PARTNER’S DATA PROCESSING AGREEMENT

Recitals

(A) Mitel and Partner has entered into a partner agreement (“**Agreement**”) whereby Partner sells Mitel ’s products and/or services to its end user customers. In addition to Mitel products and services, Partner also sells Partner’s technical support services to customers who license Mitel’s software (each a “**Customer**”).

(B) Partner has purchased support and or professional services (“**Services**") from Mitel in respect to one or more Customers such that Partner can (i) escalate to Mitel Customer issues that Partner cannot resolve as part of its technical support services, and/or (ii) subcontract to Mitel to provide Services to Customer.

(C) While Mitel does not ordinarily desire or require access to Customer Personal Data to provide the Services, Mitel acknowledges that it may at times be exposed to Customer Personal Data while providing Services, and as such Mitel is the data processor. For example, a support ticket submitted to Mitel ’s may contain Customer Personal Data and/or if applicable, when Mitel accesses Customer licensed software (either onsite or remotely) to resolve a customer issue. Mitel may need to view user provisioning information, call detail records, or listen to call recording or voice mails amongst other things. The parties agree that any processing of Customer Personal Data by Mitel is ancillary (and not core) to the Services.

(D) At Partner’s request, Mitel has agreed to enter into this data processing agreement ("**DPA**") in respect of any ancillary processing of Customer Personal Data which may take place as a part of the Services.

(E) Partner acknowledges that as between Mitel and Partner with respect to any Personal Data of Partner employees submitted to Mitel support ticketing systems or otherwise, Mitel is the data controller and this DPA does not apply in those instances. Partner should review Mitel’s privacy policy for more information on Mitel’s handling of such Personal Data.

(F) This DPA forms part of and is subject to the terms of the Agreement.

Definitions

1.1 The following expressions are used in this DPA:

(a) "**Adequate Country"** means a country or territory that is recognized under EU Data Protection Laws or UK Data Protection Laws from time to time as providing adequate protection for Personal Data;

(b) ‘‘**China Standard Contractual Clauses**” or “**China SCCs**” shall mean the Standard Contract for Outbound Transfer of Personal Information formulated by the Cyberspace Administration of China for the transfer of personal information from China to abroad defined by Article 4 of the Measures for the Standard Contract for Outbound Transfer of Personal Information effective as of June 1, 2023.

(c) “**Customer**” means the legal entity with which the Partner has contracted for defined Mitel’s products, solutions, and/or services.

(d) “**Customer Personal Data”** means Personal Data of Customer that is provided to Mitel or accessed, stored, or otherwise processed by Mitel in connection with the Services.

(e) “**Data Breach**” has the meaning set forth in Section 3.1(f);

(f) "**Data Subject Request**" means a request from or on behalf of a data subject relating to access to, or rectification, erasure or data portability in respect of that data subject’s Personal Data or an objection from or on behalf of a data subject to the processing of its Personal Data;

(g) "**Data Protection Laws**" means all laws and regulations applicable to the processing of Mitel Data under the Agreement, including without limitation EU Data Protection Laws, UK Data Protection Laws, data protection laws of Canada (whether federal or provincial) and the United States (whether federal or state) including without limitation the California Consumer Privacy Act (CCPA) as amended by the California Privacy Rights Act (“CPRA”) including implementing regulations, as well as equivalent state laws and regulations; and the data protection laws of the People’s Republic of China;

(h) "**EU Data Protection Laws**" means all laws and regulations of the European Union, the European Economic Area and their member states applicable to the processing of Personal Data pursuant to an Agreement Regulation (EU) 2016/679 (“**GDPR**”) and Directive 2002/58/EC (including any implementing legislation of such Directive);

(i) “**EU Standard Contractual Clauses**” or “**EU SCCs**” means the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

(j) “Partner” means the Mitel’s accredited Partners, authorized to resell Mitel’s products, solutions and services to Customers.

(k) "**Personal Data**" means all data which is defined as ‘Personal Data’ or similar under Data Protection Laws and to which Data Protection Laws apply and which is provided to Mitel or accessed, stored or otherwise processed by Mitel in connection with the Services;

(l) "**processing**", "**data controller**", "**data subject**", **"special categories of personal data"**, "**supervisory authority**" and "**data processor**" shall have the meanings ascribed to them in the EU Data Protection Laws where the European Union is the relevant jurisdiction. Otherwise, the European definitions apply *mutatis mutandis* e.g., for California processing shall include selling as defined in the CCPA;

(m) **"Mitel Group"** means Mitel and any corporate entities which are from time to time under Common Control with Mitel;

(n) "**Standard Contractual Clauses**" means, as applicable, the EU SCCs, the UK SCCs, Swiss SCCs, or China SCCs or such other applicable standard contractual clauses in relation to any other jurisdictions (in each case as amended or replaced by the competent regulatory authority from time to time.

(o) "**Swiss SCCs**" means the standard contractual clauses as approved by the Swiss Federal Data Protection and Information Commissioner ("FDPIC")

(p) **"UK Data Protection Laws"** means the EU General Data Protection Regulation 2016/679, the Data Protection Act 2018 and The Privacy and Electronic Communications (EC Directive) Regulations 2003 (as may be modified or replaced from time to time), each as amended by Data Protection, Privacy and Electronic Communications (Amendments etc.)(EU Exit) Regulations 2019 (as may be modified or replaced from time to time) and incorporated into UK law under the UK European Union (Withdrawal) Act 2018;

(q) "**UK GDPR**" has the meaning as defined in Section 3 of the Data Protection Act 2018;

(r) "**UK Standard Contractual Clauses**" or "**UK SCCs**" means the international data transfer addendum to the European Commission's standard contractual clauses of 21 March 2021 adopted pursuant to Article 46 of the UK GDPR.

(s) An entity **"Controls"** another entity if it: (i) holds a majority of the voting rights in it; (ii) is a member or shareholder of it and has the right to remove a majority of its board of directors or equivalent managing body; (iii) is a member or shareholder of it and controls alone or pursuant to an agreement with other shareholders or members, a majority of the voting rights in it; or (iv) has the right to exercise a dominant influence over it pursuant to its constitutional documents or pursuant to a contract; and two entities are treated as being in "**Common Control**" if either controls the other (directly or indirectly) or both are controlled (directly or indirectly) by the same entity.

(p) **Catch All**. Any other terms that are used in this DPA but not otherwise defined shall have the meaning provided in Data Protection Laws unless otherwise defined in the Agreement.

2. Relationship of the parties

2.1 Partner appoints Mitel as a processor (or sub-processor, as the case may be) to process Customer Personal Data on behalf of Partner as necessary to provide the Services and as further described in Annex 1, or as otherwise agreed in writing by the parties. Any direct Customer engagement by Mitel on behalf of Partner, shall be deemed to be Mitel processing on behalf of Partner and covered by this DPA.

2.2 Both parties shall provide to the other a means to from time to time communicate or make enquiries regarding Customer Personal Data and each of Mitel and the Partner shall take commercially reasonably efforts to deal with any such communications and enquiries promptly.

3. Partner's obligations

Partner acknowledges and agrees that Partner:

3.1 shall have sole responsibility for the accuracy, quality, and legality of the Customer Personal Data and the means by which it acquires the Customer Personal Data.

3.2 shall comply with the obligations that apply to it under applicable Data Protection Laws.

3.3 shall take commercially reasonable efforts to provide, and/or disclose, only as applicable, Personal Data relevant to the Services and that a reasonable person would consider appropriate in the circumstances.

3.3 shall not, and will also require Customer not to, provide, disclose, expose, upload or transmit to Mitel via ticketing tool or any means, any special categories of Personal Data, including without limitation as a "special category" of personal data under the GDPR, as protected health Information under the Health Insurance Portability and Accountability Act of 1996, as personally identifiable financial information under the Gramm-Leach-Bliley Act, as data controlled by the U.S. International Traffic in Arms Regulations, as personal information under the Children's Online Privacy Protection Act and as "Core and/or Important Data" under the laws of the People's Republic of China, to Mitel, without Mitel's prior written consent.

4. Mitel's obligations

4.1 To the extent Customer Personal Data is processed by Mitel during provision of the Services, if at all, Mitel will:

(a) only process Customer Personal Data to the extent required to provide the Services and shall act only in accordance with this DPA, or as otherwise agreed in writing by the parties;

(b) in the unlikely event that applicable law requires Mitel to process Customer Personal Data other than to provide the Services, Mitel will notify the Partner (unless prohibited from so doing by applicable law);

(c) inform the Partner (as soon as reasonably practicable upon becoming aware) if, in Mitel's opinion, any instructions provided by the Partner under Clause 3.1(a) infringe the GDPR and/or any other Applicable Data Protection Laws;

(d) notify the Partner as soon as practicable after making a determination that Mitel is unable to meet any material obligations under this DPA, or applicable Data Protection Law;

(e) implement appropriate technical and organisational measures in its provision of the Services to ensure a level of security appropriate to the risks that are presented by the processing, in particular protection against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Customer Personal Data. Such measures include, without limitation, the security measures set out in Annex 2. Where Customer Personal Data that Mitel processes for the provision of the Services is processed on Customer's infrastructure or Customer's third-party provider's infrastructure, for any security measures that are managed solely by the Customer or Customer's third-party infrastructure provider, such as physical security for the applicable data centres, Partner acknowledges that Mitel does not control such infrastructure, and Mitel will rely on the security measures implemented and maintained by Customer or Customer's third-party infrastructure provider. For clarity , Mitel is not responsible for security (e.g. technical and organisational measures) of Customer systems.

(f) take reasonable steps to ensure that only authorised personnel providing the Services have access to Customer Personal Data and that any persons whom Mitel authorises are under obligations of confidentiality. All personnel who have access to the Customer Personal Data must have received appropriate training on data protection and cyber security;

(g) if Mitel confirms there has been a breach of Mitel's security leading to a material accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Customer Personal Data which would reasonably require Partner to disclose to Customer under Data Protection Laws (a "**Data Breach**"), Mitel shall inform Partner without undue delay and shall provide reasonable information and cooperation to Partner so that Partner can fulfil any data breach reporting obligations it may have under Data Protection Laws;

(h) promptly notify the Partner if it receives a Data Subject Request. Except as required by Data Protection Laws, Mitel will not respond to a Data Subject Request received by Mitel without the Partner's prior written consent except to confirm that such request relates to the Partner to which the Partner hereby agrees; and

(i) taking into account the nature of processing and the information available to Mitel, provide Partner with reasonable assistance to the extent required under Data Protection Laws. Partner agrees to pay Mitel for providing such assistance, at Mitel's standard consultancy rates.

(j) delete (at Partner's direction) all Customer Personal Data (including copies thereof) processed pursuant to this DPA upon written request by Partner, or if the Customer Personal Data is no longer required to provide the Services, as soon as reasonably practicable. This requirement shall not apply to the extent that Mitel is required by applicable law to retain some or all of the Customer Personal Data.

4.2 [CALIFORNIA ONLY] - Without limiting the generality of the foregoing, where Mitel processes Customer Personal Data that is subject to the CCPA and/or the CPRA in the course of providing the Services, the following terms shall apply, in addition to the above terms.

A. Mitel shall not:

i. sell or share Customer Personal Data.

ii. retain, use, disclose or otherwise process Customer Personal Data for any purpose other than for the specific purpose of providing the Services, including but not limited to (i) marketing or commercially exploiting Customer Personal Data or (ii) disclosing Customer Personal Data for a commercial purpose other than providing the Services.

iii. retain, use, disclose or otherwise process Customer Personal Data outside of the direct business relationship between both parties; and

iv. combine Customer Personal Data received from or on behalf of Customer that it processes as part of the Services with Personal Data that it receives from, or on behalf of, another person or persons, or collects from its own interaction with a consumer, except where both (i) are expressly required to perform the Services and (ii) permitted by Applicable Laws.

B. Mitel certifies that it understands the restrictions set out in this subsection and will comply with them.

5. Sub-processing

5.1 Partner grants a general authorization (a) to Mitel to appoint other members of Mitel Group as sub-processors, and (b) to Mitel and other members of Mitel Group to appoint third parties to support the performance of the Services.

5.2 Mitel will provide a list of sub-processors upon written request. The list shall be considered Mitel confidential and proprietary information and shall not be shared with any third party without Mitel's prior written consent, except where required under Data Protection Laws or where the list is provided to (A) a data subject whose personal information is processed or (B) a third party for whom Partner processes personal information. If the Partner has a reasonable objection to any sub-processor, it shall notify Mitel of such objections in writing within ten (10) days of the receipt of the list and the parties will seek to resolve the matter in good faith within a sixty (60) day period. Mitel may use any sub-processor whilst the objection procedure in this clause 5.2 is in process. Where Partner's objection to a sub-processor cannot be resolved in good faith, Mitel will, at its sole discretion, either not appoint the Sub-processor, or permit the Partner to terminate or suspend the affected Service in accordance with the termination provisions in the Agreement without liability to either Party (but without prejudice to the fees incurred by Partner prior to suspension or termination).

5.3 Mitel will ensure that any sub-processor it engages to provide services on its behalf in connection with the Agreement does so only on the basis of a written contract which imposes on such sub-processor terms substantially no less protective of Customer Personal Data than those imposed on Mitel in this DPA (the "**Relevant Terms**"). Mitel will be liable to the Partner for any breach by such person of any of the Relevant Terms.

6. Audit and records

6.1 Mitel will make available to Partner information relevant to Mitel's performance of this DPA in Mitel´s possession or control which Partner reasonably requests in writing (and which Mitel is lawfully entitled to disclose). Upon written Partner 's request, Mitel agrees to provide Partner with a summary copy of Mitel's audit report(s), if any, relating to Services. Such reports shall be considered Mitel confidential and proprietary information and shall not be shared with any third party except with Mitel's prior written consent or as required under Data Protection Laws. This Section 6.1 does not provide Partner with any right to conduct an onsite audit.

6.2 To the extent required under Data Protection Laws, Mitel shall maintain complete and accurate records of all processing of Customer Personal Data carried out by it, or on its behalf, pursuant to the DPA.

7. Data transfers

7.1 Partner acknowledges and agrees that Mitel may process Customer Personal Data under this DPA on a global basis (e.g., Services may be provided remotely out of different jurisdictions). To the extent that Mitel transfers Customer Personal Data which originates from a country with laws imposing data transfer restrictions, Mitel shall ensure that it takes such measures as are necessary to ensure the transfer is in compliance with the Applicable Data Protection Law.

7.2 Where such Customer Personal Data originates from a country with an approved transfer mechanism, such as the Standard Contractual Clauses (SCCs), the applicable SCCs is hereby incorporated by reference and shall apply as further detailed in Annex 3 to this DPA. Annex 1 and 2 of this DPA forms an integral part of this DPA and shall be deemed Appendixes 1 and 2 to the SCCs mutatis mutandis.

7.3 Where Mitel engages sub-processors who are involved in the processing of Customer Personal Data, Mitel will ensure that a suitable mechanism is in place between Mitel and the sub-processor prior to transferring any Customer Personal Data, which originates from a country with laws imposing data transfer restrictions, to the sub-processor.

8. Liability

8.1 MITEL'S TOTAL LIABILITY SHALL IN ALL CIRCUMSTANCES BE LIMITED IN ACCORDANCE WITH THE AGREEMENT OR, IF NO LIABILITY CAP IS DETAILED IN THE AGREEMENT, MITEL AND MITEL'S AFFILIATES' MAXIMUM TOTAL AGGREGATE LIABILITY TO PARTNER UNDER OR IN CONNECTION WITH THIS DPA (INCLUDING UNDER THE STANDARD CONTRACTUAL CLAUSES SET OUT IN ANNEX 3) SHALL NOT UNDER ANY CIRCUMSTANCES EXCEED THE LESSER OF THE: TOTAL AGGREGATE FEES PAID TO MITEL UNDER THE AGREEMENT IN THE PRECEEDING TWELVE (12) MONTHS OR ONE HUNDRED THOUSAND UNITED STATES DOLLARS.

8.2 Partner shall indemnify, defend and hold harmless Mitel, its affiliates, officers, directors and employees against all claims, expenses, costs (including reasonable legal costs), damages, losses, demands and regulatory fines awarded against or incurred or paid by Mitel arising from or in connection with the Customer's Personal Data.

9. General

9.1 If Partner determines that it or a Customer must notify any authority, data subject and/or the public (or portions of the public) of a Data Breach, Partner will notify Mitel before the communication is made and supply Mitel with copies of (i) any written documentation to be filed with the authority, and (ii) any notification that Partner or Customer proposes to make (whether to an authority(ies), data subject(s) the public or portions of the public), which references Mitel, its security measures and/or its role in the Data Breach, whether or not by name. Subject to the Partner 's or Customer's compliance with any mandatory notification deadlines under Data Protection Law, the Partner will consult with Mitel in good faith and take account of any clarifications or corrections Mitel reasonably requests to such filing and/or notifications and require Customers to do the same.

9.2 This DPA is without prejudice to the rights and obligations of the parties under any Agreement which shall continue to have full force and effect. In the event of any conflict between the terms of this DPA and the terms of any Agreement, the terms of this DPA shall prevail so far as the subject matter concerns the processing of Personal Data.

9.3 This DPA sets out all of the terms that have been agreed between the parties in relation to the subjects covered by it. No other representations or terms shall apply or form part of this DPA.

9.4 Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

9.5 Subject to the terms of Annex 3, this DPA shall be governed by and construed in accordance with the laws of the country of territory stipulated for in the Agreement at issue and each of the parties agrees to submit to the choice of jurisdiction as stipulated in the relevant Agreement in respect of any claim or matter arising under this DPA.

9.6 A person who is not a party to this DPA shall not have any rights to enforce this DPA including (where applicable) under the Contracts (Rights of Third Parties) Act 1999 of England and Wales to enforce any term of this DPA.

9.7 This DPA may not be amended in any other way except through a written agreement by authorized representatives of each party.

9.8 Other than in respect of any accrued liabilities of either party and the provisions of clauses 1, 2 and this clause 9, this DPA shall terminate automatically on the expiry or termination for whatever reason of the last Agreement between Partner and Mitel.

Annex 1
Details of the Personal Data and processing activities

(a) Personal Data. During its provision of the Services, Mitel may process Customer Personal Data such as:

- (A) user first name, last name, phone number, job title, address email address, photo, geographic location, username and password;
- (B) inbound and outbound call logs, 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) Any other information that may be provided to Mitel.

(b) Purpose of Processing. Mitel will only process Customer Personal Data necessary to provide the Services for the purposes of providing the Services. Mitel will only transfer Customer Personal Data from Customer (or Customer’s customer) premise to the extent necessary to provide Services.

(c) 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 Services and will take reasonable steps to permanently delete the Customer Personal Data as soon as reasonably practicable and legally permissible upon resolution of issue leading to such Services.

LIST OF PARTIES

Data exporter (Partner):

[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:
Role: 'pick one'

Data importer (Mitel):

[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
Role: Processor

Annex 2
Technical and Organizational Security Measures

Information Security Organization

Mitel has an information security organization that is responsible for planning, implementing, and overseeing all information security measures. At the head of this organization is the Chief Information Security Officer (CISO), who takes over the strategic direction and coordination of information security measures. The CISO is supported by a team of IT security experts who are responsible for the operational implementation and continuous improvement of security measures.

Security Policies

Mitel is committed to maintaining the highest security standards through security policies that safeguard our customers' data and business operations. Our policies are designed to align with industry’s best practices, regulatory requirements, and risk management frameworks, ensuring confidentiality, integrity, and availability. Mitel policies apply to anyone who has access to Mitel information systems and data. We periodically review and amend our security policies to maintain protection of employee and customer information.

Network and System Security

Network Security is a critical component of Mitel’s overall security posture, encompassing measures to protect the integrity, confidentiality, and availability of data and resources within Mitel’s network.

- **Secure Configuration**: Mitel ensures that network devices and systems are securely configured. This includes applying security patches and updates.
- **Network Segmentation**: The Mitel network is segmented to limit the impact of a security breach. Customer data is segmented physically and logically for all cloud platforms as well as from the corporate network. Production, test and development environments are also kept separated.
- **Monitoring and Logging**: Mitel implements monitoring and logging to track network activity and identify any unusual or suspicious behavior.
- **Firewalls**: Mitel utilizes firewalls to monitor and control incoming and outgoing network traffic based on predetermined security rules, ensuring that only authorized and secure communications are allowed.
- **IDS/IPS**: Mitel implements IDS/IPS at the perimeter firewalls. High severity real-time threats against known vulnerabilities are blocked by IPS and alerts are forwarded to the SIEM for triage and analysis.
- **Secure Remote Access**: Mitel has deployed Secure Remote Access technology to encrypt all network traffic between remote devices and the corporate network.
- **Media Handling**: Mitel will implement protections to secure portable storage media from damage, destruction, theft or unauthorized copying and the personal data stored on portable media through encryption and secure removal of data when it is no longer needed. Additional similar measures will be implemented for mobile computing devices to protect personal data.

Workstations Security

Mitel implements endpoint protections on end-user devices and will monitor those devices to be following best practice security standards requiring as a minimum: strong authentication, screen saver/lock for idle time, up-to-date antivirus with regular scans, real-time software protection, firewall software, supported OS with automated patching, critical software patching, and hard disk encryption. Controls are implemented to detect and remediate workstation compliance deviations.

Data Center Cloud Infrastructure Partners

Mitel’s data center cloud infrastructure partners, at a minimum, adhere to Tier III data center requirements. Such facilities are access-controlled with 24/7 on site security restricting entry into the facilities to authorized personnel. These data centers have redundant power, redundant cooling and redundant network connectivity. Our cloud partners maintain a comprehensive disaster recovery (DR) plan that includes backup strategies and procedures for recovering data and applications in the event of disaster.

Data Encryption

- **Encryption at Rest**: All sensitive data stored on company servers or storage devices is encrypted using strong encryption algorithms.

- **Encryption in Transit:** Data transmitted over the network is encrypted as per Mitel corporate standards.

Access

Physical Access Control and Security

Mitel's access controls ensure that only authorized persons have access to systems that process or use personal data and to the facilities where such processing takes place.

- All Mitel Data Center sites are secured against unauthorized access through automated access control systems and monitoring.
- Office ingress points and secured areas are secured by an electronic access control system including real-time monitoring where appropriate.
- Employee and Visitor access rights are reviewed and controlled by Mitel policy which includes employee assisted visitor logging and escort.
- A clean desk, secure disposal and physical security policy is in place.

Logical Access Control

The goal of logical access control is to ensure that only authorized persons are able to access systems that process and use personal data, and that such access is based on legitimate and authorized need to access. Data terminals (workstations, servers, network components and devices) are accessed by means of authorization and authentication in all systems. Mitel's access control regulations include the following measures:

- Strong authentication mechanisms, using passwords in combination with multi-factor authentication (MFA), are used to verify the identity of users.
- Strong and complex password policy including regular password changes.
- Role-based access control (RBAC) is implemented to restrict access to data and systems based on the principle of least privilege.
- Access to sensitive data is logged and monitored to detect and respond to unauthorized access attempts.
- Tracking and regular review of all existing privileged accounts is carried out.
- Rights management both onboarding and offboarding are controlled by Mitel policy.

Incident Response

Mitel will maintain an incident response plan and follow documented incident response policies including data breach notification to Data Controller without undue delay where a breach is known or reasonably suspected to affect Client Personal Data.

Risk Management

Mitel will assess risks related to processing of Personal Data, Security and Business Operations and will create an action plan to mitigate identified risks.

Vulnerability Management

The Vulnerability Management process systematically identifies, reviews, addresses, and remediates vulnerabilities within Mitel managed computing environments. This includes:

- **Vulnerability Assessment**: Mitel conducts regular vulnerability assessments using automated scanning tools and manual techniques to identify vulnerabilities in systems, applications, and network infrastructure.
- **Patch Management**: Mitel has a patch management policy and process to promptly apply security patches and updates to meet objectives.
- **Security Advisories**: Mitel actively monitors and assesses security threats, notifications and advisories that are applicable to the Mitel environment.

Business Continuity

- **Data Backup**: Regular backups of critical data are performed. Immutable backups are stored off network and are encrypted.
- **Regular Testing**: Regular testing of the backup and restore procedures are conducted to validate their effectiveness and identify areas for improvement.
- **Monitoring and Alerts**: Monitoring and alerting are in place for backup processes and storage usage to proactively identify issues and ensure timely resolution.
- **Hybrid Workforce**: In the event of facility closures or disruptions, Mitel's workforce is equipped to work remotely to ensure

business continuity.

- **Industry Standard Technologies:** To protect against loss of critical services caused by system component failures (power supply, fans, drives, or line interference) Mitel utilizes several technologies including: redundant power, cooling and networking with failover capabilities and data backups stored in a physically separate location from the primary site. Access to these backups is restricted to authorized personnel.

Organizational Measures

Data Protection Officer

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 (i) global data protection and (ii) security and awareness training as part of their onboarding process and receive continuous training annually thereafter. Training completion rate is 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. Security and awareness training program is designed to educate and empower Mitel employees to recognize, report and respond to potential security risks and suspected incidents. By enhancing the awareness of our workforce, we aim to create a culture of security consciousness that permeates throughout the organization.

Contractor and Vendor Management

Mitel takes commercially reasonable steps to select and retain only third-party vendors 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.

Annex 3
Standard Contractual Clauses Details

1. **UK Standard Contractual Clauses**.
The UK Information Commissioner is the exclusive Supervisory Authority for Personal Data protected and within the scope of the UK Data Protection Laws, 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**.
Where Personal Data protected and within the scope of the EU Data Protection Laws is transferred/ processed in a jurisdiction that is not adequate, the following shall apply:

2.1 The parties select and 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 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 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 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 Personal Data, we will disclose only the minimum amount of 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 a 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 Personal Data that is protected by the Swiss Data Protection Laws, the EU SCCs will apply, with the following modifications:

i. 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;

ii. 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

iii. 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.