Zoom Datenschutzerklärung

Diese Datenschutzerklärung soll Ihnen ermöglichen, sich über die Verarbeitung Ihrer personenbezogenen Daten bei Nutzung des Tools „Zoom“ der Zoom Video Communications, Inc. zu informieren. Die Fahrschule Gärtling bietet zur Bewältigung der aktuellen SARS-CoV-2-Krisensituation die Durchführung von Online-Vorlesungen und Online- Seminaren über den Online-Meeting-Dienst Zoom an.

Informationen nach Art. 13/14 EU-Datenschutz-Grundverordnung (DS-GVO) zum Einsatz des "Video-Konferenzsystems Zoom“ an der Fahrschule Gärtling Stand: 15.04.2021

Im Gegensatz zu anderen auf dem Markt angebotenen Systemen liefert ZOOM eine sehr hohe Qualität und Funktionalität, ist insbesondere bei großen Gruppen zuverlässig einsetzbar, in der Bedienung anwenderfreundlich und transparent und bietet eine große Anzahl an datenschutzfreundlichen Einstellungsmöglichkeiten. .

Der Schutz Ihrer personenbezogenen Daten ist der Fahrschule Gärtling ein wesentliches Anliegen. Daher hat die Fahrschule alles ihr Mögliche unternommen, um die Datenverarbeitung bei der Nutzung von ZOOM den gesetzlichen Vorgaben entsprechend, sicher, transparent und datensparsam zu gestalten. Diese Datenschutzerklärung ermöglicht es Ihnen, sich über die Verarbeitung Ihrer personenbezogenen Daten bei der Nutzung von ZOOM ausführlich zu informieren.

Datenschutzerklärung

I. Verantwortlicher

Verantwortlicher für die Datenverarbeitung im Sinne der DS-GVO sowie anderer datenschutzrechtlicher Bestimmungen ist:

Rolf Gärtling

Fahrschule

Schenkenseestraße 2

74523 Schwäbisch Hall

II. Auftragsverarbeiter

Die ZOOM Video Communications, Inc., 55 Almaden Boulevard, 6th Floor, San Jose, CA 95113, ist als Auftragsverarbeiter im Sinne von Artikel 28 DS-GVO für die Fahrschule Gärtling tätig

III. Verarbeitung personenbezogener Daten

Die Form der Datenverarbeitung hängt davon ab, wie der Dienst genutzt wird. ZOOM ermöglicht eine flexible Gestaltung der Online-Meetings. Als Host oder Moderator werden die in Ihrem ZOOM-Account hinterlegten personenbezogenen Daten zur Verwaltung der ZOOM-Räume verarbeitet. Als Teilnehmer*in können Sie darüber entscheiden, ob Sie am Chat teilnehmen oder ob Sie Ihr Mikrofon bzw. Ihre Kamera freigeben. In der Regel werden bei der Nutzung von ZOOM folgende Daten mit Personenbezug verarbeitet:

1. **Benutzer*innen-Daten**

2. **Video-, Audio- und Textdaten**

    1. Videodaten, sofern Sie die Kamera Ihres Endgeräts freigegeben haben
    2. Audiodaten, sofern Sie das Mikrofon Ihres Endgeräts freigegeben haben
    3. Textdaten, sofern die Chat-, Fragen- oder Umfragefunktion genutzt wird

3. **Meeting-Metadaten**

    1. Dauer des Meetings
    2. Beginn und Ende (Zeit) der Teilnahme von Personen
    3. Name und Beschreibung des Meetings
    4. Geplantes Datum / Uhrzeit des Meetings
    5. Chat-Status
    6. IP-Adressen der zur Teilnahme verwendeten Endgeräte sowie weitere Geräte-/Hardware-Informationen (MAC-Adresse, andere Geräte-IDs (UDID), Gerätetyp, Betriebssystemtyp und -version, Client-Version, Kameratyp, Mikrofon oder Lautsprecher, Art der Verbindung u.a.), ungefähre Position zur Herstellung einer Verbindung zum nächstgelegenen ZOOM-Rechenzentrum

4. **Meeting-Aufzeichnungen (optional)**

    1. mp4 aller Video- und Audioaufnahmen und Präsentationen
    2. m4a aller Audioaufnahmen
    3. Textdatei aller Annotationen, Chats, Audio-Protokolldatei
    4. Audio-Protokolldatei und andere Informationen, die während der Nutzung des Dienstes geteilt werden.

Video- und Audiodaten enthalten jedenfalls Ihr Abbild sowie Ihre Stimme als personenbezogene Daten im Sinne des Artikel 4 Nummer 1 DS-GVO, da sich die Daten auf Sie als identifizierte bzw. identifizierbare natürliche Person beziehen. Darüber hinaus kann der Inhalt Ihrer Beiträge Rückschlüsse auf Ihre Person zulassen. Auch IP-Adresse und Geräte-/Hardware-Informationen können einen Rückschluss auf Ihre Person zulassen und sind daher als personenbezogene Daten zu behandeln. Bei einer Nutzung von ZOOM mit privaten Endgeräten, sind Sie bei Nutzung einer VPN-Verbindung anhand der nach Ziffer 3f übermittelten Daten außerhalb der Fahrschule nicht identifizierbar.

Die bei Zoom verfügbare „Aufmerksamkeitsüberwachung“ ist deaktiviert. Der Text innerhalb der Chatfunktion wird in einer separaten Datei gespeichert und ist im Falle einer Aufzeichnung nicht Teil des Videos.

Weitere Informationen zur Datenverarbeitung bei Zoom-Nutzung können Sie unter https://zoom.us/de-de/privacy.htmlsowie https://zoom.us/docs/de-de/privacy-and-security.html abrufen. Bitte beachten Sie, dass es sich dabei um eine externe Website handelt, die

von der Zoom Video Communications, Inc. in eigener Verantwortlichkeit betrieben wird und bei deren Besuch personenbezogene Daten verarbeitet werden.

IV. Rechtsgrundlage

Die Fahrschule Gärtling setzt ZOOM sowohl in den Bereichen Studium und Lehre, Wissenschaft und Forschung als auch im Rahmen der Verwaltung sowie Presse- und Öffentlichkeitsarbeit ein. Die einschlägige Rechtsgrundlage für die Datenverarbeitung richtet sich nach dem jeweiligen Einsatzgebiet. Dabei verarbeitet die Fahrschule personenbezogene Daten von Fahrschüler:innen sowie ggf. Externen für die Teilnahme an Online-Unterricht.

Die Verarbeitung dieser Daten ist zur Erfüllung der im öffentlichen Interesse liegenden Aufgaben der Fahrschule sowie zur Erfüllung einer rechtlichen Verpflichtung der Fahrschule erforderlich. Rechtsgrundlage ist Artikel 6 Absatz 1 Unterabsatz 1 lit. c), e), Absatz 3 DS-GVO i.V.m.

Personenbezogene Daten von Fahrschüler:innen sowie Beschäftigten verarbeitet die Fahrschule, soweit dies zur Eingehung, Durchführung, Beendigung oder Abwicklung des jeweiligen Dienst- oder Arbeitsverhältnisses oder zur Durchführung innerdienstlich planerischer, organisatorischer, personeller, sozialer oder haushalts- und kostenrechnerischer Maßnahmen, insbesondere zu Zwecken der Personalplanung und des Personaleinsatzes, erforderlich oder in einer Rechtsvorschrift, einem Tarifvertrag oder einer Dienst- oder Betriebsvereinbarung (Kollektivvereinbarung) vorgesehen ist.

Die Rechtsgrundlage für die Verarbeitung von personenbezogenen Daten, die Sie optional von sich preisgeben können, ist Ihre Einwilligung gemäß Artikel 6 Absatz 1 Unterabsatz 1 lit. a), 7 DS-GVO.

V. Speicherung

Die oben angegebenen Daten werden solange verarbeitet, wie es für die Durchführung der Online-Meetings und damit zusammenhängender Services erforderlich ist. Das gilt nicht, sofern abweichend da-von ein längerer Speicher- oder Aufbewahrungszeitraum gesetzlich vorgeschrieben oder für die Rechts-durchsetzung innerhalb der gesetzlichen Verjährungsfristen erforderlich ist.

Wird ein Online-Meeting aufgezeichnet, erfahren Sie dies über eine Vorankündigung der Organisato-rin/des Organisators und/oder über eine technische Signalisierung. Sie können Ihre Kamera und ihr Mik-rofon selbstständig deaktivieren und das Meeting jederzeit verlassen. Mit der Aufzeichnung werden die Daten des Audio- und Videostreams sowie optional die Nachrichten in der Chat-, Fragen- oder Umfragefunktion gespeichert und bleiben über die Dauer des Meetings hinaus gespeichert. Die auf den Cloudser-ver des Anbieters von ZOOM gespeicherten Daten werden nach spätestens 30 Tagen automatisch ge-löscht. Soweit Online-Meetings nicht aufgezeichnet werden, speichert der Anbieter die Meeting-Inhalte nach eigenen Angaben nach Abschluss des Meetings nicht.

Wenn Sie mit einem ZOOM-Account angemeldet sind, können Berichte über „Online-Meetings“ (Meeting-Metadaten, Daten zur Telefoneinwahl, Fragen und Antworten in Webinaren, Umfragefunktion in Webina-ren) bis zu einem Monat bei ZOOM gespeichert werden.

VI. Datenverarbeitung außerhalb der EU / des EWR

Aktuell ist es noch nicht möglich, ZOOM so zu konfigurieren, dass alle oben unter III. angegeben Daten aus-schließlich in Rechenzentren innerhalb der EU / des EWR verarbeitet werden. Die unter III. 1. 3 aufgeführten Meeting-Metadaten werden weiterhin in Rechenzentren in den USA verarbeitet. Die Übermittlung der Meeting-Metadaten in die USA erfolgt auf Grundlage der zwischen ZOOM und der Fahrschule geschlossenen Standard-Vertragsklauseln (SCC) der EU-Kommission (Artikel 46 Absatz 2 lit. c) DS-GVO). Dazu sind ZOOM und die Fahrschule dabei, eine weitere Vereinbarung zu den

SCC mit zusätzlichen Garantien nach den Vorgaben des Landesbeauftragten für Datenschutz und Informationsfreiheit abschließen.

Nach den Angaben von ZOOM ist die Übermittlung der Daten notwendig, um die Auslastung der ZOOM-Server zu kontrollieren. Ohne diese Kontrolle kann der Service nicht zuverlässig zur Verfügung gestellt werden. In Europa konnte die dafür erforderliche Infrastruktur bisher nicht aufgebaut werden, was perspektivisch aber geplant ist. Wenn Sie die Übermittlung der Meeting-Metadaten einschränken möchten, empfehlen wir Ihnen, sich bei ZOOM-Meetings mit einem Pseudonym anzumelden, das keine Rückschlüsse auf Ihren Namen oder Ihre Person zulässt und über eine VPN-Verbindung teilzunehmen.

VII. Empfänger

Interne Empfänger sind diejenigen Beschäftigten der Fahrschule, die die Daten für ihre Tätigkeit im Rahmen der Aufgabenerfüllung benötigen. Weitere Empfänger existieren für den Fall, dass wir gesetzlich zu einer Weitergabe verpflichtet sind.

Externe Empfänger der Daten, die Sie im Rahmen des Online-Meetings preisgeben, sind auch die anderen Teilnehmer*innen des Online-Meetings.

Als Auftragsverarbeiter verarbeitet die ZOOM Video Communications, Inc. im Rahmen des Auftragsverarbeitungsverhältnisses Ihre Daten im oben geschilderten Umfang.

VIII. Verschlüsselung

Dazu bietet ZOOM neben einer Transportverschlüsselung inzwischen auch die Möglichkeit einer Ende-zu-Ende-Verschlüsselung (E2EE) der Verbindung an. Bitte machen Sie, insbesondere bei Meetings mit sensiblen Gesprächsinhalten, von dieser Möglichkeit Gebrauch oder bitten den Host/Veranstalter, das Meeting entsprechend anzulegen. Weitere Informationen zu E2EE finden Sie hier: https://blog.zoom.us/de/zoom-rolling-out-end-to-end-encryption-offering/

IX. Datenverarbeitung in der Cloud

ZOOM hat sich gegenüber der Fahrschule zu einer datenschutzkonformen Verarbeitung personenbezogener Daten verpflichtet. Dazu hat die Fahrschule alles ihr Mögliche unternommen, um die Datenverarbeitung den gesetzlichen Vorgaben entsprechend, sicher, transparent und sparsam zu gestalten. Dennoch bleibt zu beachten, dass die Fahrschule bei der Nutzung von externen Cloud-Diensten grundsätzlich keinen direkten Einfluss auf die Sicherheit der Datenverarbeitung nehmen kann und insofern auf die Compliance des Vertragspartners angewiesen ist. Daher sollten Sie bei der Nutzung nicht unnötig viele bzw. vertrauliche Daten von sich preiszugeben und wenn möglich auf die Fahrschuleseigenen Dienste wie BigBlueButton oder AdobeConnect zurückzugreifen.

X. Ihre Rechte

Hinsichtlich der Sie betreffenden personenbezogenen Daten haben Sie folgende Rechte:

1. Recht auf Widerruf Ihrer Einwilligung mit Wirkung für die Zukunft (Artikel 7 Absatz 3 DS- GVO)
2. Recht auf Bestätigung, ob Sie betreffende Daten verarbeitet werden und auf Auskunft über die verarbeiteten Daten, auf weitere Informationen über die Datenverarbeitung sowie auf Kopien der Daten (Artikel 15 DS-GVO)
3. Recht auf Berichtigung oder Vervollständigung unrichtiger bzw. unvollständiger Daten (Ar-tikel 16 DS-GVO)

4. Recht auf unverzügliche Löschung der Sie betreffenden Daten (Artikel 17 DS-GVO)
5. Recht auf Einschränkung der Verarbeitung (Artikel 18 DS-GVO)
6. Recht auf Erhalt der Daten in einem strukturierten, gängigen und maschinenlesbaren Format, sofern die Verarbeitung auf einer Einwilligung gemäß Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe a oder Artikel 9 Absatz 2 lit. a) oder auf einem Vertrag gemäß Artikel 6 Absatz 1 Unterabsatz 1 lit. b) beruht und keine Ausnahme vorliegt (Artikel 20 DS-GVO)
7. Sie haben zudem das Recht, sich bei einer Aufsichtsbehörde über die Verarbeitung der Sie betreffenden personenbezogenen Daten durch die Fahrschule Gärtling zu beschweren (Ar-tikel 77 DS-GVO).

XI. Widerspruchsrecht nach Art. 21 DS-GVO

Sie haben ein Recht auf Widerspruch gegen die künftige Verarbeitung der Sie betreffenden Daten, sofern die Daten nach Maßgabe von Artikel 6 Absatz 1 Unterabsatz 1 lit. e) oder f) DS-GVO verarbeitet werden.

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 and the Agreement, the terms and conditions of this Addendum shall supersede and control to the extent of such conflict.

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 Agreement, "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, 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 or the United Kingdom ("**UK**"), 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.

1.3. "**Authorized Subprocessor**" means a subprocessor engaged by Processor who agrees to receive Personal Data from Processor exclusively for Processing activities to be carried out on behalf of Customer per Customer instructions, the terms of this Addendum and the terms of the written subcontract; and who is authorized by Customer to do so under Section 5 of 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. "**Customer**" means the contracting party set out below in the signature line.

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

1.7. "**Instruction**" means a documented direction issued by Customer to Zoom and directing Zoom to Process Personal Data.

1.8. "**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. For the avoidance of doubt, Personal Data excludes anonymous data and includes Sensitive Personal Information.

1.9. "**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise processed.

1.10. "**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.

1.11. "**Processor**" means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Controller. Processor or "data importer" in this Agreement refers to Zoom.

1.12. "**Sale of Personal Data**" means the disclosure of Personal Data to any Third Party in exchange for monetary or other valuable consideration, except that Zoom's disclosure of personal data to a service provider for a business purpose, subject to a written agreement that requires the service provider to take data protection measures at least as protective as those applicable to Zoom under this Addendum, shall not qualify as the Sale of Personal Data.

1.13. "**Sensitive Personal Information**" means a Data Subject's (i) government-issued identification number (including social security number, driver's license number or state-issued identification number); (ii) financial account number, credit card number, debit card number, credit report information, with or without any required security code, access code, personal identification number or password, that would permit access to an individual's financial account; (iii) genetic and biometric data or data concerning health; or (iv) Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation, criminal convictions and offences (including commission of or proceedings for any offense committed or alleged to have been committed), or trade union membership.

1.14. "**Services**" means the various video conferencing, web conferencing, webinar, meeting room, screen sharing, and other collaborative services as well as voice connectivity services and shall have the meaning set forth in the Agreement.

1.15."**Standard Contractual Clauses**" means the agreement executed by and between Customer and Zoom and attached hereto as EXHIBIT C pursuant to the European Commission's decision (C(2010)593) of February 5, 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of protection as amended, superseded or replaced from time to time in accordance with this Addendum .

1.16. "**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.

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, the Zoom Privacy Statement, available at https://zoom.us/privacy, will apply. Zoom will Process such data in compliance with Applicable Data Protection Laws and the Technical and Organizational Security Measures set out in Exhibit B.

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 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 Personal Data on behalf of the Customer only (i) to perform the Agreement and as set out in EXHIBIT A; (ii) under the terms and conditions outlined in this Addendum and the Zoom Privacy Statement, available at https://zoom.us/privacy, and (iii) any other documented Instructions provided by Customer; including concerning transfers of 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 Personal Data.

3.3. Zoom shall immediately notify the Customer, wherein its 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 to this Addendum. Following the completion of the Services, at Customer's choice, Zoom shall either enable Customer to delete all 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 Personal Data from any further Processing (except to the extent necessary for its continued hosting or Processing required by law, rule or regulation) and shall continue to appropriately protect the Personal Data remaining in its possession, custody, or control and, where any Authorized Subprocessor continues to possess 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 the 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. Zoom shall not engage a subprocessor without general written authorization of the Customer.

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 at its own discretion in accordance with this Section 5.3:

5.3.1. Zoom shall at least fifteen (15) days before enabling any new subprocessors to access or participate in the Processing of 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 an engagement, 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 Controller'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 owed to Zoom 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 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 an organization's data protection practices before allowing the organization 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 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), (i) the above authorizations will constitute Customer's prior written consent to the subcontracting by Zoom 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 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 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 from the EU**

7.1. Customer acknowledges and agrees that Zoom may transfer and process 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 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 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 set forth in EXHIBIT C to this Addendum. Where the Standard Contractual Clauses apply, Zoom and Customer agree that:

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 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. For the avoidance of doubt, when the European Union law ceases to apply to the UK upon the end of the UK Brexit Withdrawal Agreement and the UK is deemed to provide adequate protection for Personal Data (within the meaning of applicable European Data Protection Law) then to the extent Zoom processes (or causes to be processed) any Personal Data on behalf of the Customer that is protected by European Data Protection Law applicable to EEA and Switzerland in the United Kingdom, Zoom shall process such data in compliance with the Standard Contractual Clauses or any applicable Alternative Transfer Mechanism implemented in accordance with Section 7.4.

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. **Assistance, 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 at Zoom, or at a Sub-Processor of Zoom, that relates to Customer's Personal Data, 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 or European or US 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, 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 Annex (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 Agreement, which 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.

EXHIBIT A

Details of Processing

Nature and Purpose of Processing: Zoom will Process Personal Data on behalf of Customer for the purposes of providing the Services in accordance with the Agreement.

Duration of Processing: The term of the Agreement plus the period until Zoom deletes all Personal Data processed on behalf of Customer in accordance with the Agreement.

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 employees, contractors, and end-users.

Type of Personal 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 (incl image sharing)

EXHIBIT B

Technical and Organizational Security Measures

Zoom's technical and organizational security measures for Processing Customer Personal Data in Customer Content, Customer Operation Data and Customer Account Data will meet the Minimum-Security Control Requirements set out in this Exhibit B ("**Minimum Control Requirements**"). These Minimum Control Requirements are stated at a relatively high level. 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 Minimum Control Requirements from time to time. The term "should" in these Minimum Control Requirements 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 Minimum Control Requirements, (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 this 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 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 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 Customer Personal Data, including Customer 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 post-implementation 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 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 real-time 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.

EXHIBIT C

Customer should complete and execute EXHIBIT C if it will transfer Personal Data to Zoom directly from a Member State of the European Union, Iceland, Liechtenstein, Norway, Switzerland or the United Kingdom. This EXHIBIT D cannot be modified in any way. Please leave EXHIBIT C blank (and DO NOT SIGN) if Customer's use of Zoom's services will not involve Customer transferring Personal Data to Zoom from any of the countries mentioned above.

Standard Contractual Clauses

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

Name of the data exporting organisation: ……

Address: ……

Tel.: ……; fax: ……; e-mail: ……

Other information needed to identify the organisation:

……

(the data **exporter**)

And

Name of the data importing organisation: Zoom Video Communications, Inc.

Address: 55 Almaden Blvd. Suite 600, San Jose, CA 95113

Tel.: 1.888.799.9666; fax: none; e-mail: privacy@zoom.us

Other information needed to identify the organisation: not applicable

……

(the data **importer**)

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995

on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC Processor;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organizational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1, which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of

which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transferor to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the

personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

  (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

  (ii) any accidental or unauthorised access, and

  (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case, the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business-related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses[1]. Where the subprocessor fails to fulfil its data protection obligations under such written agreement, the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph

---

[1] This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this Decision.

1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter

The data exporter is a customer or other user of the data importer's communication software, services, systems, and/or technologies.

Data importer

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

Data subjects

Individuals about whom data is provided to Processor via the Services by (or at the direction of) Controller or Controller's end users, including without limitation Controller's employees, consultants, contractors, agents, and end-users

Categories of data

Any 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 and presentations, M4A of all Audio, Text file of all in meeting chats, Audio transcript file
- **In-Meeting Chat Logs**
- **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 or Webinar details: title, date and 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
- **Meeting and Webinar Invitee/Participant Details:** screen name and meeting invitation and attendance details of meeting or webinar invitees or participants.

Special categories of data (if appropriate)

Special categories of data are not required to use the service. The data exporter may submit special categories of data to Customer, the extent of which is determined and controlled by the 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.

Processing operations

The personal data transferred may be subject to the following basic 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

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

Please see EXHIBIT B for a description of Zoom's Security Measures.