Annex 1 – Service Description

1. Service Description

Provision of support for Zoom’s web meeting and video conferencing platform.

2. Scope

i. Mitel under an Agreement has resold to Customer, Zoom’s web meetings and video conferencing platform (“Platform”). Mitel would as part of the resale provide support services to Customer with Zoom Video Communications, Inc. providing escalation support where applicable.

ii. The DPA and all annexes apply to Mitel’s Processing of Customer Personal Data for the provision of support to Customer.

Annex 2 –Details of Personal Data and Processing Activities

Explanatory note: section (A) deals with Mitel's processing of Customer Personal Data as processor to Customer in providing first level support to Customer in relation to the Zoom web meeting and video conferencing platform. Section (B) deals with Zoom's processing of Customer Personal Data in providing escalation support as sub-processor to Mitel. We have split these into different sections because Zoom processes a wider scope of Customer Personal Data as sub-processor. A DPA is available between Zoom and Customer for the delivery of the Zoom web meeting and video conferencing platform.

1. For support services related to the use of the Zoom platform, the following shall apply:
(A). Details of processing and transfer of Customer Personal Data by Mitel

1. Categories of Personal Data:

i. Data required to provide support such as:

A. first name, last name, phone number, job title, address email address, photo, geographic location, username and password;

B. inbound and outbound call logs (or CPNI information), Meeting ID, Engagement ID, email and text message communications, recorded calls, inbound and outbound faxes, voicemails, meeting information, chat histories, calendar data, personal contacts, birthdate, user-saved or stored content shared among users;

C. IP addresses, service set-up information, service configurations and settings;

D. Support issue reported.

ii. Special categories of data (if appropriate): Special categories of data are not required to use the Zoom service or for Mitel to provide the support services. Customer can prevent the processing of these data by using end to end encryption in the meetings and preventing End Users from uploading profile information that contains such special categories of data.

2. Frequency of the transfer: continuous
3. Nature of the processing: to provide the Support Services
4. Categories of data subjects: end users
5. Purpose of Processing and transfers. Mitel will only process Customer Personal Data for the purposes of providing the support services, including resolving issues, bugs, and errors and applying knowledge gained from individual customer support requests to benefit all customers but only to the extent such knowledge is anonymized. Mitel will only transfer Customer Personal Data to Zoom and other subprocessors to the extent necessary to provide the support services.
6. Duration of Processing. To the extent that Customer Personal Data is transferred to Mitel, unless otherwise required by law, Mitel will only retain the Customer Personal Data as long as necessary for Mitel to provide the support services and will take reasonable steps to permanently delete the Customer Personal Data as soon as reasonably practicable upon resolution of issue leading to such support services.

(B) Details of processing of Customer Personal Data by Zoom as a sub processor:

1. Categories of Personal Data.:

i. Data required to provide support comprising the Personal Data referred to in Section A of this Annex 1 and the following:

Customer Content Data:

Zoom Account Profile Info: Data associated with the End User’s Zoom account, profile picture, password, company name, and Customer’s preferences. This includes:

- Zoom unique user ID,
- social media login (optional),
- profile picture (optional) and
- display name.

Customer authentication data: This includes username and password unless Single Sign On (SSO) is used.

Meeting and webinar communication content. This includes:

- video, audio, whiteboard, captions, and presentations
- in-meeting Questions & Answers, polls, and survey information
- closed captioning (Live Transcription)

Chat Messages. 1:1 in-meeting and group chat messages that are not transferred to a permanent chat channel.

Customer Initiated cloud recordings. This includes the following recordings if such a recording is permitted by the Customer administrator controls and selected by a meeting host or participant:

- video recording of video, audio, whiteboard, captions, and presentations
- audio recording
- text file of all in meeting group chats
- audio transcript text file
- in-meeting Questions & Answers, polls, and survey information
- closed captioning transcripts

Meeting and webinar participant information. This includes:

- registered participant name and contact details; and any data requested by Customer to be provided in conjunction with registration, email addresses
- status of participant (as host, as participants in a chat or as attendees)
- room names (if used)
- user categorizations
- tracking fields such as department or group
- scheduled time for a meeting
- topic names

Stored Chat Information. This is data at rest (in storage)

- and includes:
- chat messages
- files exchanged via chat
- images exchanged via chat
- videos exchanged via chat
- chat channel title
- whiteboard annotations

Address book Information. This includes contact

- information made available through Customer
- controlled integrations (e.g. Outlook)

Calendar Information. This includes meeting schedules

- made available through Customer controlled
- integrations (e.g. Outlook, Google Calendar)

Diagnostic Data:

- Meeting metadata: Metrics about Service usage,
- including when and how meetings were conducted).
- This category includes:
- event logs (including action taken, event type and subtype, in-app event location, timestamp, client UUID, user ID, and meeting ID)
- meeting session information, including
- frequency, average and actual duration,
- quantity, quality, network activity, and
- network connectivity
- number of meetings
- number of screen-sharing and non-screen sharing
- sessions
- number of participants
- meeting host information
- host name
- meeting site URL
- meeting start/end Time
- join method

Telemetry data: Data collected from locally installed software (applications and browser information about the deployment of Zoom Services and related systems environment / technical information. This includes:

- PC name
- microphone
- speaker
- camera
- domain
- hard disc ID
- network type
- operating system type and version
- client version
- MAC address
- event logs (including action taken, event type and subtype, in-app event location, timestamp, client UUID, user ID and meeting ID)
- service logs (information on systems events and states)

Other Service Generated Data:

- spam identification
- push notifications
- Zoom persistent unique identifiers such as UUID or user ids that are combined with other data elements including:
- IP address
- Data center
- PC name
- Microphone
- Speaker
- Camera
- Domain
- Hard disc ID
- Network type
- Operating System Type and Version
- Client Version
- IP Addresses along the Network Path

Support Issue Data:

- Contact name of support requestor, time, subject, problem description, post-meeting feedback (thumbs-up/down)

User supplied attachments including recordings,
transcripts or screenshots, post-meeting feedback
(open text provided with thumbs down)

ii Special categories of data (if appropriate): Special categories of data are not required to use the Zoom service. Customer can prevent the processing of this data by using end to end encryption in the meetings and preventing End Users from uploading profile information that contains such special categories of data

2. Nature of the processing: to provide the Support Services
3. Categories of data subjects: end users
4. Frequency of the transfer: continuous
5. Purpose of Processing and transfers. Zoom as subprocessor of Mitel will only process Customer Personal Data for the purposes of providing the support services, including resolving issues, bugs, and errors and applying knowledge gained from individual customer support requests to benefit all customers but only to the extent such knowledge is anonymized. Mitel will only transfer Customer Personal Data to Zoom and other subprocessors to the extent necessary to provide the support services.
6. Duration of Processing. Zoom will only retain the Customer Personal Data as long as necessary for Zoom to provide the support services and will take reasonable steps to permanently delete the Customer Personal Data in compliance with Zoom's data retention and deletion policy.

Annex 3 -Technical and Organizational Security Measures

A. Mitel's Specific Measures

i. Organizational Measures

DPO: Mitel has appointed a Group Data Protection Officer, based in Germany (EU), who shall be responsible for monitoring Mitel's personal data processing activities and providing independent advice on ongoing compliance with applicable data protection laws and regulations. The Group Data Protection Officer leads a global team of international data protection specialists with multidisciplinary expertise in data protection law, AI and digital ethics and experience working across various jurisdictions.

Employee Confidentiality Obligation: Mitel employees are by default obliged to maintain Mitel's business and professional secrets through confidentiality clauses in their employment agreements or may sign a case specific confidentiality agreement, when necessary.

Training and Awareness: All Mitel employees are assigned mandatory global data protection training as part of their onboarding process and receive continuous training annually thereafter. Training completion rate is being tracked and monitored and failure to comply may result in disciplinary action. Mitel Data Protection training is annually reviewed and updated to reflect new legislative and jurisprudential developments. Training includes procedures for handling, transferring and storing Personal Data and how to respond effectively to security events.

Contractor and vendor management: Mitel takes commercially reasonable steps to select and retain only third-party service providers that will provide guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of privacy regulations and ensure the protection of the rights of data subjects.

Data Processing Agreements: Where applicable, Mitel will enter into a Data Protection Agreement with its customers, partners and sub-processors, whereby the roles of the parties and their rights and obligations in terms of personal data processing are clearly defined and contractually agreed.

International Transfers of Personal Data: In case of transfers of personal data outside the EU, and in the absence of an adequacy decision from the EU Commission, Mitel may transfer personal data to a third country or an international organization, by concluding Standard Contractual Clauses (SCCs) in the respective module. For transfers within the Mitel Group, Mitel has executed an Intra-Group Personal Data Transfer Agreement ("Intra-Group Agreement"). The Intra-Group Agreement incorporates the EU Commission 2021 Standard Contractual Clauses and the UK Standard Contractual Clauses.

ii. Technical Measures for Support

Mitel maintains and updates a record of personnel authorized to access systems with Customer Personal Data under its control, or to access systems under customer control.

Laptops and desktops of Mitel employees used to access Customer Personal Data are subject to rules and policies determined and managed by Mitel's IT and Security organization. Rules and policies include running up-to-date antivirus protection, maintaining security patches, and hard-drive encryption ensuring each employee with access to its systems have a single unique identifier/log-in and monitoring repeated attempts to gain access to the information systems using an invalid password. Passwords must be changed regularly and are required to meet minimum strong password complexity. Mitel maintains an information security incident response program that detects and analyses, records, contains eradicates and recovers information security breaches.

Mitel's production, test and development environments are kept separate. All changes to production systems containing Customer Personal Data, or systems accessed containing Customer Personal Data under customer control, are put through Mitel's robust change management process.

Mitel employees working with Customer Personal Data are only permitted to use trusted devices that are configured with security software with automatic security patching, and which enforces the use of strong passwords (length, character and repeatability rules) and force password changes. Employees are instructed to lock computers and disable administrative sessions when leaving premises that are controlled by Mitel or when computers are otherwise left unattended. In addition, employee laptops and desktop computers are set to automatically lock after a period of inactivity. Sharing of user identifiers and passwords is prohibited. Mitel has policies requiring a “clean desk/clear screen” when leaving workstations unattended and at the end of the business day.

Hardcopy and electronic media containing Customer Personal Data are erased or destroyed by crosscut shredding paper, shredding CDs and DVDs, securely erasing and reimaging media for redeployment, or if media is to be decommissioned, securely erasing and if appropriate, physically destroying the media.

B. Zoom as a sub processor Specific Measures:

Measure	Description
Measures for pseudonymization and encryption of personal data	Zoom implements 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. Remote Access. The data flow in the remote connection must be encrypted and multi-factor authentication must be utilized during the login process. Remote connection settings must limit the ability of remote users to access both initiating network and remote network simultaneously (i.e., no split tunneling). Subprocessors’ remote access, if any, must adhere to the same controls and must have valid business justification. Wireless Access. Wireless access to the Zoom corporate network must be configured to require authentication and be encrypted.
Measures for risk management	Zoom performs risk assessments annually to verify the implementation of controls that protect business operations and customer content.
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 its processing systems and services.
Measures for access control	Access rights are 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. Logical Access Control Policy. Documented logical access policies and procedures 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 is uniquely identified. User access reviews is conducted on a periodic basis. Privileged Access. Management of privileged user accounts (e.g., those accounts that have the ability to override system controls), to include service accounts, follow a documented process and is restricted. A periodic review and governance process is maintained to ensure appropriate provisioning of privileged access. Authentication and Authorization. A documented authentication and authorization policy cover all applicable systems. That policy includes 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.

Measures for 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, is in place.
Measures for ensuring the ability to restore 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 its 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 organizational 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 the protection of data during transmission	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	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.
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. 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.
Measures for ensuring data minimization	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. Controls must ensure that any data stored, received, controlled, or otherwise accessed is accurate and reliable.

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.
Third-Party Relationships	Subprocessors are 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. Selection and Oversight. Zoom has a process to identify subprocessors providing services to Zoom; Zoom establishes contracts with subprocessors which incorporates security control requirements, including data protection controls and notification of security and privacy breaches. Review processes are in place to ensure subprocessors' fulfillment of contract terms and conditions.
Technology Asset Management	Procedures are in place to remove data from production systems in which Customer's Personal Data are stored, processed, or transmitted. Where applicable, Zoom uses industry standards to wipe or carry out physical destruction as the minimum standard for disposing of assets. Zoom has documented procedures for disposal or reuse of assets.
Organizational Security	Where legally permissible, background checks (including criminal) are performed on applicable Zoom personnel. Zoom personnel are subject to written non-disclosure or confidentiality obligations. Policies are in place to ensure that information is accessed on a need-to-know basis.
Awareness and Education Program.	Security policies and responsibilities are communicated and socialized within the organization to Zoom personnel. Zoom personnel must receive security awareness training on an annual basis

Annex 4 - Standard Contractual Clauses Details

1. UK Standard Contractual Clauses.

The UK Information Commissioner is the exclusive Supervisory Authority for the transfers of UK Personal Data under this Agreement. The UK SCCs shall be governed by the Laws of England and Wales and the parties submit to the exclusive jurisdiction of the English courts in relation to them.

2. EU Standard Contractual Clauses.

2.1 The parties select the following Standard Contractual Clause Module:

	Module One	(Controller to Controller)
☒	Module Two	(Controller to Processor)
□	Module Three	(Processor to Processor)
	Module Four	(Processor to Controller)

2.2 For each module, where applicable, the parties agree that the following terms apply:

(a) the Data Protection Commission of the country whose laws govern the SCCs pursuant to paragraph (c) below shall be the competent Supervisory Authority;

(b) data subjects for whom Mitel processes Customer Personal Data are third-party beneficiaries under the applicable SCCs;

(c) the SCCs shall be governed by the laws which governs the Agreement provided that such governing law are the laws of a member of the European Union and that it allows for third-party beneficiary rights. If neither of these conditions are satisfied, then the governing law shall be the laws of Germany; and

(d) any dispute arising from the SCCs shall be resolved by the courts of the country whose laws govern the SCCs pursuant to paragraph (c) above.

2.3 Supplementary Measures.

In order to maintain the protection of Personal Data granted in the European Economic Area ("EEA") and the UK, Mitel shall collaborate with Customer in the event of international data transfers from the EEA or from the UK to a third country which is not considered an Adequate Country under applicable Data Protection Laws. For the appropriate safeguards contained in the GDPR and UK GDPR Article 46 transfer tools to be effective, Mitel shall comply with the following supplementary measures -

(a) Challenge law enforcement requests:

i. Mitel will take commercially reasonable efforts to challenge law enforcement requests for EU Customer Personal Data from governmental bodies, whether inside or outside the EEA, where the request conflicts with EU law, is overbroad, or where we otherwise have any appropriate grounds to do so; and

ii. Mitel will take commercially reasonable efforts to challenge law enforcement requests for UK Customer Personal Data from governmental bodies, whether inside or outside the UK, where the request conflicts with UK law, is overbroad, or where we otherwise have any appropriate grounds to do so.

(b) Disclose the minimum amount necessary: Notwithstanding sub (a) above, if Mitel is compelled by a valid and binding legal request to disclose Customer Personal Data, we will disclose only the minimum amount of Customer Personal Data necessary to satisfy the request.

(c) Promptly notify the data exporter/subject of the request or order received from the public authorities of the third country, except were prohibited by law or by court order.

3. China Standard Contractual Clauses (China SCCs)

To the extent that there is a transfer of Customer Personal Data protected and within the scope of the Chinese Data Protection Law to any country outside China, the parties shall sign the China SCCs (a current copy to be provided) separately and fulfil any necessary filing formalities, as applicable.

4. **Swiss Standard Contractual Clauses (Swiss SCCs)**

To the extent Mitel processes Customer Personal Data that is protected by the Swiss Data Protection Laws, the EU SCCs will apply, 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 Annex 1 and 2.

5. Conflict.

To the extent there is any conflict between the Standard Contractual Clauses, and any other terms in this DPA, the provisions of the Standard Contractual Clauses will prevail.

Annex 5- Authorized Subprocessors

1. Zoom Video Communications, Inc

Zoom’s authorized Sub processors are listed at https://explore.zoom.us/docs/en-us/subprocessors.html

List Of Parties

Data exporter (Customer):

[Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]

Contact Name:
Position:
Email:
Role:

Data importer (Service Provider):

[Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]

Contact Name: Matthieu Pere
Position: Group Data Protection Officer
Email: gdpr@mitel.com
Role: Processor