

Anhang 1 - Beschreibung der Dienste

1. Beschreibung der Dienste

Bereitstellung von Support für die Zoom-Webmeeting- und Videokonferenz plattform.

2. Gegenstand der Verarbeitung

- i. Mitel hat im Rahmen einer Vereinbarung die Plattform für Web-Meetings und Videokonferenzen von Zoom ("Plattform") an den Kunden weiterverkauft. Im Rahmen dieses Weiterverkaufs stellt Mitel dem Kunden Supportdienste zur Verfügung, wobei Zoom Video Communications, Inc. gegebenenfalls Eskalationssupport leistet.
- ii. Diese AVV und alle Anhänge gelten für die Verarbeitung Personenbezogener Kundendaten durch Mitel für die Bereitstellung dieser Supportdienste für den Kunden.

Anhang 2 - Einzelheiten zu den Personenbezogenen Daten und Verarbeitungstätigkeiten

Erläuterung: Abschnitt (A) befasst sich mit der Verarbeitung Personenbezogener Kundendaten durch Mitel als Auftragsverarbeiter für den Kunden bei der Bereitstellung von First-Level-Support für den Kunden in Bezug auf die Zoom-Plattform für Web-Meetings und Videokonferenzen. Abschnitt (B) befasst sich mit der Verarbeitung Personenbezogener Kundendaten durch Zoom bei der Bereitstellung von Eskalations-Support als Unterauftragsverarbeiter für Mitel. Wir haben diese in verschiedene Abschnitte unterteilt, da Zoom als Unterauftragsverarbeiter einen größeren Umfang an Personenbezogenen Kundendaten verarbeitet. Für die Bereitstellung der Zoom-Plattform für Web-Meetings und Videokonferenzen besteht ein Auftragsverarbeitungsvertrag zwischen Zoom und dem Kunden.

1. Für Supportdienste im Zusammenhang mit der Nutzung der Plattform gilt Folgendes:

(A). Einzelheiten der Verarbeitung und Übermittlung Personenbezogener Kundendaten durch Mitel

1. Kategorien Personenbezogener Daten:

i. Daten, die erforderlich sind, um Support zu gewährleisten wie z. B.:

- A. Vorname, Nachname, Telefonnummer, Berufsbezeichnung, Adresse, E-Mail-Adresse, Foto, geografischer Standort, Benutzername und Passwort;
- B. ein- und ausgehende Anrufprotokolle (oder CPNI-Informationen), Meeting-ID, Anmelde-ID, E-Mail- und SMS-Kommunikation, aufgezeichnete Anrufe, ein- und ausgehende Faxe, Sprachnachrichten, Meeting-Informationen, Chatverläufe, Kalenderdaten, persönliche Kontakte, Geburtsdatum, vom Benutzer gespeicherte oder gespeicherte Inhalte, die von den Nutzern gemeinsam genutzt werden;
- C. IP-Adressen, Informationen zur Einrichtung der Dienste, Dienstkonfigurationen und -einstellungen;
- D. gemeldete Support-Probleme.

ii. Besondere Kategorien von Daten (falls zutreffend): Besondere Kategorien personenbezogener Daten sind für die Nutzung des Zoom-Dienstes oder die Bereitstellung von Support durch Mitel nicht erforderlich. Der Kunde kann die Verarbeitung dieser Daten verhindern, indem er eine Ende-zu-Ende-Verschlüsselung in den Meetings einsetzt und die Endnutzer daran hindert, Profilinformationen hochzuladen, die solche besonderen Datenkategorien enthalten.

2. Häufigkeit der Übermittlung: kontinuierlich

3. Art der Verarbeitung: Erbringung der Supportdienste

4. Kategorien von betroffenen Personen: Nutzer

5. Zweck der Verarbeitung und Übermittlung: Mitel verarbeitet Personenbezogene Kundendaten nur zum Zweck der Erbringung der Supportdienste, einschließlich von Problemlösungen, Bugs und Fehlern und der Umsetzung von Erkenntnissen, die aus individuellen Kunden-Supportanfragen gewonnen wurden, um den Dienst zu verbessern; jedoch nur in dem Umfang, in dem diese Erkenntnisse anonymisiert sind. Mitel wird Personenbezogene Kundendaten nur in dem Maße an Zoom und andere Unterauftragsverarbeiter weitergeben, wie es für die Erbringung der Supportdienste erforderlich ist.

6. Dauer der Verarbeitung: Soweit Personenbezogene Kundendaten an Mitel übermittelt werden, wird Mitel die personenbezogenen Daten des Kunden nur so lange aufbewahren, wie es für die Erbringung der Supportleistungen durch Mitel erforderlich ist. Mitel wird angemessene Maßnahmen ergreifen, um die Personenbezogenen Daten des Kunden so bald wie möglich nach Behebung des Problems, das zu diesen Supportdiensten geführt hat, dauerhaft zu löschen, es sei denn, es ist gesetzlich etwas anderes vorgeschrieben.

(B) Einzelheiten der Verarbeitung von Personenbezogenen Kundendaten durch Zoom als Auftragsverarbeiter:

1. Kategorien von Personenbezogenen Daten:

i. Die für die Unterstützung erforderlichen Daten umfassen die in Abschnitt A dieses Anhangs 1 genannten Personenbezogenen Daten sowie:

Daten zu Kundeninhalten:

Zoom-Kontoprofilinformationen: Daten, die mit dem Zoom-Konto des Nutzers, dem Profilbild, dem Passwort, dem Firmennamen und den Kundenpräferenzen verbunden sind. Dies beinhaltet:

- Einmalige Zoom-Benutzer-ID,
- Anmeldung bei sozialen Medien (optional),
- Profilbild (optional) und den
- Anzeigenamen.

Daten zur Kundenauthentifizierung: Dazu gehören Benutzername und Passwort, sofern nicht das Single Sign On (SSO) verwendet wird.

Kommunikationsinhalte für Sitzungen und Webinare: Dies beinhaltet:

- Video, Audio, Whiteboard, Untertitel und Präsentationen
- Fragen und Antworten in der Sitzung, Umfragen und Informationen zu Umfragen
- Untertitelung (Live-Transkriptionen)

Chat-Nachrichten: 1:1-Nachrichten in Meetings und Gruppenchats, die nicht in einen unbefristeten Chat-Kanal übertragen werden.

Vom Kunden veranlasste Cloud-Aufzeichnungen: Dazu gehören die folgenden Aufzeichnungen, wenn eine solche Aufzeichnung durch die Admineinstellungen des Kunden erlaubt und von einem Meetingleiter oder -teilnehmer ausgewählt wurden:

- Videoaufnahme von Video, Audio, Whiteboard, Untertiteln und Präsentationen
- Tonaufnahme
- Textdatei aller Gruppenchats während der Sitzung
- Textdatei des Audio-Transkripts
- Fragen und Antworten während des Meetings, Umfragen und Informationen zu Umfragen
- Aufzeichnung der Untertitel

Informationen für Meeting- und Webinarteilnehmer:

Diese beinhalten:

- Name und Kontaktdaten des registrierten Teilnehmers sowie alle Daten, die der Kunde in Verbindung mit der Registrierung angeben möchte, wie zum Beispiel E-Mail-Adressen
- Status des Teilnehmers (als Meetingleiter, als Teilnehmer an einem Chat oder als Teilnehmer im Meeting)
- Meetingraumname (falls verwendet)
- Nutzerkategorien
- Ergänzende Gruppenbezeichnungen
- geplante Uhrzeit für ein Meeting
- Betreffzeile

Gespeicherte Chat-Informationen: Damit sind im Speicher ruhende Daten gemeint wie:

- Chat-Nachrichten
- per Chat ausgetauschte Dateien
- per Chat ausgetauschte Bilder
- per Chat ausgetauschte Videos

- Titel des Chat-Kanals
- Whiteboard-Anmerkungen

Adressbuch-Informationen:

- Dazu gehören Kontaktinformationen, die durch den Kunden zur Verfügung gestellt werden
- Softwareintegrationen (z.B. Outlook)

Kalenderinformationen: Dazu gehören Sitzungspläne, die durch den Kunden kontrolliert und zur Verfügung gestellt sind sowie

- Softwareintegrationen (z. B. Outlook, Google Kalender)

Diagnosedaten:

- Metadaten der Sitzung: Metriken zur Servicenutzung, einschließlich des Zeitpunkts und der Art und Weise, wie die Sitzungen durchgeführt wurden).
- Diese Kategorie umfassen:
 - Ereignisprotokolle (einschließlich durchgeführter Aktion, Ereignistyp und -untertyp, Ort des In-App-Ereignisses, Zeitstempel, Client-UUID, Benutzer-ID und Sitzungs-ID)
 - Informationen zur Sitzung, einschließlich Häufigkeit, durchschnittliche und tatsächliche Dauer,
 - Quantität, Qualität, Netzaktivität und Netzwerkonnektivität
 - Anzahl der Sitzungen
 - Anzahl der gemeinsam genutzten und nicht gemeinsam genutzten Bildschirme
 - Sitzungen
 - Anzahl der Teilnehmer
 - Informationen zum Gastgeber der Sitzung
 - Hostname
 - URL des Meetings
 - Uhrzeit vom Beginn/Ende des Meetings
 - Einwahlverfahren

Telemetriedaten: Daten, die von lokal installierter Software (Anwendungen und Browserinformationen über die Bereitstellung von Zoom-Diensten und damit verbundenen Systemumgebungs-/technischen Informationen gesammelt werden. Dies beinhaltet:

- PC-Name
- Mikrophon
- Lautsprecher
- Kamera
- Domain
- Festplatten-ID
- Netzwerktyp
- Typ und Version des Betriebssystems
- Client-Version

- MAC-Adresse
- Ereignisprotokolle (einschließlich durchgeführter Aktionen, Ereignistyp und -untertyp, Ort des In-App-Ereignisses, Zeitstempel, Client-UUID, Benutzer-ID und Meeting-ID)
- Systemprotokoll (Informationen über Systemereignisse und -zustände)

- Kamera
- Domain
- Festplatten-ID
- Netzwerktyp
- Typ und Version des Betriebssystems
- Client-Version
- IP-Adressen entlang des Netzwerkpfads

Andere vom Dienst generierte Daten:

- Spam-Erkennung
- Push-Benachrichtigungen
- Eindeutige Kennungen durch Zoom wie UUID oder Benutzerkennungen, die mit anderen Datenelementen kombiniert werden:
 - IP-Adresse
 - Rechenzentrum
 - PC-Name
 - Mikrofon
 - Lautsprecher

Supportdaten:

- Kontaktname des Antragstellers, Uhrzeit, Betreff, Problembeschreibung, Feedback nach der Sitzung (Daumen hoch/runter)
Vom Nutzer bereitgestellte Anhänge, einschließlich Aufzeichnungen, Abschriften oder Screenshots, Feedback nach der Sitzung (Freitext mit Daumen nach unten)

ii Besondere Kategorien von Daten (falls anwendbar): Besondere Datenkategorien sind für die Nutzung des Zoom-Dienstes nicht erforderlich. Kunde kann die Verarbeitung dieser Daten verhindern, indem er eine Ende-zu-Ende-Verschlüsselung in den Meetings einsetzt und Endnutzer daran hindert, Profilinformationen hochzuladen, die besondere Kategorien personenbezogener Daten enthalten

2. Art der Verarbeitung: Erbringung der Supportdienste

3. Kategorien von betroffenen Personen: Nutzer

4. Häufigkeit der Übermittlung: kontinuierlich

5. Zweck der Verarbeitung und Übermittlung. Zoom wird als Unterauftragsverarbeiter von Mitel wird Personenbezogene Kundendaten nur zum Zweck der Erbringung der Supportdienste verarbeiten, einschließlich von Problemlösungen, Bugs und Fehlern und der Umsetzung von Erkenntnissen, die aus individuellen Supportanfragen gewonnen wurden, um den Dienst zu verbessern; jedoch nur in dem Umfang, in dem diese Erkenntnisse anonymisiert sind. Mitel wird Personenbezogene Kundendaten nur in dem Maße an Zoom und andere Unterauftragsverarbeiter weitergeben, wie es für die Erbringung der Supportdienste erforderlich ist.

6. Dauer der Verarbeitung. Zoom bewahrt die Personenbezogenen Kundendaten nur so lange auf, wie es für die Erbringung der Support-Services durch Zoom erforderlich ist, und ergreift angemessene Maßnahmen, um die Personenbezogenen Daten des Kunden in Übereinstimmung mit der Datenaufbewahrungs- und Löschungs politik von Zoom dauerhaft zu löschen.

Anhang 3 -Technische und organisatorische Maßnahmen

A. Mitel's Maßnahmen im Einzelnen

i. Organisatorische Maßnahmen

Datenschutzbeauftragter: Mitel hat für die Mitel-Unternehmensgruppe einen Datenschutzbeauftragten mit Sitz in Deutschland ernannt, der für die Überwachung der Verarbeitung Personenbezogener Daten durch Mitel und die unabhängige Beratung über die laufende Einhaltung der geltenden Datenschutzgesetze und das EU-Datenschutzrecht verantwortlich ist. Der Datenschutzbeauftragte leitet ein globales Team von internationalen Datenschutzexperten mit interdisziplinärem Fachwissen in den Bereichen Datenschutzrecht, KI und digitale Ethik sowie Erfahrung in der Arbeit in diesen verschiedenen Rechtsordnungen.

Vertraulichkeitsverpflichtung der Mitarbeiter: Die Mitarbeiter von Mitel sind standardmäßig durch Vertraulichkeitsklauseln in ihren Arbeitsverträgen zur Wahrung der Geschäfts- und Berufsgeheimnisse von Mitel verpflichtet oder müssen, falls erforderlich, eine solche Vertraulichkeitsvereinbarung unterzeichnen.

Schulung und Sensibilisierung: Alle Mitel-Mitarbeiter müssen im Rahmen ihrer Einarbeitung eine globale Datenschutzbildung besuchen und werden danach jährlich weiter geschult. Der erfolgreiche Abschluss der Schulungen wird überwacht, und die Nichteinhaltung kann zu disziplinarischen Maßnahmen führen. Die Datenschutzbildung von Mitel wird jährlich überprüft und aktualisiert, um neue Entwicklungen in der Gesetzgebung und Rechtsprechung zu berücksichtigen. Die Schulung umfasst Verfahren für die Handhabung, Übermittlung und Speicherung Personenbezogener Daten und die effektive Reaktion auf Sicherheitsvorfälle.

Management von Auftragnehmern und Anbietern: Mitel unternimmt wirtschaftlich angemessene Schritte, um ausschließlich Drittanbieter auszuwählen und zu beauftragen, die Garantien für die Umsetzung geeigneter technischer und organisatorischer Maßnahmen bieten, so dass die Verarbeitung den Anforderungen der Datenschutzgesetze entspricht und den Schutz der Rechte der betroffenen Personen gewährleistet.

Vereinbarungen zur Datenverarbeitung: Gegebenenfalls schließt Mitel mit seinen Kunden, Partnern und Unterauftragsverarbeitern eine Auftragsdatenverarbeitung ab, in der die Rollen der Parteien sowie ihre Rechte und Pflichten in Bezug auf die Verarbeitung Personenbezogener Daten klar definiert und vertraglich vereinbart werden.

Internationale Übermittlung Personenbezogener Daten: Im Falle von Übermittlungen Personenbezogener Daten außerhalb der EU und in Ermangelung eines Angemessenheitsbeschlusses der EU-Kommission kann Mitel Personenbezogene Daten an ein Drittland oder eine internationale Organisation übermitteln, indem es Standardvertragsklauseln (SCCs) in dem jeweiligen Modul abschließt. Für Übermittlungen innerhalb der Mitel-Unternehmensgruppe hat Mitel eine konzerninterne Vereinbarung zur Übermittlung Personenbezogener Daten ("Konzerninterne Vereinbarung") abgeschlossen. Die konzerninterne Vereinbarung enthält die Standardvertragsklauseln der EU-Kommission 2021 und die Britischen Standardvertragsklauseln.

ii. Technische Maßnahmen

Mitel führt und aktualisiert ein Verzeichnis der Mitarbeiter, die zum Zugriff auf Systeme mit Personenbezogenen Kundendaten unter seiner Kontrolle oder zum Zugriff auf Systeme berechtigt sind.

Laptops und Desktops von Mitel-Mitarbeitern, die für den Zugriff auf Personenbezogene Kundendaten verwendet werden, unterliegen den Regeln und Policies, die von der IT- und Sicherheitsorganisation von Mitel festgelegt und verwaltet werden. Zu den Regeln und Policies gehören der Einsatz eines aktuellen Virenschutzes, die Pflege von Sicherheits-Patches und die Festplattenverschlüsselung, um sicherzustellen, dass jeder Mitarbeiter, der Zugang zu den Systemen hat, über eine einzige eindeutige Kennung/Login verfügt, und um wiederholte Versuche, mit einem ungültigen Passwort Zugang zu den Informationssystemen zu erhalten, zu überwachen. Passwörter müssen regelmäßig geändert werden und müssen ein Minimum an Komplexität aufweisen. Mitel unterhält ein Programm zur Reaktion auf Informationssicherheitsvorfälle, das Verstöße gegen die Informationssicherheit aufdeckt und analysiert, aufzeichnet, beseitigt und wiederherstellt.

Die Produktions-, Test- und Entwicklungsumgebungen von Mitel werden getrennt gehalten. Alle Änderungen an Produktionssystemen, die Personenbezogene Kundendaten enthalten, oder an Systemen, auf die zugegriffen wird und die Personenbezogene Kundendaten enthalten, sind Gegenstand des Änderungsmanagementprozesses von Mitel.

Mittel-Mitarbeiter, die mit Personenbezogenen Kundendaten arbeiten, dürfen nur vertrauenswürdige Geräte verwenden, die mit einer Sicherheitssoftware mit automatischen Sicherheits-Patches konfiguriert sind, die starke Passwörter (Regeln für Länge, Zeichen und Wiederholbarkeit) und Passwortänderungen voraussetzen. Die Mitarbeiter werden dazu angewiesen, Computer zu sperren und administrative Sitzungen zu deaktivieren, wenn sie Räumlichkeiten verlassen, die von Mittel kontrolliert werden, oder wenn Computer anderweitig unbeaufsichtigt gelassen werden. Darüber hinaus sind die Laptops und Desktop-Computer der Mitarbeiter so eingestellt, dass sie nach einer gewissen Zeit der Inaktivität automatisch gesperrt werden. Die gemeinsame Nutzung von Benutzerkennungen und Passwörtern ist untersagt. Mittel hat Policies, die einen "sauberen Schreibtisch/einen leeren Bildschirm" vorschreiben, wenn Arbeitsplätze unbeaufsichtigt gelassen werden sowie nach Ende eines Arbeitstages.

Gedruckte und elektronische Datenträger, die Personenbezogene Kundendaten enthalten, werden gelöscht oder vernichtet, indem Papier geschreddert wird, CDs und DVDs geschreddert werden, Datenträger sicher gelöscht und für die erneute Bereitstellung aufbereitet werden oder, wenn die Datenträger außer Betrieb genommen werden sollen, sicher gelöscht und gegebenenfalls physisch vernichtet werden.

B. Zoom's Maßnahmen als Unterauftragsverarbeiter:

Maßnahme	Beschreibung
Maßnahmen zur Pseudonymisierung und Verschlüsselung von Personenbezogenen Daten	Zoom implementiert Kontrollen über sein Kommunikationsnetzwerk, um Daten zu schützen. Die Kontrollen müssen die Sicherung des Produktionsnetzwerks und die Implementierung von Verschlüsselung, Protokollierung und Überwachung sowie die Deaktivierung von Kommunikation umfassen, wenn keine geschäftliche Notwendigkeit besteht. Remote-Verbindungen: Der Datenfluss in der Remote-Verbindung muss verschlüsselt sein und während des Anmeldevorgangs muss eine Multi-Faktor-Authentifizierung verwendet werden. Die Einstellungen für Remote-Verbindungen müssen die Möglichkeit des gleichzeitigen Zugriffs von Remote-Benutzern auf das initiierte Netz und das Remote-Netz beschränken (d. h. kein Split-Tunneling). Der etwaige Fernzugriff von Unterauftragsverarbeitern muss denselben Kontrollen unterliegen und geschäftlich gerechtfertigt sein. Drahtloser Zugang: Der drahtlose Zugriff auf das Zoom-Firmennetzwerk muss so konfiguriert werden, dass eine Authentifizierung erforderlich ist und der Zugriff verschlüsselt wird.
Maßnahmen zum Risikomanagement	Zoom führt jährlich Risikobewertungen durch, um die Implementierung von Kontrollen zum Schutz von Geschäftsabläufen und Kundendaten zu überprüfen.
Maßnahmen zur Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Widerstandsfähigkeit der Verarbeitungssysteme und Dienste	Zoom setzt Sicherheitsmaßnahmen ein, um die Vertraulichkeit, Integrität, Verfügbarkeit und Widerstandsfähigkeit seiner Verarbeitungssysteme und Dienstleistungen zu gewährleisten.
Maßnahmen zur Zugangskontrolle	Die Zugriffsrechte werden nach dem Prinzip der geringsten Privilegien vergeben und überwacht, um Zugriffs- und Sicherheitsereignisse zu protokollieren, wobei Tools eingesetzt werden, die eine schnelle Analyse der Nutzeraktivitäten ermöglichen. Logische Zugangskontrollen: Dokumentierte logische Zugriffspolicies und -verfahren unterstützen rollenbasierten, "Need-to-know"-Zugriff (z. B. im Falle abteilungsübergreifender Aufgabenwechsel, Kündigungen) und gewährleisten eine Aufgabentrennung während des Genehmigungs- und Bereitstellungsprozesses. Jedes eingerichtete Konto wird eindeutig identifiziert. Der Nutzerzugang wird in regelmäßigen Abständen überprüft.

	Privilegierter Zugang: Die Verwaltung privilegierter Benutzerkonten (z. B. Konten, die die Möglichkeit haben, Systemkontrollen außer Kraft zu setzen), einschließlich Dienstkonten, folgt einem dokumentierten Prozess und ist eingeschränkt. Es ist ein regelmäßiges Überprüfungs- und Kontrollverfahren implementiert, um eine angemessene Bereitstellung von privilegiertem Zugang zu gewährleisten. Authentifizierung und Autorisierung: Eine dokumentierte Authentifizierungs- und Berechtigungspolicy gilt für alle anwendbaren Systeme. Diese Policy umfasst Anforderungen an die Bereitstellung von Passwörtern, Anforderungen an die Komplexität und Rücksetzung von Passwörtern, Schwellenwerte für Sperrversuche, Schwellenwerte für Inaktivität und die Gewährleistung, dass keine gemeinsamen Konten verwendet werden. Die Authentifizierungsdaten müssen verschlüsselt werden, auch bei der Übermittlung zu und von den Umgebungen der Unterauftragsverarbeiter oder bei der Speicherung durch Unterauftragsverarbeiter.
Maßnahmen zur Reaktion auf Vorfälle	Es gibt einen dokumentierten Plan und zugehörige Verfahren, die die Verantwortlichkeiten des Zoom-Personals und die Identifizierung der im Falle eines Informationssicherheitsvorfalls zu benachrichtigenden Parteien beinhalten.
Maßnahmen zur Sicherstellung der Verfügbarkeit und des Zugangs zu Personenbezogene Daten im Falle eines physischen oder technischen Zwischenfalls	Zoom ergreift Maßnahmen, um die Verfügbarkeit und den Zugang zu Verarbeitungssystemen und Dienstleistungen im Falle eines physischen oder technischen Zwischenfalls unverzüglich wiederherzustellen.
Verfahren zur regelmäßigen Prüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen, um die Sicherheit der Verarbeitung zu gewährleisten	Zoom setzt ein Verfahren ein, um die Wirksamkeit der technischen und organisatorischen Maßnahmen zu gewährleisten. Dabei wird die Sicherheit der von uns verarbeiteten Daten regelmäßig getestet, bewertet und evaluiert.
Maßnahmen zum Schutz der Daten bei der Übermittlung	Standard-Verschlüsselung: Die Verbindung zwischen einem bestimmten Gerät und Zoom wird standardmäßig verschlüsselt, wobei eine Mischung aus TLS 1.2+ (Transport Layer Security), Advanced Encryption Standard (AES) 256-Bit-Verschlüsselung und SRTP (Secure Real-time Transport Protocol) verwendet wird. Welche Methoden genau verwendet werden, hängt davon ab, ob ein Benutzer den Zoom-Client, einen Webbrowser, ein Gerät oder einen Dienst eines Drittanbieters oder das Zoom-Telefonprodukt verwendet. Für weitere Informationen, lesen Sie bitte unser Whitepaper zur Verschlüsselung .
Maßnahmen zum Schutz der Daten während der Speicherung	Alle persönlichen Daten des Kunden, einschließlich der persönlichen Daten des Kunden, die mit Unterauftragsverarbeitern geteilt werden, müssen in einer Weise gespeichert und gepflegt werden, die ihre Rückgabe oder sichere Vernichtung auf Anfrage des Kunden ermöglicht.
Maßnahmen zur Gewährleistung der Sicherheit der physischen Orte, an denen Personenbezogene Daten verarbeitet werden	Es gibt Kontrollen zum Schutz der Systeme vor physischem Eindringen böswilliger oder unbefugter Personen, vor Schäden durch Umweltverschmutzung und vor elektronischem Eindringen durch aktive oder passive elektronische Emissionen.

Maßnahmen zur Sicherstellung der Ereignisprotokollierung	Zoom implementiert einen Standard, der alle Systeme verpflichtet, relevante Sicherheitszugriffseignisse zu protokollieren.
Maßnahmen zur Sicherstellung der Systemkonfiguration, einschließlich der Standardkonfiguration	Zoom implementiert einen Standard, der die Mindestanforderungen für das Konfigurationsmanagement in der Unternehmens- und Geschäftsumgebung von Zoom festlegt.
Maßnahmen zur internen IT- und IT-Sicherheitssteuerung und -verwaltung	Zoom setzt Richtlinien und Standards für die interne IT- und IT-Sicherheit, Governance und das Management um.
Maßnahmen zur Zertifizierung/Absicherung von Prozessen und Produkten	Zoom führt Sicherheitsüberprüfungen durch und hat Rechenschaftspflichten umgesetzt. Mindestens einmal jährlich führt Zoom eine unabhängige Überprüfung seiner Sicherheitspolicies, -standards, -abläufe und -verfahren im Zusammenhang mit den für den Kunden erbrachten Diensten durch.
Maßnahmen zur Gewährleistung der Datensparsamkeit	Zoom implementiert eine Datenschutzprüfung in seinem Softwareentwicklungszyklus, um die Produktentwicklung mit dem Prinzip der Datenminimierung in Einklang zu bringen.
Maßnahmen zur Sicherung der Datenqualität	Zoom implementiert eine System- und Informationsintegritätspolicy. Die Kontrollen müssen sicherstellen, dass alle gespeicherten, empfangenen, kontrollierten oder anderweitig abgerufenen Daten korrekt und zuverlässig sind.
Maßnahmen zur Gewährleistung einer begrenzten Datenspeicherung	Wir bewahren Personenbezogene Daten so lange auf, wie es für die in unserer Datenschutzerklärung beschriebenen Verwendungszwecke erforderlich ist, es sei denn, das geltende Recht schreibt eine längere Aufbewahrungsfrist vor. Die Kriterien für die Festlegung unserer Aufbewahrungsfristen sind unter anderem die Folgenden: • Dauer der laufenden Kundenbeziehung; • ob Kontoinhaber Informationen in ihren Konten ändern oder diese löschen; • ob wir gesetzlich verpflichtet sind, die Daten aufzubewahren (z.B. sind wir aufgrund bestimmter Gesetze verpflichtet, Aufzeichnungen über Ihre Transaktionen eine bestimmte Zeit lang aufzubewahren, bevor wir sie löschen können); oder • ob eine Speicherung im Hinblick auf unsere Rechtslage ratsam ist (z.B. im Hinblick auf die Durchsetzung unserer Vereinbarungen, die Beilegung von Streitigkeiten und geltende Verjährungsfristen, Rechtsstreitigkeiten oder behördliche Untersuchungen).
Maßnahmen zur Gewährleistung der Rechenschaftspflicht	Zoom überprüft diese Sicherheitsmaßnahmen und dokumentiert sie.

Beziehungen zu Drittparteien	Unterauftragsverarbeiter werden identifiziert, bewertet, verwaltet und überwacht. Unterauftragsverarbeiter, die wesentliche Dienste erbringen oder Zoom bei der Erbringung von wesentlichen Dienstleistungen für Kunden unterstützen, müssen Maßnahmen einsetzen, die nicht weniger streng sind als die in diesem Dokument dargelegten Anforderungen. Auswahl und Beaufsichtigung: Zoom hat ein Verfahren zur Identifizierung von Unterauftragsverarbeitern, die Dienstleistungen für Zoom erbringen; Zoom schließt Verträge mit Unterauftragsverarbeitern ab, die Anforderungen an Sicherheitskontrollen enthalten, einschließlich Datenschutzkontrollen und Benachrichtigung bei Sicherheits- und Datenschutzverletzungen. Es gibt Überprüfungsprozesse, um sicherzustellen, dass die Unterauftragsverarbeiter die Vertragsbedingungen erfüllen.
Technologie Asset Management	Es bestehen Verfahren zur Entfernung von Daten aus Produktionssystemen, in denen Personenbezogene Daten des Kunden gespeichert, verarbeitet oder übertragen werden. Gegebenenfalls verwendet Zoom Industriestandards zur Löschung oder physischen Zerstörung als Mindeststandard für die Entsorgung von Vermögenswerten. Zoom verfügt über dokumentierte Verfahren für die Entsorgung oder Wiederverwendung von Vermögenswerten.
Organisatorische Sicherheit	Gegebenenfalls werden bei Zoom-Mitarbeitern Background-Checks (einschließlich strafrechtlicher Überprüfungen) durchgeführt. Zoom-Personal unterliegt einer schriftlichen Geheimhaltungs- oder Vertraulichkeitsverpflichtung. Es gibt Policies, die sicherstellen, dass der Zugang zu Informationen auf einer Need-to-know-Basis erfolgt.
Programm zur Sensibilisierung und Aufklärung.	Sicherheitsrichtlinien und Verantwortlichkeiten werden innerhalb der Mitel-Unternehmensgruppe an die Zoom-Mitarbeiter kommuniziert. Das Zoom-Personal muss jährlich an einer Schulung zum Sicherheitsbewusstsein erfolgreich teilnehmen.

Anhang 4 – Details zu den Standardvertragsklauseln

1. UK Standardvertragsklauseln (UK SCCs)

Der UK Information Commissioner (IC) ist die ausschließliche Aufsichtsbehörde für die Übermittlung Personenbezogener Daten aus dem Vereinigten Königreich im Rahmen dieses Vertrages. Die UK SCCs für das Vereinigte Königreich unterliegen den Gesetzen von England und Wales, und die Parteien unterwerfen sich in Bezug auf sie der ausschließlichen Gerichtsbarkeit der englischen Gerichte.

2. EU-Standardvertragsklauseln (EU SCC)

2.1 Die Parteien wählen das folgende Standardvertragsklauselmodul:

- Modul (Verantwortlicher an Verantwortlicher)
☒ Modul zwei (Verantwortlicher an Auftragsverarbeiter)
☐ Modul drei (Auftragsverarbeiter an Auftragsverarbeiter)
Modul Vier (Auftragsverarbeiter an Verantwortlicher)

2.2 Für jedes Modul vereinbaren die Parteien gegebenenfalls die Anwendung der folgenden Bestimmungen:

- (a) Die Datenschutzbehörde des Landes, dessen Recht den Standardvertragsklauseln gemäß Buchstabe c) unten unterliegt, ist die zuständige Aufsichtsbehörde;
- (b) Betroffene Personen, für die Mitel Personenbezogene Kundendaten verarbeitet, sind Drittbegünstigte im Sinne der geltenden EU SCCs;
- (c) Die EU SCCs unterliegen dem Recht, das auf das Abkommen anwendbar ist, sofern es sich um das Recht eines Mitgliedstaats der Europäischen Union handelt und dieses Recht Rechte von Drittbegünstigten zulässt. Ist keine dieser Bedingungen erfüllt, so gilt deutsches Recht; und
- (d) alle Streitigkeiten, die sich aus den EU SCC ergeben, werden von den Gerichten des Landes entschieden, dessen Recht die EU SCCs gemäß Buchstabe c) unterliegen.

2.3 Ergänzende Maßnahmen.

Um den Schutz der im Europäischen Wirtschaftsraum ("EWR") und im Vereinigten Königreich geschützten Personenbezogenen Daten aufrechtzuerhalten, arbeitet Mitel bei internationalen Datenübermittlungen aus dem EWR oder dem Vereinigten Königreich in ein Drittland, das nach den jeweils geltenden Datenschutzgesetzen nicht als angemessen gilt, mit dem Kunden zusammen. Damit die in der Datenschutzgrundverordnung (DSGVO) und in Artikel 46 der Britischen DSGVO (Britische DSGVO) enthaltenen angemessenen technischen und organisatorischen Maßnahmen wirksam sind, muss Mitel die folgenden zusätzlichen Maßnahmen einhalten.

- (a) Anfechtung von Ersuchen durch Strafverfolgungsbehörden:
 - i. Mitel unternimmt wirtschaftlich vertretbare Anstrengungen, um Anfragen von Strafverfolgungsbehörden nach personenbezogenen Daten von EU-Kunden durch staatliche Stellen innerhalb oder außerhalb des EWR abzulehnen, wenn die Anfrage mit EU-Recht kollidiert, zu weit gefasst ist oder wenn wir anderweitig angemessene Gründe dafür haben; und
 - ii. Mitel unternimmt wirtschaftlich vertretbare Anstrengungen, um Strafverfolgungsanfragen nach Personenbezogenen Daten britischer Kunden von Regierungsbehörden innerhalb oder außerhalb des Vereinigten Königreichs abzulehnen, wenn die Anfrage mit britischem Recht kollidiert, zu weit geht oder wenn wir anderweitig angemessene Gründe dafür haben.
- (b) Offenlegung der erforderlichen Mindestmenge: Ungeachtet des obigen Unterpunkts (a) werden wir, wenn Mitel durch eine gültige und verbindliche gesetzliche Aufforderung zur Offenlegung Personenbezogener Kundendaten gezwungen wird, nur die Mindestmenge an Personenbezogenen Kundendaten offenlegen, die zur Erfüllung der Aufforderung erforderlich ist.
- (c) Unverzügliche Unterrichtung des Datenexporteurs/der betroffenen Person über das Ersuchen oder die Anordnung der Behörden, es sei denn, dies ist gesetzlich oder per Gerichtsbeschluss verboten.

3. Chinesische Standardvertragsklauseln (Chinesische SCCs)

Soweit es zu einer Übermittlung Personenbezogener Kundendaten, die durch chinesische Datenschutzgesetze geschützt sind und in dessen Geltungsbereich fallen, in ein Land außerhalb Chinas kommt, müssen die Parteien die

Chinesischen SCCs (eine aktuelle Kopie ist zur Verfügung zu stellen) gesondert unterzeichnen und gegebenenfalls alle erforderlichen Anmeldeformalitäten erfüllen.

4. Schweizer Standardvertragsklauseln (Schweizer SCCs)

Soweit Mitel personenbezogene Kundendaten verarbeitet, die durch die Schweizer Datenschutzgesetze geschützt sind, gelten die EU SCCs mit den folgenden Änderungen:

- a. Verweise in den EU-SCCs auf die "Richtlinie 95/46/EG" oder die "Verordnung (EU) 2016/679" sind als Verweise auf die Schweizer DSGVO zu verstehen;
- b. Verweise auf "EU", "Union", "Mitgliedstaat" und "Recht der Mitgliedstaaten" sind als Verweise auf die Schweiz bzw. das schweizerische Recht zu verstehen; und
- c. Verweise auf die "zuständige Aufsichtsbehörde" und die "zuständigen Gerichte" sind als Verweise auf die EDSB und die zuständigen Gerichte in der Schweiz auszulegen, es sei denn, die oben umgesetzten EU SCC können nicht für die rechtmäßige Übermittlung solcher personenbezogener Daten im Einklang mit dem Schweizer DSG verwendet werden; in diesem Fall werden stattdessen die Schweizer SCCs durch Verweis einbezogen und bilden einen integralen Bestandteil dieses Nachtrags und gelten für solche Übermittlungen. In diesem Fall werden die entsprechenden Anhänge der Schweizer SCCs unter Verwendung der in Anhang 1 und 2 enthaltenen Informationen ausgefüllt.

5. Widersprüche

Im Falle eines Widerspruchs zwischen den Standardvertragsklauseln und anderen Bestimmungen dieser AVV haben die Bestimmungen der Standardvertragsklauseln Vorrang.

Anhang 5- Autorisierte Unterauftragsverarbeiter

1. Zoom Video Communications, Inc.

Die autorisierten Auftragsverarbeiter von Zoom sind unter <https://explore.zoom.us/docs/en-us/subprocessors.html> aufgeführt.

Parteien

Datenexporteur (Kunde):

[Offizieller Name und Kontaktdaten des/der Datenexporteure(s) und gegebenenfalls seines/ihres Datenschutzbeauftragten und/oder Vertreters in der Europäischen Union]

Name der Kontaktperson:

Position:

E-Mail-Adresse:

Rolle:

Datenimporteur (Dienstanbieter):

[Offizieller Name und Kontaktdaten des/der Datenimporteure(s), einschließlich der für den Datenschutz zuständigen Kontaktperson]

Name des Ansprechpartners: Matthieu Pere

Position: Datenschutzbeauftragter von Mitel

E-Mail: gdpr@mitel.com

Rolle: Auftragsverarbeiter