords
	  • Waiting rooms with the ability to automatically admit participants from your domain name or another selected domain
	  • Meeting lock feature that can prevent anyone from joining the meeting
	  • Ability to remove participants
	  • Authentication profiles that only allow entry to registered users, or restrict to specific email domains

Measures for the protection of data during transmission	• *Optional End-to-End Encryption for Meetings:* Users may choose to enable end-to-end encryption for Zoom meetings. This provides a high level of security since no third party — including Zoom — has access to the meeting's private keys. • *Default Encryption:* The connection between a given device and Zoom is encrypted by default, using a mixture of TLS 1.2+ (Transport Layer Security), Advanced Encryption Standard (AES) 256-bit encryption, and SRTP (Secure Real-time Transport Protocol). The precise methods used depend on whether a user uses the Zoom client, a web browser, a third-party device or service, or the Zoom phone product. For further information, please see our Encryption Whitepaper.
Measures for the protection of data during storage	• *Cloud Recording Storage:* Cloud Recordings are processed and stored in Zoom's cloud after the meeting has ended; these recordings can be

	passcode-protected or available only to people in your organization. If a meeting host enables cloud recording and audio transcripts, both will be stored encrypted. • *File transfer storage:* If a meeting host enables file transfer through in-meeting chat, those shared files will be stored encrypted and will be deleted within 31 days of the meeting. • *Cloud recording access*: Recording access for a meeting is limited to the meeting host and account admin. The meeting/webinar host authorizes others to access the recording with options to share publicly, internal-only, add registration to view, enable/disable ability to download, and an option to protect the recording. • *Authentication:* Zoom offers a range of authentication methods such as SAML, Google Sign-in and Facebook Login, and/or Password based which can be individually enabled/disabled for an account. • *2-Factor Authentication ("2FA"):* Admins can enable 2FA for your users, requiring them to set up and use 2FA to access the Zoom web portal.
Measures for ensuring physical security of locations at which personal data are processed	Controls are in place to protect systems against physical penetration by malicious or unauthorized people, damage from environmental contaminants and electronic penetration through active or passive electronic emissions.
Measures for ensuring events logging	Zoom implements a standard requiring all systems to log relevant security access events.
Measures for ensuring system configuration, including default configuration	Zoom implements a standard specifying the minimum requirements for configuration management as it applies to Zoom's corporate and commercial environment.
Measures for internal IT and IT security governance and management	Zoom implements policies and standards governing internal IT and IT security governance and management.

Measures for certification/assurance of processes and products	Zoom implements a Security Audit and Accountability policy.
Measures for ensuring data minimisation	Zoom implements a privacy review in its software development lifecycle to align product development with the principle of data minimization.
Measures for ensuring data quality	Zoom implements a System and Information Integrity Policy.
Measures for ensuring limited data retention	We retain personal data for as long as required to engage in the uses described in our Privacy Statement, unless a longer retention period is required by applicable law. The criteria used to determine our retention periods include the following: • The length of time we have an ongoing customer relationship; • Whether account owners modify or their users delete information through their accounts; • Whether we have a legal obligation to keep the data (for example, certain laws require us to keep records of your transactions for a certain period of time before we can delete them); or • Whether retention is advisable in light of our legal position (such as in regard to the enforcement of our agreements, the resolution of disputes, and applicable statutes of limitations, litigation, or regulatory investigation).
Measures for ensuring accountability	Zoom implements a Security Audit and Accountability policy.
Measures for allowing data portability and ensuring erasure]	Zoom's paying customers can access their account data through their dashboard.

Data importer

The data importer is a provider of communication software, services, systems, and/or technologies.