TeamViewer
Auftragsverarbeitungsvertrag (AVV)

1 Anwendbarkeit

Für die in Anlage 1 dieser Vereinbarung beschriebenen Verarbeitungstätigkeiten, bei denen der Kunde als Verantwortlicher und TeamViewer als Auftragsverarbeiter des Kunden auftritt, vereinbaren die Parteien bis auf Weiteres die folgenden Regelungen zur Auftragsverarbeitung, die die TeamViewer Endbenutzer-Lizenzvereinbarung (**EULA**) ergänzen (Auftragsverarbeitungsvertrag, „**AVV**“).

Der AVV findet keine Anwendung, wenn der Kunde eine natürliche Person ist, die die Software oder die Dienstleistungen im Rahmen einer rein persönlichen oder familiären Tätigkeit nutzt (vgl. Art. 2 Abs. 2(c) EU-Datenschutz-Grundverordnung (EU 2016/679), „**DS-GVO**“).

Die Regelungen dieses AVV und gleichzeitig damit abgeschlossenen EULA ergänzen sich und bestehen nebeneinander. Bei etwaigen Widersprüchen im Bereich Datenschutz geht der AVV den Regelungen der EULA vor.

Zur Orientierung für den Kunden gibt TeamViewer in seiner Übersicht zur Datenverarbeitung in der jeweils gültigen Fassung einen Überblick darüber, wie im Zusammenhang mit der Nutzung von TeamViewer-Software und -Services personenbezogene Daten erfasst und verarbeitet werden.

2 Rechte und Pflichten von TeamViewer

2.1 Anwendbares Recht

Die Pflichten von TeamViewer ergeben sich aus diesem AVV und dem anwendbaren Recht. Das anwendbare Recht umfasst insbesondere das Deutsche Bundesdatenschutzgesetz („**BDSG**“) und die DS-GVO.

2.2 Verarbeitung nur nach Weisung

Soweit dieser AVV Anwendung findet, wird TeamViewer personenbezogene Daten nur im Rahmen dieses AVVs und auf dokumentierte Weisungen des Kunden verarbeiten, die von den Parteien in der EULA gegenseitig vereinbart und insbesondere durch die Produktfunktionalität definiert sind, sofern TeamViewer nicht durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem TeamViewer unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt TeamViewer dem Kunden diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Der Kunde kann zusätzliche schriftliche Weisungen erteilen, soweit dies zur Einhaltung des anwendbaren Datenschutzrechts erforderlich ist. Die Dokumentation zu erteilten Weisungen ist für die Laufzeit des AVVs durch den Kunden aufzubewahren.

2.3 Verpflichtung zur Vertraulichkeit

TeamViewer wird sicherstellen, dass die zur Verarbeitung der personenbezogenen Daten eingesetzten Personen zur Vertraulichkeit verpflichtet sind, es sei denn, sie unterliegen einer angemessenen gesetzlichen Vertraulichkeitsverpflichtung.

2.4 Technische und Organisatorische Maßnahmen gemäß Art. 32 DS-GVO

TeamViewer hat angemessene und geeignete technische und organisatorische Maßnahmen zum Schutz der personenbezogenen Daten gemäß Art. 32 DS-GVO getroffen und hält diese aufrecht (nachfolgend als "**TOMs**" bezeichnet). Die TOMs sind in der Dokumentation der TOMs ausführlich beschrieben, die diesem AVV als Anlage 2 beigefügt sind. Weitere Informationen zu TeamViewers Sicherheitsstandards können dem TeamViewer Trust Center entnommen werden.

Die TOMs berücksichtigen den Stand der Technik, die Kosten der Umsetzung sowie Art, Umfang, Kontext und Zwecke der Verarbeitung personenbezogener Daten, um für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau sicherzustellen. Dazu werden die Schutzziele von Art. 32 Abs. 1 DS-GVO, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, sowie Umstände der Verarbeitungen derart berücksichtigt, dass durch geeignete TOMs das Risiko auf Dauer mitigiert wird. Das Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit des jeweils aktuellen Stands der TOMs wird in **Anlage 2** näher beschrieben.

Die TOMs unterliegen technischem Fortschritt und Weiterentwicklung. TeamViewer kann die TOMs von Zeit zu Zeit ohne Benachrichtigung des Kunden überprüfen und aktualisieren, vorausgesetzt, dass eine solche Aktualisierung die Sicherheit der personenbezogenen Daten und der Software und Dienste von TeamViewer nicht unterschreitet.

2.5 Unterstützung bei Betroffenenanfragen

TeamViewer wird angesichts der Art der Verarbeitung den Kunden nach Möglichkeit durch geeignete technische und organisatorische Maßnahmen bei der Erfüllung von Anträgen auf Wahrnehmung der in Kapitel III der DS-GVO genannten Betroffenenrechte unterstützen. Sollte sich ein Betroffener direkt an TeamViewer wenden, um die Betroffenenrechte hinsichtlich der im Auftrag des Kunden verarbeiteten Daten wahrzunehmen, wird TeamViewer dieses Ersuchen unverzüglich an den Kunden weiterleiten. Auf Verlangen von TeamViewer, wird der Kunde TeamViewer den insoweit entstehenden Aufwand im angemessenen Umfang vergüten, sofern und soweit nach anwendbarem Datenschutzrecht zulässig.

2.6 Unterstützung bei der Einhaltung von Art. 32 - 36 DS-GVO

TeamViewer wird den Kunden unter Berücksichtigung der Art der Verarbeitung und der TeamViewer zur Verfügung stehenden Informationen durch geeignete technische und organisatorische Maßnahmen bei der Einhaltung der in Art. 32-36 DS-GVO genannten Pflichten unterstützen, insbesondere hinsichtlich der Sicherheit der Verarbeitung, der Meldung von Verletzungen des Schutzes personenbezogener Daten, der Datenschutz-Folgeabschätzung und der Konsultation mit Aufsichtsbehörden. Auf Verlangen von TeamViewer. wird Kunde TeamViewer den insoweit entstehenden Aufwand im angemessenen Umfang vergüten, sofern und soweit nach anwendbarem Datenschutzrecht zulässig.

2.7 Verzeichnis von Verarbeitungstätigkeiten

TeamViewer wird dem Kunden die für die Führung des Verzeichnisses der Verarbeitungstätigkeiten notwendigen Informationen zur Verfügung stellen.

2.8 Löschung und Rückgabe der Daten

TeamViewer hat nach Wahl des Kunden die personenbezogenen Daten, die im Auftrag verarbeitet werden, zu löschen oder zurückzugeben, sofern und soweit das Recht der Europäischen Union oder eines Mitgliedsstaats, dem TeamViewer unterliegt, keine Verpflichtung zur Speicherung vorsehen.

2.9 Unterstützung beim Nachweis der Einhaltung datenschutzrechtlicher Verpflichtungen und Überprüfungen

TeamViewer wird dem Kunden alle Informationen zur Verfügung stellen, die erforderlich sind, um die Einhaltung der sich aus den Ziffern 2 und 3 dieses AVV ergebenden Verpflichtungen nachzuweisen. TeamViewer kann außerdem, soweit erforderlich, Zertifikate regelmäßiger Audits durch anerkannte Prüfer oder andere qualifizierte Dritte zur Verfügung stellen.

Sofern objektiv begründete Anhaltspunkte für einen Verstoß durch TeamViewer gegen diesen AVV oder datenschutzrechtliche Regelungen besteht, wird TeamViewer zusätzliche Überprüfungen, einschließlich Inspektionen, die vom Kunden oder von einem vom Kunden beauftragten qualifizierten Prüfer durchgeführt werden, ermöglichen und hierzu beitragen. Bei Durchführung der Überprüfung wird der Kunde Betriebsabläufe von TeamViewer nicht unverhältnismäßig stören.

2.10 Mitteilungspflicht bei Zweifeln an Weisungen

TeamViewer wird den Kunden unverzüglich informieren, wenn TeamViewer der Auffassung ist, dass die Ausführung einer Weisung zu einer Verletzung des geltenden Datenschutzrechts führen könnte. TeamViewer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Kunden nach Überprüfung schriftlich bestätigt oder geändert wird.

2.11 Mitteilungen bei Verstößen

Stellt TeamViewer Verstöße gegen das anwendbare Datenschutzrecht, dieses AVV, oder Weisungen des Kunden in Bezug auf die Auftragsverarbeitung fest, hat TeamViewer dies dem Kunden unverzüglich mitzuteilen.

2.12 Datenschutzbeauftragter

TeamViewer hat einen externen Datenschutzbeauftragten bestellt, erreichbar unter privacy@teamviewer.com, oder TeamViewer Germany GmbH, z.Hd. Datenschutzbeauftragte, Bahnhofsplatz 2, 73033 Göppingen, Deutschland.

2.13 Datenübermittlungen in ein Drittland

TeamViewer wird personenbezogene Daten, die im Rahmen dieses AVVs verarbeitet werden, in ein Land außerhalb der EU oder des Europäischen Wirtschaftsraums („EWR“), für das kein Angemessenheitsbeschluss der EU-Kommission im Sinne von Art. 45 Abs. 3 DS-GVO besteht („unsicheres Drittland“), grundsätzlich nur übermitteln, sofern:

a. der Kunde bzw. der Nutzer des Kunden TeamViewer eine Weisung zu einer solchen Übermittlung erteilt, z.B. durch die Aufforderung, eine Verbindung mit einem Endpunkt herzustellen, der in einem unsicheren Drittland liegt (wobei in solchen Fällen der Kunde dafür verantwortlich ist zu gewährleisten, dass die Datenübermittlung im Einklang mit Art. 44 ff. DS-GVO erfolgt), oder

b. TeamViewer nach dem Recht der Europäischen Union oder eines Mitgliedstaats, dem TeamViewer unterliegt, dazu verpflichtet ist; in einem solchen Fall teilt TeamViewer dem Kunden diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

Darüber hinaus ist TeamViewer berechtigt, Unterauftragsverarbeiter in einem Drittland zur Verarbeitung personenbezogener Daten einzusetzen, soweit die Voraussetzungen des Art. 44 DS-GVO erfüllt sind.

3 Unterauftragsverarbeiter

3.1 Genehmigte Unterauftragsverarbeiter

TeamViewer nimmt die Dienste einer Reihe weiterer Auftragsverarbeiter (nachfolgend, „**Unterauftragsverarbeiter**“) in Anspruch. Die Liste der von TeamViewer eingesetzten Unterauftragsverarbeiter für relevante TeamViewer Produkt-Gruppen ist unter dem folgenden Link als Anlage 3 abrufbar. Mit dem Abschluss des AVV stimmt der Kunde der Beauftragung der Unterauftragsverarbeiter zu, die im Zeitpunkt des Abschlusses des AVV in der Anlage 3 für jeweiligen TeamViewer Produkt aufgeführt sind.

3.2 Ernennung weiterer Unterauftragsverarbeiter

Sofern TeamViewer zur Erbringung der vertraglich vereinbarten Leistungen (z.B. Hosting) weitere oder andere Unterauftragsverarbeiter beauftragen möchte, sind diese mit der gesetzlich gebotenen Sorgfalt auszuwählen. TeamViewer benachrichtigt den Kunden spätestens 15 Tage im Voraus über die Ernennung neuer Unterauftragsverarbeiter. Der Kunde hat das Recht, unter Darlegung von objektiv nachvollziehbaren Gründen, der Einschaltung des Unterauftragsverarbeiters zu widersprechen. Erfolgt innerhalb dieser Frist kein Widerspruch, so gilt der entsprechend mitgeteilte neue Unterauftragsverarbeiter als genehmigt. Kann im Falle eines fristgerechten Widerspruchs keine Lösung erzielt werden, sind beide Parteien berechtigt, den AVV mit einer Frist von 2 Wochen zu kündigen. Mit Wirksamwerden der Kündigung des AVV gilt auch die EULA als beendet. Auf Ziffer B.5.5. (Folgen der Vertragsbeendigung) der EULA wird verwiesen.

3.3 Unterauftragsverarbeiter in Drittländern

Eine Beauftragung von Unterauftragsverarbeitern in Drittländern darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

3.4 Verpflichtungen der Unterauftragsverarbeiter

TeamViewer wird die Verträge mit Unterauftragsverarbeitern so gestalten, dass sie den Anforderungen der geltenden Datenschutzgesetze und dieses AVVs entsprechen und die Unterauftragsverarbeiter insbesondere dazu verpflichten, keine weiteren oder anderen Unterauftragsverarbeiter mit der Verarbeitung personenbezogener Daten zu beauftragen und die Bestimmungen der Ziffer 3.2 entsprechend gegenüber TeamViewer zu beachten. TeamViewer wird dem Unterauftragsverarbeiter vertraglich Pflichten auferlegen, die hinreichende Sicherheit dafür bieten, dass die angemessenen technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen der DS-GVO und dieses AVVs erfolgt.

4 Änderungen dieses AVVs

TeamViewer ist grundsätzlich berechtigt, dieses AVV zu ändern. TeamViewer wird den Kunden über die geplante Änderung und den Inhalt des neuen AVVs mindestens 28 Tage vor Wirksamwerden informieren. Die Änderung gilt als genehmigt, wenn der Kunde gegenüber TeamViewer nicht innerhalb von 15 Tagen ab Zugang dieser Information widerspricht. Widerspricht der Kunde der Änderung, besteht der AVV zu den bestehenden Konditionen fort.

5 Haftung

Auf Art. 82 DS-GVO wird verwiesen.

Im Übrigen wird vereinbart, dass die Regelungen zur Haftungsbeschränkung aus dem entsprechenden Lizenzvertrag gelten sollen.

6 Besondere Regelungen für Regional Restricted Access

Für die im Vertrag genannten spezifischen Produkte ‚Regional Restricted Access" verarbeitet TeamViewer personenbezogene Daten des Kunden im Rahmen dieser AVV in den Vereinigten Staaten. Eine Verarbeitung außerhalb der Vereinigten Staaten kann erfolgen (i) soweit dies für Wartungs-, Support- oder Entwicklungszwecke erforderlich ist und wie in den jeweils aktuellen Datenschutzhinweisen beschrieben, sowie (ii) auf Anfrage des Kunden, insbesondere wenn der Kunde die Dienste von einem Standort außerhalb der Vereinigten Staaten nutzt.

Anlage 1 zum Auftragsverarbeitungsvertrag

Einzelheiten der Verarbeitung – TeamViewer Produkte

Stand vom 9. März 2026

Inhalt

1 Gegenstand

Der allgemeine Gegenstand der Verarbeitung ist in der EULA sowie in der jeweiligen Produktspezifikation beschrieben.

2 Dauer

Die Dauer der Verarbeitung entspricht der Laufzeit der EULA.

3 Art und Zweck der Verarbeitung

TeamViewer wird personenbezogene Daten als Auftragsverarbeiter des Kunden verarbeiten, um die Nutzung der im Rahmen der EULA bereitgestellten Software und Services nach dokumentierten Weisungen (im Rahmen der Produktfunktionalität) des Kunden und/oder seiner Benutzer zu ermöglichen.

Dies umfasst im Wesentlichen die Verarbeitung der übertragenen Inhalte sowie das Management der Inhalte des Benutzerkontos. Bei der Nutzung von TeamViewer Core wird TeamViewer die nachfolgend aufgeführten Verarbeitungen im Auftrag des Kunden durchführen.

Die weitere Spezifikation der Software und Services finden Sie auf der Produktspezifikationsseite.

Die Verarbeitung außerhalb des Geltungsbereichs dieses AVVs wird in der jeweiligen Datenschutzinformation beschrieben.

Produkte	Art und Zweck der Verarbeitung
Alle TeamViewer Produkte (außer Frontline, Assist AR, Engage/Co-Browsing, und Classroom, siehe separaten Abschnitt unten)	- Verarbeitung der Daten im Benutzerkonto, insbesondere Speicherung und Zugänglichmachung der Daten für andere Benutzer im Rahmen einer Verbindung, z.B. Name, Kontakte, E-Mail-Adresse, Profilbild sowie Inhaltsdaten der Verbindungen, z.B. Chat. - Verarbeitung der im Benutzerkonto gespeicherten Kontaktlisten. - Übermittlung der vom jeweiligen Benutzer übertragenen Inhaltsdaten an andere Benutzer innerhalb einer Remote-Verbindung oder Sitzung (Bildschirm, übermittelten Daten und Dateien sowie alle anderen sonstigen ausgetauschten Informationen). - Verarbeitung von Daten im Rahmen der Verwaltung des Firmenprofils, wie z.B. lizenzierte Geräte, festgelegte Regeln, Verwaltung des Firmenprofils, Verteilung von Firmenrichtlinien, Verwaltung des Benutzerzugriffs, Verbindungsberichte, Wake on LAN-Funktionalität usw. - Übermittlung der verschleierten Kundenkontodaten durch das neue Sicherheitsfeature (falls zutreffend). - Verarbeitung von Daten im Rahmen der Sitzungsplanung für Besprechungen, z.B. Startzeit, Besprechungsthema, Teilnehmer, Besprechungs (Meeting)-ID.

	- Verarbeitung von Daten im Rahmen der Erbringung eines Integrationsdienstes. - Verarbeitung von Daten zur Kundenbetreuung und für die Erbringung von technischer Unterstützung. - Verarbeitung von Daten für die Erbringung von Professional Services - Bereitstellung der Funktion „Verbindungsbericht“. - Ermöglichung von iOS In-App-Käufen und deren Verknüpfung mit einem Konto. - Verarbeitung von Daten in Verbindung mit der Nutzung bestimmter Merkmale oder Funktionen (je nach Lizenz im jeweiligen Produkt verfügbar), z. B.: • **Remote Monitoring**, welches die Überwachung kritischer Aspekte der Geräte des Kunden umfasst. • **Network Device Monitoring**, welches die Überwachung der Verfügbarkeit und Probleme von Netzwerkgeräten wie Routern, Druckern etc. umfasst. • **Asset Management**, **Asset Management und Discovery**, welches die Sichtbarkeit aller IT-Assets des Kunden umfasst. • **Patch Management**, welches die Überwachung von Schwachstellen und das Patchen der Software und des Betriebssystems des Kunden sowie der Anwendungen von Drittanbietern umfasst. • **Endpoint Protection**, die den Schutz der Geräte des Kunden vor Viren, Trojanern, Spyware, Ransomware etc. umfasst. • **Endpoint Protection/ Endpoint Detection und Response**, Verarbeitung von personenbezogenen Daten zum Zweck der Erbringung von Sicherheits- und Datenschutzdienstleistungen, der Verbesserung der Bedrohungsabwehr und der Bereitstellung von Lizenzen für TeamViewer- und Endpoint Protection/ Endpoint Detection & Response -Produkte und -Dienstleistungen. • **Mobile Device Management**, Verarbeitung von Daten zum Zweck der Erbringung von Mobile-Device-Management-Diensten. • **Remote Scripting**, das die Erstellung, Speicherung, Bereitstellung und Ausführung von Skripten auf entfernten Geräten umfasst. • **Backup**, das die Sicherung der Geschäftsdaten des Kunden umfasst. • **Grafana Plugin**, Hosting-Service für die Bereitstellung des Grafana PlugIns für den Zugriff auf die Daten für das entsprechende Konto, falls vom Kunden gewünscht. • **Zugangskontrolle (Conditional Access)**, z.B. Bereitstellung eines eigenen Servers für den Kunden. • **REACH-Registry**, Verarbeitung von Daten im Rahmen dieser Funktionalität.

	• **Meeting**, Verarbeitung von Kontakten, die im Adressbuch des Benutzers gespeichert sind, um Meetings zu organisieren, z.B. Versenden von Einladungen, Outlook-Integration und Übertragung der vom jeweiligen Benutzer eingegebenen Inhaltsdaten an andere Benutzer innerhalb eines Meetings (Bild und Ton sowie mögliche Übertragung der Daten und Dateien). • **IoT**, Verarbeitung der Sensordaten mit der TeamViewer IoT-Cloud und anschließende Übertragung über die APIs. • **Servicecamp/ Service Desk**, einschließlich, aber nicht beschränkt auf Ticket-Inhalte, Erstellung und Zuweisung der Tickets, Ticket-Berichte, Ticket-Status und Konfigurationsparameter der Service-Instanz. • **Automatisierungen,** verbindet TeamViewer Daten mit einer Vielzahl von Lösungen.
Frontline und Assist AR	- Hosting der Login-Oberfläche sowie Verwaltung relevanter Bereiche, wie Benutzer, Geräte, Systeme etc. - Einrichtung von sog. Frontline-Arbeitsplätzen (sowohl mobil als auch Wearable), einschließlich der Einrichtung der Geräte und der Benutzer. - Hosting und Anzeige der Dashboards sowie Kontaktlisten, Asset Management, sowie Workflow Management und Aufgabenverteilung. - Bereitstellung der eingebauten Sprachbefehlserkennung (auf Wunsch des Kunden). - Sprache-zu-Text-Funktionen, einschließlich Live-Untertitelung, Transkription und Übersetzung. - Hosting von Daten in Verbindung mit xPick (z.B. Pick-Order-Management, Workflow- und Aufgabeninformationen, KPIs usw. einschließlich der Pflege von Fremdkomponenten in Workflows). - Hosting des Integrationsdienstes (auf Wunsch des Kunden). - Übertragung der Remote-Support-Anrufe sowie Hosting von den Aufzeichnungen und Remote-Anrufprotokolle in Zusammenhang mit der allgemeinen Remote-Support-Verwaltung auf Wunsch des Kunden. - Dienstleistungen im Bereich der Holo-Lens-Technologie, z.B. Bereitstellung von Eye-Tracking-Funktionalität und Augmented-Reality-3D-Punkten. - Bereitstellung von Supportleistungen, insbesondere im Hinblick auf das Kundenfeedback. - Hosting und Verwaltung der Twilio-Konsole (auf Wunsch des Kunden). - Third-Level-Support für die Serverinstanzen des Kunden (auf Wunsch des Kunden). - Übertragung der Inhaltsdaten während der virtuellen Fernwartungssitzung (Bild, Video und Ton sowie eventuelle Übertragung der Daten und Dateien). - Aktivierung einer Chat-Funktion, einschließlich der Übersetzung von Chat-Inhalten.

	- Bereitstellung der OCR-Funktion (Optical Character Recognition). - Automatisierte Erstellung von Workflows mit der Funktion PDF to Workflows.
Engage/ Co-Browsing-Funktionsmodul	- Erbringung von Dienstleistungen im Rahmen des TeamViewer Engage-/ Co-Browsing Funktionsmoduls, insbesondere das Hosting der Kundendaten sowie Wartungs- und Supportleistungen. - Bereitstellung von Diensten im Rahmen von sog. Videochat- und Livechat-Funktionalitäten, einschließlich der Übertragung und des Hostings der Chat-Inhalten und anderen damit verbundenen Diensten, z.B. Chatbots. - Bereitstellung von Leistungen im Rahmen von Terminplanungs- und eSignatur-Funktionalitäten. - Bereitstellung von sogenannten Software Development Kits (SDKs) für Kundenanwendungen, die die Integration bestimmter TeamViewer Engage-/Co-Browsing-Funktionalitäten in kundeneigene mobile Apps ermöglichen (z.B. Co-Browsing, Chats, etc.).
Classroom	- Bereitstellung von Diensten im Rahmen sogenannter Videokonferenz- und Live-Chat-Funktionalitäten, einschließlich der Übertragung und des Hostings von Chat-Inhalten (einschließlich Dateitransfer) und anderer damit verbundener Dienste, z.B. Konferenznotizen. Bereitstellung von Diensten für Whiteboard, Dokumentenaustausch und -verfolgung, Abstimmungen und Breakout-Rooms. - Bereitstellung von Kontodienstleistungen einschließlich Registrierung und Kontoführung.
KI-Dienste	- Bereitstellung von KI-gestützten Funktionen durch die Verarbeitung von Nutzerinteraktionen während der Sitzung sowie der eingegebenen oder generierten Daten (einschließlich der daraus resultierenden Ausgaben), z. B. Sitzungszusammenfassungen, Kategorisierung, Kennzeichnung, Erfassung, Zusammenfassung, Anonymisierung und Hosting der Sitzungsdaten.
DEX-Dienste	- Verarbeitung personenbezogener Daten im Zusammenhang mit der Nutzung der DEX-Dienste, z.B.: • **Endpoint Troubleshooting,** für Einblicke in und Kontrolle über jeden Endpunkt. • **Experience Analytics,** Analyse gesammelter Gerätedaten zur Überwachung häufiger Reibungspunkte, die sich auf den digitalen Arbeitsplatz auswirken. • **Endpoint Automation:** umfasst Funktionen zur Endpunktverwaltung, z. B. zur Reduzierung von Konfigurationsabweichungen, zur Identifizierung von Ursachen für Vorfälle und zur Durchführung von selbstheilenden Korrekturen. • **Inventory Insights:** Normalisierung von Bestands- und Hardwaredaten in Lieferanten-, Produkt- und Versionsaufzeichnungen für Analyse- und Berichtszwecke.

	• **Application Experience Management:** bietet Transparenz über die Anwendungserfahrung der Benutzer und Bewertung der Benutzererfahrung. • **Patch-Einblicke,** die einen Überblick über die letzten erforderlichen Patches in der Kundenumgebung bieten. • **Content-Verteilung,** Bereitstellung von Inhalten zum lokalen Austausch von Inhalten zwischen den Geräten zwecks Reduzierung von Redundanzen. • **Virtual Desktop Experience,** bietet proaktives Gesundheitsmanagement und optimiert Abläufe. • **1E Intelligence,** Zusammenführung von Edge- und Cloud-KI für schnelle, präzise und fundierte Entscheidungen und Maßnahmen, z.B. Einblicke in aufkommende DEX-Probleme, automatisierte Ursachenanalysen, Empfehlungen und Abhilfemaßnahmen. • **1E Catalog:** Kuratieren von Daten für Software- oder Hardware-Informationen für Anbieter, Titel, Umgangssprache, Version und Edition. • **PXE Everywhere,** ermöglicht es Computern, automatisch in Windows PE zu booten, um das Windows-Betriebssystem zu installieren. - Verarbeitung von personenbezogenen Daten im Rahmen der Bereitstellung von Integrationsdiensten, wie z. B.: • **Automated Self Service für ServiceNow (SCC (Service Catalog Connect) und Virtual Assistant),** umfasst eine Reihe von Automatisierungsfunktionen, um den Servicekatalog und den virtuellen Agenten zu erweitern und Anfragen sofort zu erfüllen, ohne dass Endbenutzer warten müssen. • **Service Desk Augmentation (ITSM Connect und 1E Core),** bietet die Echtzeit-Funktionen zur Untersuchung und Behebung von Vorfällen innerhalb von ServiceNow. • **CMDB Connector,** stellt die Gerätedetails der CMDB von Service Now zur Verfügung. • **Service Graph Connector,** stellt Geräte- und Softwaredetails der CMDB von ServiceNow zur Verfügung. - Bereitstellung der SaaS-Lösungen, z. B.: • **Intune,** Bereitstellung von Mobile Device Management (MDM) und Mobile Application Management (MAM) zur Steuerung der Gerätenutzung und Verwaltung von Anwendungen auf firmeneigenen und privaten Geräten. • **Device Refresh,** Optimierung der Strategien zur Geräteaktualisierung. • **Business Impact,** das Daten verarbeitet, wenn Vorfalltickets in einer ITSM-Lösung geöffnet werden, oder Daten an andere Lösungen wie Splunk auslagert.

	• **Software Reclaim,** bietet einen Überblick über die Nutzung des Softwarebestands für nicht oder nur selten genutzte Software von den Endgeräten Ihres Unternehmens.

4 Art der personenbezogenen Daten

Folgende Arten von personenbezogenen Daten werden von TeamViewer als Auftragsverarbeiter verarbeitet:

Produkte	Art der verarbeiteten personenbezogenen Daten
Alle TeamViewer Produkte (außer Frontline, Assist AR, Engage/ Co-Browsing-Funktionsmodul und Classroom, siehe unten)	- Inhaltsdaten, die während einer Verbindung zwischen TeamViewer-Clients ausgetauscht werden, z.B. Video- und Audiostream (Bildschirmansichten und Benutzerkamera), Dateitransfers, Text-Chat, Fernsteuerungsbefehle, Ticketinhalte, Whiteboard, sowie personenbezogene Daten, die für die Herstellung der Verbindung erforderlich sind. - Benutzerkontoinformationen, z.B. TeamViewer ID, Benutzername, Anzeigename, E-Mail-Adresse, IP-Adresse, Profilbild (optional), Spracheinstellung, Meeting-ID, Standort, Passwort. Die Domäne des Kunden sowie das Alter des Kontos (z.B. „älter als 6 Monate“) werden dem Sitzungshost vor der Verbindung als Teil unserer Sicherheitsfunktion "Showing Supporter Data During Connection" angezeigt. - Benutzerkontoverwaltung und -administration, z.B. Speichern und Freigeben von Benutzerprofilen, Kontodetails, Freundesliste, Kontaktinformationen, Chat-Verlauf, Dateianhänge. - Verwaltung und Managementdaten des Firmenprofils, z.B. Firmenprofil, Firmenrichtlinien, Zuordnungen zu Benutzerkonten, Verwaltung des Benutzerzugangs, Verbindungsberichte. - Personenbezogene Daten, die im Zusammenhang mit den (je nach Lizenz verfügbaren) Funktionen verarbeitet werden, einschließlich und nicht beschränkt auf: kundenspezifische Module; Push-Benachrichtigungen, die von den Benutzern initiiert werden; Mailing-Dienste (z. B. Benachrichtigungs-, Aktualisierungs- und Reporting-Parameter, wie vom Kunden definiert); Zurücksetzen von Passwörtern (z. B. Zurücksetzen des Hosting-Kontos und Mailing-Services, E-Mail mit Link zum Zurücksetzen, Zuweisung des neuen Passworts zum Konto) sowie Verwaltung vertrauenswürdiger Geräte (z. B. E-Mail-Benachrichtigungen zur Verhinderung des Missbrauchs eines Geräts für den Login); Audit-Protokolle, um Änderungen des Benutzers zu verfolgen. - Lokal auf dem Gerät des Benutzers gespeicherte Verbindungsdaten (Log-Dateien, txt-Dateien mit den Verbindungen). - Personenbezogene Daten, die im Rahmen eines Integrationsdienstes verarbeitet werden (z.B. Verbindungsdaten, Ticketinhalte, etc.). - Personenbezogene Daten, die im Rahmen des Kunden- und/oder technischen Supports verarbeitet werden.

	- Personenbezogene Daten, die bei der Erbringung von Professional Services verarbeitet werden. - Personenbezogene Daten, die im Verbindungsbericht angezeigt werden (Gerätedaten, Text, Bild, Audio, Video und Metadaten der Sitzung). - iOS In-App-Kaufdaten und Ablaufdatum des Abonnements. - Personenbezogene Daten, die im Zusammenhang mit der Nutzung bestimmter Merkmale oder Funktionen (je nach Lizenz im jeweiligen Produkt verfügbar) verarbeitet werden, z. B.: • **Remote Monitoring:** Geräteinformationen (z.B. Gerätename, Maschinenname, Festplattenspeicherplatz, Online-Stand, Ereignisse, CPU-Auslastung usw. wie in den Produktspezifikationen beschrieben); Historische Alarmdaten pro Gerät, z.B. verdächtige Alarme oder Ereignisse, wie sie durch die individuellen Einstellungen des Kunden definiert sind; Scripting Daten, z.B. Gerätename, Benutzeranmeldeinformationen, ausgeführte Skripte pro Gerät (je nachdem, wie der Kunde das jeweilige Skript ausführen möchte); Inhalt der Verbindungen zwischen der Remote Management Konsole und verwalteten Geräten. Die Inhaltsdaten sind immer verschlüsselt, sodass TeamViewer niemals auf die Inhalte zugreifen kann; Fehlerprotokolldaten, die auf dem Gerät des Benutzers gespeichert sind; Informationen in Zusammenhang mit maßgeschneiderten individuellen Überwachungsrichtlinien (Policies). • **Asset Management, Asset Management und Discovery:** Geräteinformationen (z.B. Typ der Geräte, Gerätename, Hardware-Details, installierte Software usw. wie in den Produktspezifikationen beschrieben); Erkennung von Geräten im Netzwerk durch Scanner. • **Patch Management:** Geräteinformationen, z.B. Typ der Geräte, Gerätename, Maschinenname, Festplattenspeicherplatz, Online-Stand, Ereignisse, CPU-Auslastung usw. sowie die ausgeführten Patches pro Gerät. • **Endpoint Protection:** Geräteinformationen zusammen mit den Sicherheits- und Virenschutzwarnungen pro Gerät sowie historische Warndaten (betroffenes Gerät, Malware-Typ, Datum usw.). • **Endpoint Protection/ Endpoint Detection & Response:** Kontaktinformationen, IP-Adresse und Geräteinformationen, Lizenzdaten, maschinen- und benutzerspezifische Daten, Standortdaten und andere Daten, die zur Bereitstellung des Dienstes erforderlich sind. Einige Daten werden zur Verbesserung der Bedrohungserkennung als Teil des Dienstes verarbeitet. • **Mobile Device Management:** Bestimmte Lizenzinformationen, Ihr Name, Ihre E-Mail-Adresse, Ihr Benutzername, Ihre IP-Adresse, Metadaten, Standortdaten, Anmeldedaten und Daten zu mobilen Geräten und ähnliches, um Ihre Lizenz zu aktivieren bzw. mit Ihrem Konto für die Nutzung des Mobile Device Management im weiteren Sinne zu verknüpfen. Darüber hinaus können Daten, die über verknüpfte Konten von Drittanbietern geändert werden, mit Ihrem TeamViewer-Konto synchronisiert und mit Daten im TeamViewer-Service zusammengeführt werden. • **Backup:** Alle Daten, die der Kunde zur Sicherung auswählt, z.B. verschiedene Dateien und Ordner, die auch personenbezogene Daten enthalten können. Alle Daten werden verschlüsselt, und nur der Kunde ist in der Lage, den Inhalt

	aus der Sicherung herunterzuladen und zu entschlüsseln. Erstellung, Speicherung, Wiederherstellung und Löschung von Backups erfolgen in Übereinstimmung mit den vom Kunden definierten Parametern. • **IoT:** Inhaltsdaten, die während einer IoT Verbindung zwischen TeamViewer-Clients ausgetauscht werden, z.B. Dateitransfer, Fernsteuerungsbefehle); Daten in Verbindung mit der Sensorverwaltung, z.B. IoT-Sensorinformationen (Sensor-ID, Sensornamen, metrische Namen, Typ des metrischen Werts (z.B. Celsius, Kilogramm, Meter), Datentyp (Text, Zahl usw.) sowie IoT-API-Anmeldeinformationen (z.B. Zertifikate und Anmeldeinformationen, die zur Authentifizierung von IoT-Geräten für die Übertragung von IoT-Sensordaten verwendet werden); Daten im Zusammenhang mit der Analyse, Visualisierung und Einstellung der Messungen von Sensoren sowie der Verarbeitung dieser Daten in der vom Kunden verwalteten und eingestellten TeamViewer IoT-Cloud. • **Meeting:** Sitzungsthema, Zeitzone, Sitzungs-ID, Startzeit und Endzeit der Sitzung; Planung von Besprechungen und Outlook-Integration (z.B. Uhrzeit und Datum von Besprechungen, Teilnehmer usw.) Benutzerkontoinformationen (TeamViewer-ID, Benutzername, IP-Adresse, Profilbild, Spracheinstellungen, Meeting-ID, Standort, Passwort). • **Servicecamp/ Service Desk:** Personenbezogene Daten im Zusammenhang mit der Ticketbearbeitung und dem Reporting, (z.B. TeamViewer IDs, E-Mails, Ticket-Subjekte, Datum und Uhrzeit der Tickets, Inhalt der Tickets, Zuständige für die Tickets sowie weitere vom Kunden definierte Parameter); Hosting der Ticket-Metadaten (z.B. Erstellungs- und Abschlussdatum/-zeit, Status, Bearbeiter usw.); Personenbezogene Daten im Zusammenhang mit dem Ticket-Reporting (z.B. Standort, Status, Priorität, Bearbeiter, durchschnittliche Lösungszeiten, Benutzeraktivitäten etc. wie vom Kunden definiert). • **Remote Scripting:** Geräteinformationen, Aufforderungen, Anzahl der Aufforderungen über einen bestimmten Zeitraum usw. • **Web-Monitoring:** IP-Adresse, Standortdaten, Antwortzeit, Anmeldedaten, Systemstatus. • **Automatisierungen**: Je nach Kundenkonfiguration, z.B. Ereignisprotokolle, Verbindungsdaten, etc.
Frontline	- Benutzerkontodaten (z.B. E-Mail, Passwort, Domain, IP-Adresse, Profilbild, Anzeigename, Telefonnummer, Rollen und Berechtigungen, Teamname, Rolle, Organisation, Sprache, Status (online/offline), 2-Faktor-Authentifizierung, Telefonbuchinformationen). - Personenbezogene Daten im Zusammenhang mit der initiierten Sitzung, z.B. Sitzungs-ID, Sicherheits-Token (Login und Refresh), IP-Adresse, Benutzername, Startzeit, Geräteinformationen, Sitzungsgültigkeit sowie übertragenen Inhalte. - Personenbezogene Daten in Verbindung mit dem verwendeten Gerät, das dem Benutzer die Nutzung von Frontline ermöglicht, z. B. Geräte-ID, Name, IP-Adresse, Benutzername, Anwendungsversion, Bluetooth-MAC-Adresse, Geräte-Firmware-Version, Geräteprotokolle, Schrittzählungen (falls verfügbar). - Personenbezogene Daten im Zusammenhang mit den Anrufen, die über die Geräte mit xAssist getätigt werden. z.B. ID, Benutzername, Teamname, Anruflink und Titel,

	Start-/Endzeit und Datum, Anrufereignisprotokolle, Multimedia-Asset-Informationen (Video, Bild, Text, Ton usw.), Anrufstatus. - Personenbezogene Daten in Verbindung mit den Workflows, z.B. IDs, Titel, Erstellungs-/Aktualisierungszeit und -datum, Besitzer, Schritt-Eingabe-Informationen, Versionsnummer, Tags. - Personenbezogene Daten in Verbindung mit Serviceberichten, z.B. Anrufdetails, Titel, interne Nummer, Datum/Uhrzeit, Beschreibung, Status. - Personenbezogene Daten im Zusammenhang mit Assets, insbesondere Frontline-spezifischen Assets, inkl., aber nicht beschränkt auf Workflows (.uwe), Komponenten (.uce), und Applikation (.uab). - Kommissionier-, Artikel- und Systeminformationen sowie Lagerinformationen, sofern diese Benutzerdaten enthalten. - Personenbezogenen Daten in Verbindung mit Sensorinformationen, falls vorhanden (z.B. Ersteller, Benutzer usw.). - Personenbezogene Daten im Zusammenhang mit Aufgaben (Tasks), falls vorhanden (z.B. Ersteller, Benutzer etc.). - Personenbezogene Daten in Verbindung mit gesetzten Cookies, die eine Personalisierung und Verbesserung der Produkte ermöglichen. - Personenbezogene Daten im Zusammenhang mit den Sprache-zu-Text-Funktionen, z.B. persönliche Kennung (Account ID) sowie der Audioinhalt der Sitzung. - Daten, die in Verbindung mit der Funktion PDF to Workflows verarbeitet werden, einschließlich des hochgeladenen Workflow-Dokuments.
Assist AR	- Personenbezogene Daten in Verbindung mit der initiierten Sitzung, z. B. Sitzungs-ID, Sicherheits-Token (Login und Refresh), IP-Adresse, Benutzername, Geräteinformationen, Sitzungsgültigkeit sowie übertragener Stream (Video- und Audio-Feeds), Dateiübertragungen, Text-Chat, Fernsteuerungsbefehle, Ticket-Inhalte, Whiteboard, Teamname, Anruf-Link und -Titel, Start-/Endzeit und Datum, Anruf-Ereignisprotokolle, Chat-Protokolle, Multimedia-Asset-Informationen (Video, Bild, Text, Ton etc.), Anrufstatus. - Informationen zum Benutzerkonto, z.B. TeamViewer ID, Benutzername, Anzeigename, E-Mail, IP-Adresse, Profilbild (optional), Spracheinstellung, Telefonnummer(n), Standort, Passwort. - Personenbezogene Daten im Zusammenhang mit der Benutzerkontoverwaltung und -administration, z. B. Speichern und Freigeben von Benutzerprofilen, Kontodetails, Buddy-Liste, Kontaktinformationen, Dateianhänge, Passwort, Domain, IP-Adresse, Rollen und Berechtigungen, Status (online/offline), 2-Faktor-Authentifizierung, Telefonbuchinformationen. - Personenbezogene Daten im Zusammenhang mit der Verwaltung und dem Management des Firmenprofils, z.B. Firmenprofil, Firmenrichtlinien, Zuordnungen zu Benutzerkonten, Verwaltung des Benutzerzugangs. - Personenbezogene Daten, die während des TeamViewer Assist AR Augmented Reality Videofeeds übertragen werden, sowie das Hosting der Inhalte. - Personenbezogene Daten, die im Zusammenhang mit dem Produkt SMS einladen verarbeitet werden (z.B. Telefonnummer).

	- Push-Benachrichtigungen, wie von den Benutzern initiiert. - Personenbezogene Daten im Zusammenhang mit den Sprache-zu-Text-Funktionen, z.B. persönliche Kennung (Account-ID) sowie der Audioinhalt der Sitzung. - Personenbezogene Daten, die im Rahmen der Mailing-Dienste verarbeitet werden (z.B. vom Kunden definierte Benachrichtigungs-, Aktualisierungs- und Reporting-parameter). - Personenbezogene Daten in Verbindung mit Serviceberichten, z.B. Anrufdetails, Titel, interne Nummer, Datum/Uhrzeit, Beschreibung, Status. - Personenbezogene Daten im Zusammenhang mit Assets, insbesondere Assist AR-spezifische Assets, inkl. aber nicht beschränkt auf Applikations-Assets (.uab). - Personenbezogene Daten, die im Zusammenhang mit dem Zurücksetzen von Passwörtern verarbeitet werden (z.B. Hosting-Service zum Zurücksetzen von Konten, E-Mail mit Rücksetzungslink, Zuweisung des neuen Passworts zum Konto) sowie vertrauenswürdiges Gerätemanagement (z.B. E-Mail-Benachrichtigungen zur Verhinderung des Missbrauchs eines Geräts für den Login). - Personenbezogene Daten, die für die Optische Zeichenerkennung (OCR) erforderlich sind, einschließlich Videodaten und Sitzungsmetadaten.
Engage/ Co-Browsing-Funktions-modul	Personenbezogene Daten, die im Zusammenhang mit der Nutzung folgender Funktionen verarbeitet werden: - **TeamViewer Co-Browsing** • IP-Adresse, die beim Aufbau einer Verbindung durch Co-Browsing erfasst wird, da Browser und Server IP-Adressen austauschen. Standardmäßig speichert oder verarbeitet TeamViewer die IP-Adresse nicht weiter, außer zur Bestimmung eines ungefähren Benutzerstandorts durch den ISP (Internet Service Provider). • Je nachdem, wie und wo ein Kunde Co-Browsing nutzt. Wenn Co-Browsing z.B. während eines Bestellvorgangs verwendet wird, bei dem der Benutzer personenbezogene Daten wie Name, E-Mail, Adresse, Zahlungsinformationen usw. eingeben kann, dann können personenbezogene Daten für den Agenten sichtbar gemacht werden. Die Abfolge der Tastenanschläge des Benutzers wird nicht in einen Kontext gebracht, um die darin enthaltenen personenbezogenen Daten (wie Name usw.) zu identifizieren, zu strukturieren, zu verarbeiten, zu kategorisieren oder zu analysieren. • Co-Browsing-Aufzeichnung, die personenbezogene Daten wie in diesem Abschnitt beschrieben enthalten kann (optional). • Personenbezogene Daten, die über so genannte lokale Speichervariablen und Cookies verarbeitet werden, einschließlich der Sitzungs-ID, Akzeptanz der Datenschutzrichtlinie (true/false). Solche Variablen und Cookies werden standardmäßig nur für die Dauer der Sitzung gesetzt und werden nicht verwendet, um den Benutzer zu einem späteren Zeitpunkt erneut zu identifizieren. Weitere Informationen zu Cookies und lokalen Speichervariablen sind in ***Anhang – Engage/ Co-Browsing Funktionsmodul*** (siehe unten) enthalten. • Benutzerinteraktionen, einschließlich Mausbewegungen, Klicks, Scrollen, besuchte Webseiten.

	• Personenbezogene Daten des Mitarbeiters, z.B. Name, E-Mail, Sprache, zugewiesene Co-Browsing-Sitzungen, Co-Browsing-Aufzeichnungen, Anzahl der Co-Browsing-Sitzungen, Aktivitätsprotokolle, Status, durchschnittliche Co-Browsing- und Chat-Dauer pro Mitarbeiter, initiierte und akzeptierte Co-Browsing-Sitzungen, abgelehnte Sitzungen, beendete Sitzungen und ähnliches, je nach Kundenwunsch. • Personenbezogene Daten, die in verschiedenen Berichten enthalten sind, einschließlich, aber nicht beschränkt auf Leistungs-, Statistik- und ähnliche Berichte. - **Livechat, Videochat, Chatbots** • IP-Adresse, die gesammelt wird, wenn eine Chat-Konversation eingeleitet wird, da der Browser und der Server IP-Adressen austauschen. Standardmäßig speichert oder verarbeitet TeamViewer die IP-Adresse nicht weiter, außer zur Bestimmung eines ungefähren Benutzerstandorts durch den ISP (Internet Service Provider). • Personenbezogene Daten, die von den Benutzern selbst zur Verfügung gestellt werden, einschließlich, aber nicht beschränkt auf Namen, E-Mail-Adressen, Telefonnummern, Rechnungsnummern, Kontonummern, finanzielle Informationen, Anhänge wie Bilder, Dateien, Videos und ähnliches. • Personenbezogene Daten, die sich auf den Live-Chat beziehen, z.B. Session-ID, Browser- und Geräteinformationen, oder Hinweise von Mitarbeitern des Kunden sowie Chat-Aufzeichnungen. • Personenbezogene Daten im Zusammenhang mit dem Videochat, sowie er zwischen den Nutzern des Kunden und den Mitarbeitern des Kunden initiiert wird, einschließlich Audio- und Videoübertragung, sowie personenbezogene Daten im Zusammenhang mit ihrer Interaktion, die z.B. Whiteboard, Screensharing, oder Dokumente umfasst. • Personenbezogene Daten, die über so genannte lokale Speichervariablen und Cookies verarbeitet werden, einschließlich der Sitzungs-ID, Akzeptanz der Datenschutzrichtlinie (true/false), Interaktion mit dem Chat. Solche Variablen und Cookies werden standardmäßig nur für die Dauer der Sitzung gesetzt und können je nach den Standardkonfigurationen des Kunden zur erneuten Identifizierung des Benutzers zu einem späteren Zeitpunkt verwendet werden. Weitere Informationen zu Cookies und lokalen Speichervariablen sind in ***Anhang - Engage/ Co-Browsing Funktionsmodul*** enthalten. • Chat-Verlauf, der von den Kunden des Controllers für einen bestimmten Zeitraum im Rechenzentrum gespeichert wird. • Persönliche Daten des Mitarbeiters, z. B. Name, E-Mail, Sprache, zugewiesene Chats, Anzahl der Chats, Aktivitätsprotokolle, Status, Anzahl der Chats, Chat-Dauer pro Mitarbeiter, Anzahl der Konversationen pro Mitarbeiter und ähnliches, je nach Kundenwunsch. Weitere Informationen können sein, wie lange ein Mitarbeiter gebraucht hat, um einen zugewiesenen Chat zu öffnen, wie viel Zeit er mit dem Lesen des Chats verbracht hat, wie viel Zeit er mit dem Beantworten verbracht hat (auch wie viele Textblöcke/Nachrichtenvorlagen ein Mitarbeiter verwendet hat) usw., je nach den Standardkonfigurationen des Kunden.

	• Persönliche Daten, die in verschiedenen Dashboards und Berichten enthalten sind, einschließlich, aber nicht beschränkt auf Leistungs-, Statistik- und ähnliche Berichte. • Personenbezogene Daten, die in den vom Kunden definierten Regeln enthalten sind. - **Terminvereinbarung** • Kontaktinformationen der Benutzer des Kunden (z.B. Name, E-Mail-Adresse, Telefonnummer). • Versenden und Speichern von Terminbestätigungen sowie von Erinnerungen. • Hosting von Termininformationen und -historie. • personenbezogene Daten, die in den vom Kunden definierten Regeln verschiedenen Dashboards und Berichten enthalten sein können, einschließlich, aber nicht beschränkt auf Leistungs-, Statistik- und ähnliche Berichte.
Classroom	- IP-Adresse, die gesammelt wird, wenn eine Sitzung mit den TeamViewer-Diensten aufgebaut wird, da der Browser und der Server IP-Adressen austauschen. Standardmäßig speichert oder verarbeitet TeamViewer die IP-Adresse nicht weiter, außer zur Bestimmung eines ungefähren Benutzerstandorts durch den ISP (Internet Service Provider). - Personenbezogene Daten, die von den Benutzern selbst bereitgestellt werden, einschließlich, aber nicht beschränkt auf Namen, E-Mail-Adressen, Anhängen wie Bilder, Dateien, Videos und ähnliches. - Personenbezogene Daten im Zusammenhang mit der Videokonferenzsitzung, z. B. Sitzungs-ID, Browser- und Geräteinformationen oder Mitteilungen der Mitarbeiter des Kunden sowie Chat-Aufzeichnungen. - Personenbezogene Daten im Zusammenhang mit der Videokonferenz, die zwischen den Nutzern des Kunden und den Mitarbeitern des Kunden initiiert wird, einschließlich Audio- und Videoübertragung, sowie personenbezogene Daten im Zusammenhang mit ihrer Interaktion, z. B. mit Whiteboard, Screen-Sharing oder Dokumenten, je nach Fall. - Personenbezogene Daten, die über so genannte lokale Speichervariablen und Cookies verarbeitet werden, einschließlich der Sitzungs-ID, Akzeptanz der Datenschutzrichtlinie (true/false), der Interaktion mit dem Chat. Solche Variablen und Cookies werden standardmäßig nur für die Dauer der Sitzung gesetzt und können je nach den Standardkonfigurationen des Kunden zur erneuten Identifizierung des Nutzers zu einem späteren Zeitpunkt verwendet werden. Weitere Informationen zu Cookies und lokalen Speichervariablen sind in ***Anhang - Classroom*** (siehe unten) enthalten. - Chatverlauf, von den Kunden des Verantwortlichen für einen bestimmten Zeitraum im Rechenzentrum gespeichert wird. - Persönliche Daten von Mitarbeitern, z. B. Name, E-Mail, Sprache oder Aktivitätsprotokolle. - Aufzeichnungen von Videokonferenzen, wenn sich der Kunde dafür entscheidet, diese aufzuzeichnen und zu speichern.

KI-Dienste	- Interaktionen der Benutzer während der Sitzung. - Eingegebene oder generierte Daten, abhängig von der verwendeten Funktion.
DEX-Dienste	- Gerätedaten, die von allen DEX-Diensten verarbeitet werden, einschließlich Geräteleistungs-, Betriebssystemleistungs- und Softwareleistungsdaten, Daten zur Installation und Netzwerkdaten. - Personenbezogene Daten, die im Zusammenhang mit Ihrer Nutzung bestimmter Module verarbeitet werden: • **Experience Analytics:** Nutzungsdaten, z. B. Daten zur Geräteinteraktion, Daten zur Browserinteraktion und Antworten auf Benutzerumfragen. • **Application Experience Management:** Softwaredaten, z. B. Softwarehersteller und -version, Softwareinteraktionsdaten, Daten zu Softwareabstürzen und -hängern. • **Virtual Desktop Experience:** Daten zur virtuellen Desktop-Infrastruktur, einschließlich Zeitstempel für Verbindungsstart und -ende. • **1E Intelligence:** personenbezogene Daten, einschließlich Anweisungsmetadaten und Autor. • **Patch Insights:** fehlende und angewandte Patches. - Integrationsdienste: z. B. Geräteinformationen, Benutzernamen. - SaaS-Lösungen: Geräteinformationen, z.B. Software-Inventar, (nicht persistente) Audit-Protokolldomäne, E-Mail-Adresse, Persona (falls vom Lösungsadministrator konfiguriert).

5 Kategorien von betroffenen Personen

Die folgenden Kategorien von Personen sind von der Verarbeitung betroffen:

Produkte	Kategorien von Personen
Alle TeamViewer Produkte (außer Engage/ Co-Browsing-Funktionsmodul und Classroom, siehe unten)	- Der Kunde (soweit die personenbezogenen Daten des Kunden gemäß Ziffer 4 verarbeitet werden) und ggf. die Benutzer des Kunden ((z.B. Endbenutzer von verwalteten Geräten). - Die Verbindungspartner des Kunden/der Benutzer des Kunden. - Dritte, die vom Kunden / den Benutzern des Kunden verwaltet werden, oder Dritte, deren personenbezogene Daten vom Kunden/von den Benutzern des Kunden in einer Verbindung weitergegeben werden.
Engage/ Co-Browsing-Funktionsmodul / Classroom	- Benutzer (Kunden des Kunden, Website-Besucher, Interessenten, Dritte). - Mitarbeiter des Kunden (Agenten).

KI-Dienste	- Der Kunde (soweit die personenbezogenen Daten des Kunden gemäß Ziffer 4 verarbeitet werden) und ggf. die Benutzer des Kunden (z.B. Endbenutzer von verwalteten Geräten). - Die Verbindungspartner des Kunden/der Benutzer des Kunden. - Dritte, die vom Kunden / den Benutzern des Kunden verwaltet werden, oder Dritte, deren personenbezogene Daten vom Kunden/von den Benutzern des Kunden in einer Verbindung weitergegeben werden.
DEX-Dienste	- Der Kunde (soweit die personenbezogenen Daten des Kunden gemäß Ziffer 4 verarbeitet werden) und ggf. die Benutzer des Kunden (z.B. Endbenutzer von verwalteten Geräten). - Dritte, die vom Kunden / den Benutzern des Kunden verwaltet werden, oder Dritte, deren personenbezogene Daten vom Kunden/von den Benutzern des Kunden in einer Verbindung weitergegeben werden.

Anhang – Engage/Co-Browsing- Funktionsmodul zu Anlage 1

1. Lokaler Speicher als Website-Integration

Key	**Zugehörige Funktion/ Plugin**	**Zweck/Beschreibung**	***Lebenserwartung***
cvvid	/	VisitorId - kann temporär oder permanent vergeben werden	Sitzung oder permanent
CV_i	Live-Chat	"true", wenn die Datenschutzrichtlinie im Chat akzeptiert wurde.	Sitzung
cv_sp	Live-Chat	Indikator, ob eine Nachricht gesendet wurde oder eine Interaktion (z. B. ein Schaltflächenklick) durch den Benutzer stattgefunden hat.	Sitzung
besucht	Live-Chat	"true", sobald der Benutzer zum ersten Mal mit dem WebChat interagiert - z.B., um einen Chatbot nur einmal auszulösen.	Sitzung
cvsid	Co-Browsing	SessionId, um die Kontinuität einer Co-Browsing-Sitzung beim Seitenwechsel oder über mehrere Registerkarten hinweg sicherzustellen.	Sitzung
cv-shrid	Co-Browsing	5-stelliger Zahlencode, über den sich ein Mitarbeiter per Co-Browsing mit einem Mitarbeiter verbinden kann.	Sitzung
cv-s	Co-Browsing	"true", sobald der Kunde seine Sitzung freigibt oder Co-Browsing angefordert hat.	Sitzung
cv-lvcs	Co-Browsing	Indikator, dass die Sitzung geschlossen wurde - notwendig, um die Co-Browsing-Sitzung über mehrere geöffnete Registerkarten hinweg zu beenden.	Sitzung
CV_LVD	Co-Browsing	Temporäre Daten für den Wechsel zwischen zwei Registerkarten - um die Kontinuität der Co-Browsing-Sitzung zu gewährleisten	Sitzung

2. Cookies für die Website-Integration

Um kontinuierliche Sitzungen nicht nur auf der gleichen Domain (z.B. Benutzer wechselt von yourwebsite.com zu yourwebsite.com/imprint) sondern auch domänenübergreifend für Kunden (z.B. Benutzer wechselt von yourwebsite.com zu wiki.yourwebsite.com) zu ermöglichen, werden die lokalen Speichervariablen in Cookies "umgewandelt". In diesem Fall bleiben der Zweck und die Namensgebung gleich wie bei den Lokalen Speichervariablen.

Key	**Zugehörige Funktion/ Plugin**	**Zweck/Beschreibung**	***Lebenserwartung***
cvsid	Co-Browsing	SessionId, um die Kontinuität einer Co-Browsing-Sitzung beim Seitenwechsel oder über mehrere Registerkarten hinweg sicherzustellen.	Sitzung
cv-shrid	Co-Browsing	5-stelliger Zahlencode, über den sich ein Mitarbeiter per Co-Browsing mit einem anderen Mitarbeiter verbinden kann.	Sitzung
cv-s	Co-Browsing	"true", sobald der Kunde seine Sitzung freigibt oder Co-Browsing angefordert hat.	Sitzung
cv-lvcs	Co-Browsing	Indikator, dass die Sitzung geschlossen wurde - notwendig, um die Co-Browsing-Sitzung über mehrere geöffnete Registerkarten hinweg zu beenden.	Sitzung
CV_LVD	Co-Browsing	Temporäre Daten für den Wechsel zwischen zwei Registerkarten - um die Kontinuität der Co-Browsing-Sitzung zu gewährleisten.	Sitzung

3. Lokale Speicherung für Videochat und Videokonsultationen

Key	***Zugehörige Funktion/ Plugin***	***Zweck/Beschreibung***	***Lebenserwartung***
jitsiMeetId	Video-Chat & Video-Beratung	Eindeutige ID für Video-Chat-Sitzung	Sitzung
Sprache	Video-Chat & Video-Beratung	Legt die Sprache der Benutzeroberfläche fest und pflegt sie	Sitzung

Merkmale/Basis/Einstellungen	Video-Chat & Video-Beratung	Technische Variable	Sitzung
funktionen/basis/bekannte-domains	Video-Chat & Video-Beratung	Technische Variable	Sitzung
Funktionen/Dropbox	Video-Chat & Video-Beratung	Technische Variable	Sitzung
funktionen/kalender-synchronisation	Video-Chat & Video-Beratung	Technische Variable	Sitzung
Merkmale/Aktuelles/Liste	Video-Chat & Video-Beratung	Technische Variable	Sitzung
Funktionen/Video-Layout	Video-Chat & Video-Beratung	Technische Variable	Sitzung
callStats-Benutzername	Video-Chat & Video-Beratung	Technische Variable	Sitzung
cvvid	Video-Chat & Video-Beratung	VisitorId - kann temporär oder permanent vergeben werden	Sitzung oder permanent
CV_DOC_UID	Video-Chat & Video-Beratung	VisitorId - für die Funktionalität der Dokumente	Sitzung
cv-t	Video-Chat & Video-Beratung	TabID - definiert, auf welcher Registerkarte im Videochat sich der Benutzer gerade befindet (Video, Dokument, Whiteboard, Co-Browsing)	Sitzung
cv_sp	Video-Chat & Video-Beratung	Indikator, ob eine Nachricht gesendet wurde oder eine Interaktion (z.B. ein	Sitzung

		Schaltflächenklick) durch den Benutzer stattgefunden hat.	

Anhang – Classroom zu Anlage 1

1. Lokale Speicherung für Videokonferenzen

Key	Zugehörige Funktion/ Plugin	Zweck/Beschreibung	Lebenserwartung
jitsiMeetId	Video-Konferenz	Eindeutige ID für die Videokonferenzsitzung	Sitzung
Sprache	Video-Konferenz	Legt die Sprache der Benutzeroberfläche fest und pflegt sie	Sitzung
Merkmale/Basis/Einstellungen	Video-Konferenz	Technische Variable	Sitzung
funktionen/basis/bekannte-domains	Video-Konferenz	Technische Variable	Sitzung
Funktionen/Dropbox	Video-Konferenz	Technische Variable	Sitzung
merkmale/kalender-synchronisation	Video-Konferenz	Technische Variable	Sitzung
Merkmale/Aktuelles/Liste	Video-Konferenz	Technische Variable	Sitzung
Merkmale/Video-Layout	Video-Konferenz	Technische Variable	Sitzung

callS-tatsUser-Name	Video-Konferenz	Technische Variable	Sitzung
cvvid	Video-Konferenz	VisitorId - kann temporär oder permanent vergeben werden	Sitzung oder dauer-haft
CV_DOC_UID	Video-Konferenz	VisitorId - für die Funktionalität der Doku-mente	Sitzung
cv-t	Video-Konferenz	TabID - legt fest, auf welcher Registerkarte im Videochat sich der Benutzer gerade be-findet (Video, Dokument, Whiteboard)	Sitzung
cv_sp	Video-Konferenz	Indikator dafür, ob eine Nachricht gesen-det wurde oder eine Interaktion (z. B. Ankli-cken einer Schaltfläche) durch den Nutzer stattgefunden hat.	Sitzung

TeamViewer

Übersicht der technisch-organisatorischen Maßnahmen

Stand vom 17. März 2025

Inhalt

1 Zugangskontrolle

1.1 Datenzentren

TeamViewer besitzt, mietet oder betreibt keine TeamViewer Server-Infrastruktur für seine Büros oder Produktionsumgebung. Die TeamViewer-Unternehmensumgebung ist eine rein cloud-basierte Infrastruktur, die in Rechenzentren untergebracht ist, welche durch Drittanbieter betriebenen werden. Alle Drittparteien sind nach der Norm ISO 27001 zertifiziert.

TeamViewer verfügt über Zugangskontrollmaßnahmen, die den unbefugten Zutritt zu Datenverarbeitungsanlagen verhindern sollen, in denen personenbezogene Daten gespeichert oder verarbeitet werden.

1.2 TeamViewer-Büros

Ausschließlich autorisierte Personen haben physischen Zugang zu Geländen, Gebäuden oder Räumen, in denen personenbezogene Daten verarbeitet werden. Die Einrichtungen von TeamViewer sind durch Schlüsselsysteme, Einbruchmeldeanlagen, Zugangskontrollmaßnahmen und aktives Schlüsselmanagement geschützt. Zugangsrechte werden autorisierten Personen auf individueller Basis gewährt, einschließlich Besuchern, die von autorisiertem Personal begleitet werden müssen. Mitarbeiter und Besucher sind verpflichtet, ihre Ausweise jederzeit sichtbar zu tragen, wenn sie sich in den Räumlichkeiten aufhalten.

2 System-Zugangs- und Zugriffskontrolle

TeamViewer stützt sich auf die folgenden Maßnahmen zur Systemzugriffskontrolle, um zu verhindern, dass unbefugte Personen Datenverarbeitungssysteme, in denen personenbezogene Daten gespeichert oder verarbeitet werden, nutzen können.

2.1 Netzwerk- und Hardwaresicherheit

Das TeamViewer-Firmennetzwerk ist durch Firewalls und Systeme zur Erkennung und anschließenden Beseitigung von Bedrohungen vor dem öffentlichen Netz geschützt. Es werden die auf dem neusten Stand befindende Antiviren-/Malware-Erkennungssoftware eingesetzt, um schädlichen Code zu erkennen, zu entfernen und vorzubeugen. Ein Sicherheits-Patch-Management ist implementiert und der Fernzugriff auf das TeamViewer-Unternehmensnetzwerk ist durch starke Authentifizierungsmechanismen und ein Virtual Private Network (VPN) geschützt.

TeamViewer verwendet eine rollenbasierte Sicherheitsarchitektur und erfordert, dass Benutzer des Systems identifiziert und authentifiziert werden, bevor sie Systemressourcen nutzen können. Die Ressourcen werden durch systemeigene Sicherheits- und Zusatzsoftwareprodukte geschützt, die Benutzer identifizieren und authentifizieren die Zugriffsanfragen anhand der autorisierten Rollen der Benutzer in Zugriffskontrolllisten zu validieren.

Alle Ressourcen werden im Asset-Inventarisierungssystem verwaltet und jeder Ressource wird einen Verantwortlichen zugewiesen. Diese sind für die Genehmigung des Zugriffs auf die Ressource und für die Durchführung von Überprüfungen des Zugriffs nach Rolle verantwortlich.

Mitarbeiter melden sich im TeamViewer-Netzwerk mit einer Active Directory-Benutzer-ID und einem Passwort an. Die Benutzer müssen sich außerdem separat an allen Systemen oder Anwendungen anmelden, die nicht die geteilte Sign-On-Funktionalität von Active Directory nutzen. Die Passwörter müssen definierten Passwortstandards entsprechen und werden durch Parametereinstellungen im Active Directory erzwungen. Diese Einstellungen sind Teil der Konfigurationsstandards und zwingen die Benutzer, die Passwörter in einem definierten Intervall zu ändern. Benutzer-IDs werden nach einer bestimmten Anzahl von erfolglosen Anmeldeversuchen gesperrt, um den Zugriff auf System und Ressourcen zu unterbinden. Zusätzlich wird der Bildschirm von Benutzern nach einer definierten Zeit der Inaktivität, automatisch gesperrt.

TeamViewer hat eine Passwortrichtlinie, die die ordnungsgemäße Verwendung und Einrichtung von Passwörtern regelt, einschließlich der Häufigkeit, mit der sie geändert werden müssen, der Mindestanforderungen und der Komplexität.

Mitarbeiter, die von außerhalb des TeamViewer-Netzwerks auf das System zugreifen, müssen einen Virtual Private Network (VPN)-Tunnel und ein Zwei-Faktor-Authentifizierungssystem verwenden. Die Mitarbeiter erhalten bei ihrer Einstellung VPN-Zertifikate und der Zugang wird bei ihrem Austrittsgespräch deaktiviert.

TeamViewer-Mitarbeiter greifen über das Internet auf die Zwei-Faktor-Authentifizierungsdienste zu, indem sie die Secure Socket Layer (SSL)-Funktionalität ihres Webbrowsers nutzen. Die Mitarbeiter geben zunächst eine gültige Benutzer-ID und ein Passwort ein, um Zugang zu den TeamViewer-Cloud-Ressourcen zu erhalten. Die Passwörter müssen den Anforderungen an die Passwortkonfiguration entsprechen, die auf den virtuellen Geräten unter Verwendung des virtuellen Server-Administrationskontos konfiguriert wurden. Virtuelle Geräte werden zunächst gemäß den TeamViewer-Konfigurationsstandards konfiguriert, aber diese Konfigurationsparameter können über das Administrationskonto des virtuellen Servers geändert werden.

TeamViewer unterhält ein sog. Security Operations Center (SOC), das rund um die Uhr wichtige Systeme und Warnmeldungen überwacht, um Sicherheitsvorfälle zu bewältigen. Diese Dienste werden auf eine konforme und datenschutzfreundliche Art und Weise betrieben und gewährleisten gleichzeitig eine Reaktion auf Bedrohungen, die dem Risikoniveau des Unternehmens angemessen ist.

TeamViewer-Mitarbeiter können sich über virtuelle Server-Administrationskonten bei ihren Systemen anmelden. Diese Administrationskonten verwenden ein zweistufiges, auf digitalen Zertifikaten basierendes Authentifizierungssystem.

Benutzer-IDs und Zugriffsregeln werden entsprechend der Rolle des jeweiligen Mitarbeiters festgelegt. Die Zugriffsregeln sind auf der Grundlage der definierten Rollen vordefiniert. Bei Änderungen an einer Position werden die zugehörigen Rechte und Zugriffsregeln entsprechend geändert.

Regelmäßig werden die Zugriffsrechte von den technischen Verantwortlichen auf der Grundlage der Bedürfnisse des Teams, den zu trennenden Aufgaben und den mit den Zugriffsrechten verbundenen Risiken abgeglichen.

Der Entzug von Rechten und Zugang sowie die Deaktivierung des Kontos im Falle des Austritts eines Mitarbeiters ("Offboarding") oder im Falle eines Positionswechsels wird vom IT-Service Desk durchgeführt, um den Zugang des Mitarbeiters zu löschen bzw. die Zugangsrechte anzupassen.

Berichtspflichtige Manager prüfen die Listen und tragen die erforderlichen Änderungen in den Ereignisverwaltungsdatensatz ein. Der Datensatz wird zur Bearbeitung an den Sicherheits-Helpdesk zurückgesandt. Der IT-Service-Desk-Manager identifiziert alle Einträge, die nicht innerhalb von zwei Wochen zurückgegeben werden, und setzt sich mit dem Manager in Verbindung.

Nur autorisierte Personen können auf Systeme zugreifen, die personenbezogene Daten verarbeiten. TeamViewer verwendet mehrere Berechtigungsstufen bei der Gewährung des Zugangs zu Systemen. Alle Mitarbeiter greifen über ein personalisiertes Konto (Benutzer-ID) auf die Unternehmenssysteme von TeamViewer zu und haben nur Zugriff auf die Systeme, auf die sie zur Erfüllung ihrer Aufgaben zugreifen müssen. Berechtigungen und Privilegien werden regelmäßig überprüft. Ebenso überprüft werden Rechte für den Zugriff auf Systeme, wenn Mitarbeiter neue Rollen zugewiesen bekommen oder TeamViewer verlassen.

2.2 Einstellung ("Onboarding") und Austritt ("Offboarding") von Mitarbeitern

Bei der Einstellung werden die Mitarbeiter einer Position im Personalverwaltungssystem zugewiesen. Vor dem Startdatum des Mitarbeiters erstellt das HR-Team ein sog. "Onboarding"-Ticket, das die Benutzer-IDs des Mitarbeiters und die zu gewährenden Zugriffsrechte enthält. Das Ticket wird vom IT-Service-Desk verwendet, um Benutzer-IDs und Zugriffsregeln zu erstellen. Die Zugriffsregeln sind nach dem Minimalprinzip definiert (jeder Mitarbeiter erhält nur die Berechtigungen, die er/sie benötigt, um seine/ihre Aufgabe zu erfüllen). Darüber hinaus enthält das Ticketsystem eine Vorlage für Mitarbeiter, die ihre Position und die damit verbundenen Rechte wechseln, die innerhalb der bestehenden Zugriffsregelungen entsprechend geändert werden müssen.

Regelmäßig werden die Zugriffsrechte der technisch Verantwortlichen überprüft, um festzustellen, ob diese widerrufen werden müssen. Bei der Bewertung der Zugriffsrechte berücksichtigen die Teamleiter die Stellenbeschreibung, die zu trennenden Aufgaben und die mit den Zugriffsrechten verbundenen Risiken.

Nach Kündigung des Arbeitsverhältnisses eines Mitarbeiters wird von der HR-Abteilung ein Offboarding-Ticket erstellt. Diese Tickets werden automatisch bearbeitet, um den Zugriff des Mitarbeiters in allen Systemen zu entfernen. Der IT-Service Desk verwendet die Tickets, um Benutzer-IDs zu sperren und alle Zugriffsrollen von IDs zu löschen, die dem Mitarbeiter des Tickets gehören. TeamViewer wird diese Listen regelmäßig überprüfen, um sicherzustellen, dass die automatischen Korrekturen korrekt umgesetzt wurden.

2.3 Datenzugriffskontrolle

TeamViewer kontrolliert den Zugriff auf Systeme, die personenbezogene Daten enthalten, durch eine Mischung aus rollenbasierter Zugriffskontrolle (role-based access control, sog. RBAC) und Benutzerrechteverwaltung. Dadurch wird sichergestellt, dass der Zugriff auf und die Nutzung von Daten sowohl in Bezug auf die allgemeine Verarbeitung als auch in Bezug auf die Liste und den Umfang des Zugriffs für TeamViewer-Mitarbeiter minimiert wird. Diese Zugriffskontrollen variieren in Abhängigkeit von der Sensibilität der gespeicherten Daten und den betrieblichen Anforderungen. Neben der Gewährung des Zugangs für einzelne Mitarbeiter kann für einige Systeme ein bestimmter Zugang für einen begrenzten Zeitraum mit einem Genehmigungsverfahren gewährt werden. Außerdem wird ein Workload Identity Federation genutzt, um den Zugang zu Ressourcen auf bestimmten Systemen zu gewähren.

2.4 Datentrennung

Netzwerke werden getrennt und segmentiert. Dies funktioniert im Rahmen von RBAC, um Risiken im Einklang mit fundierten Sicherheits- und Datenschutzpraktiken zu minimieren. So werden Daten für unterschiedliche Produkte/Zwecke, wenn möglich,

getrennt verarbeitet, u.a. durch Trennung von Produktions- und Testumgebungen. Wo zweckdienlich werden die Daten getrennt verarbeitet, um eine unnötige Vermischung von Daten und eine Verarbeitung über den Zweck hinaus zu vermeiden.

2.5 Pseudonymisierung

TeamViewer setzt die Pseudonymisierung dort ein, wo sie ohne Beeinträchtigung der Effizienz der Prozesse angewendet werden kann und/oder wo sie zum Schutz der Daten im Falle einer notwendigen Offenlegung von Daten notwendig ist. Wo es im Rahmen des Offenlegungsprozesses möglich ist, wird die Anonymisierung eingesetzt. Daten, die in pseudonymisierten Daten enthaltene Betroffenen identifizieren können, werden separat gespeichert und wenn möglich verschlüsselt.

TeamViewer verfügt über einen Prozess zur Bewertung der internen Datenweitergabe und verwendet Pseudonymisierung, um die Nutzung der personenbezogenen Daten für bestimmte Zwecke einzuschränken.

3 Maßnahmen zur Herstellung der Integrität

3.1 Weitergabekontrolle

Bei TeamViewer gibt es Weitergabekontrollen, die sicherstellen, dass die Daten während der Übertragung sicher sind und das Schutzlevel nicht unter einen Mindeststandard fällt, sobald sie den Perimeter verlassen.

Zu diesen Sicherheitsmaßnahmen gehören die Sicherung von Übertragungen mit SSL/TLS, https usw. und der Einsatz von VPNs im gesamten Unternehmen. TeamViewer unterhält Firewalls und andere Standardsicherheitssysteme, um den Betrieb und die Daten zu schützen.

Firewall-Systeme sind vorhanden, um nicht autorisierten eingehenden Netzwerkverkehr aus dem Internet zu filtern und jede Art von Netzwerkverbindung zu verweigern, die nicht ausdrücklich autorisiert ist.

3.2 Dateneingangsteuerung

TeamViewer hat Systeme im Einsatz, die protokollieren, wer auf personenbezogene Daten zugegriffen oder diese verändert hat, einschließlich der Verknüpfung solcher Kontrollen mit individuellen Accounts.

4 Datenverfügbarkeit und Belastbarkeit der Systeme

TeamViewer erstellt Backups von wichtigen Daten in Übereinstimmung mit gängiger Praxis und stellt sicher, dass diese Backups im Falle eines katastrophalen Ausfalls als zuverlässige Ausfallsicherung fungieren.

Die Kundendaten werden gesichert und von Mitarbeitern der Operations-Abteilung auf Vollständigkeit und Ausfälle überwacht. Im Falle eines Ausfalls führt die Operations-Abteilung eine Fehlerbehebung durch, um die Ursache zu identifizieren, und führt dann den Backup sofort oder als Teil des nächsten geplanten Backups erneut aus.

Die Backup-Infrastruktur ist physisch in verschlossenen Schränken und/oder Käfigumgebungen innerhalb der Rechenzentren von Drittanbietern gesichert. Die Backup-Infrastruktur befindet sich in privaten Netzwerken, die logisch von anderen Netzwerken gesichert sind.

Es existieren Richtlinien und Verfahren zur Reaktion auf IT-Vorfälle, die das Personal bei der Meldung von sowie den entsprechenden Umgang mit solchen Vorfällen anleiten. Es gibt Verfahren, um Sicherheitsverletzungen im System und andere Vorfälle zu erkennen, zu melden und darauf zu reagieren. Es gibt Verfahren zur Reaktion auf Vorfälle, um diese im Netzwerk zu erkennen und darauf zu reagieren.

TeamViewer überwacht die Auslastung der physischen und computergestützten Infrastruktur sowohl intern als auch für Kunden, um sicherzustellen, dass die Dienstleistung den Service Level Agreements entspricht.

TeamViewer evaluiert den Bedarf an zusätzlicher Infrastrukturkapazität als Reaktion auf das Wachstum bestehender Kunden bzw. die Aufnahme neuer Kunden. Die Überwachung der Infrastrukturkapazität umfasst unter anderem folgendes:

- Rechenzentrumsfläche, Strom und Kühlung

- Plattenspeicher
- Bandspeicher
- Netzwerk-Bandbreite

TeamViewer hat einen Patch-Management-Prozess implementiert, um sicherzustellen, dass die vertraglich vereinbarten Kunden- und Infrastruktursysteme in Übereinstimmung mit den vom Hersteller empfohlenen Betriebssystem-Patches gepatcht werden. TeamViewer-Systemverantwortliche überprüfen vorgeschlagene Betriebssystem-Patches, um festzustellen, ob die Patches angewendet werden.

TeamViewer ist dafür verantwortlich, das Risiko des Aufspielens oder Nichtaufspielens von Patches auf der Grundlage der Sicherheits- und Verfügbarkeitsauswirkungen dieser Systeme und aller kritischen Anwendungen, die darauf gehostet werden, zu bestimmen. TeamViewer-Mitarbeiter überprüfen, ob alle Patches installiert wurden und ob gegebenenfalls ein Neustart durchgeführt wurde.

Redundanz ist in die Systeminfrastruktur eingebaut, die die Dienste des Rechenzentrums unterstützt, um sicherzustellen, dass es keinen einzelnen Ausfallpunkt ("Single Point of Failure") gibt, der Firewalls, Router und Server umfasst. Wenn ein primäres System ausfällt, wird die redundante Hardware so konfiguriert, dass sie dessen Platz einnimmt.

Penetrationstests werden durchgeführt, um die Sicherheitslage eines Zielsystems oder einer Umgebung zu messen. Der beauftragter Drittanbieter verwendet eine von TeamViewer spezifizierte, branchenübliche Methodik für Penetrationstests. Der Ansatz des Drittanbieters beginnt mit einer Schwachstellenanalyse des Zielsystems, um festzustellen, welche Schwachstellen auf dem System vorhanden sind, die durch einen Penetrationstest ausgenutzt werden können, wobei ein verärgerter/betroffener Insider oder ein Angreifer simuliert wird, der sich internen Zugang zum Netzwerk verschafft hat.

Sobald die Schwachstellen identifiziert sind, versucht der Drittanbieter, die Schwachstellen auszunutzen, um festzustellen, ob ein unberechtigter Zugriff oder andere böswillige Aktivitäten möglich sind.

Penetrationstests umfassen Tests der Netzwerk- und Anwendungsebene sowie Tests der Kontrollen und Prozesse rund um die Netzwerke und Anwendungen und erfolgen sowohl von außen (externe Tests) als auch innerhalb des Netzwerks.

Schwachstellen-Scans werden täglich von TeamViewer in Übereinstimmung mit den internen Richtlinien durchgeführt. Auf Anfrage des Kunden und nach TeamViewers Ermessen kann auch ein Penetrationstest durch einen Drittanbieter gemäß den TeamViewer-Richtlinien erfolgen. Der Drittanbieter verwendet Industriestandard-Scantechnologien und eine formelle, von TeamViewer spezifizierte Methodik. Diese Technologien sind so angepasst, dass sie die Infrastruktur und Software des Unternehmens auf effiziente Weise testen und gleichzeitig die mit dem aktiven Scannen verbundenen potenziellen Risiken minimieren.

Re-tests und On-Demand-Scans werden je nach Bedarf durchgeführt. Schwachstellen-Scans werden außerhalb der Hauptgeschäftszeiten durchgeführt.

Tools, die im TeamViewer-System installiert werden müssen, werden über den Change-Management-Prozess implementiert. Das Scannen wird mit genehmigten Scan-Vorlagen und mit aktivierten Optionen zur Bandbreiten-Drosselung durchgeführt.

4.1 Incident Response Management

TeamViewer unterhält Notfallpläne, um auf potenzielle Sicherheitsbedrohungen zu reagieren. Der Incident-Response-Plan enthält definierte Prozesse zur Erkennung, Minderung, Untersuchung und Meldung von Sicherheitsvorfällen. Er umfasst die Überprüfung von Vorfällen, die Analyse von Angriffen, die Minderung, die Sammlung von Daten und die Behebung von Problemen.

Erlangt TeamViewer Kenntnis von einer Sicherheitsverletzung, die zur zufälligen oder unrechtmäßigen Zerstörung, zum Verlust, zur Veränderung, zur unbefugten Offenlegung oder zum Zugriff auf personenbezogene Daten des Kunden führt, während diese von TeamViewer verarbeitet werden, wird TeamViewer den Kunden über einen solchen Sicherheitsvorfall informieren, Informationen über den Sicherheitsvorfall zur Verfügung stellen und geeignete Maßnahmen ergreifen, um nachteilige Auswirkungen abzumildern und den Schaden durch den Sicherheitsvorfall zu minimieren, gemäß den Bestimmungen der Vereinbarung über die Datenverarbeitung.

Um über aktuelle Sicherheitsupdates informiert zu werden, kann ein Sicherheitsbulletin abonniert werden.

5 Datenschutzmanagement

TeamViewer unterhält umfassende Datenschutzrichtlinien und -verfahren, für die der Datenschutzbeauftragter (DSB) und das Management von TeamViewer letztlich verantwortlich sind. TeamViewer aktualisiert ständig seine Datenschutz- und Sicherheitsmaßnahmen im Einklang mit aktualisierten Richtlinien, Gesetzen und Best Practices. Dazu gehören regelmäßige Überprüfungen der Dokumentation von Verfahren, Schulungen sowie technischen und organisatorischen Maßnahmen, die Pflege und Erstellung von Verarbeitungsverzeichnisse und ggf. die Durchführung von Datenschutz-Folgenabschätzungen, einschließlich anderer relevanter Bewertungen.

TeamViewer verfügt über Prozesse, Richtlinien und Verfahren, die die physische Sicherheit, den logischen Zugriff, den Computerbetrieb, die Änderungskontrolle und die Datenkommunikationsstandards beschreiben. Alle Mitarbeiter sind verpflichtet, dass sie sich an die TeamViewer-Richtlinien und -Verfahren halten, die definieren, wie Dienstleistungen erbracht werden sollen. Diese befinden sich im Intranet des Unternehmens und können von jedem TeamViewer-Mitarbeiter eingesehen werden.

Die Mitarbeiter werden regelmäßig datenschutzrechtlich geschult und auf Vertraulichkeit verpflichtet. TeamViewer führt regelmäßige (mindestens einmal jährlich) Awareness-Schulungen für Mitarbeiter durch, deren Häufigkeit sich jedoch je nach Bedarf erhöhen kann.

TeamViewer benennt pro Abteilung mindestens eine verantwortliche Person, die für die Einhaltung und Umsetzung der Vorgaben der Datenschutz-Grundverordnung (DS-GVO) verantwortlich ist. Alle verantwortlichen Datenschutz-Mitarbeiter verfügen mindestens über eine für ihren Arbeitsbereich relevante IAAP CIPP-Qualifikation.

Eine Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen wird mindestens jährlich durchgeführt. Datenschutz-Folgenabschätzungen und andere relevante Bewertungen werden dann durchgeführt, wenn es notwendig ist.

Es gibt eine formalisierte Richtlinie für die Bearbeitung von Anfragen von Betroffenen unter der DS-GVO.

Alle Mitarbeiter werden intern gem. Art. 32 Abs. 4 DS-GVO geschult und sind verpflichtet, den datenschutzkonformen Umgang mit personenbezogenen Daten sicherzustellen.

Nach Beendigung des Vertragsverhältnisses mit einem Mitarbeiter werden die Daten datenschutzkonform gelöscht und dabei die Grundsätze der Datenminimierung berücksichtigt.

5.1 Unterauftragsverarbeiter

TeamViewer schließt Auftragsverarbeitungsverträge (AVV) mit allen Unterauftragsverarbeiter von personenbezogenen Daten. Ferner stellt TeamViewer sicher, dass alle Unterauftragsverarbeiter die jeweils einschlägigen Standards für Sicherheit und Datenschutz erfüllen und, dass diese Anforderungen und Verpflichtungen als Teil des AVVs aufgenommen werden. Die AVVs erfüllen die Anforderungen der DS-GVO einschließlich (sofern zutreffend) der neuesten Fassung der Standardvertragsklauseln.

Im Falle einer langfristigen Zusammenarbeit werden die Unterauftragsverarbeiter und das Schutzniveau der mit ihnen verarbeiteten Daten ständig überprüft.

6 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

Personenbezogene Daten werden nur in dem Umfang erhoben und verarbeitet, der für den vorgeschriebenen Zweck erforderlich ist. Den betroffenen Personen steht ein einfacher Weg offen, ihre Rechte auszuüben.

Bereits im Rahmen der Softwareentwicklung werden Grundsätze des Datenschutzes beachtet. Insbesondere sind die Mitarbeiter angehalten und geschult, technische und organisatorische Maßnahmen im Rahmen der Produktentwicklung umzusetzen, die die Einhaltung der Anforderungen der DS-GVO und speziell der Betroffenenrechte gewährleisten. Die Software wird grundsätzlich in der Art gestaltet, dass die Menge der erhobenen Daten sowie der Umfang der Verarbeitung auf das Erforderliche beschränkt ist. Insoweit verschiedene Einstellungsmöglichkeiten innerhalb der Software bestehen, ist im Auslieferungszustand immer die Einstellung gewählt, bei der die geringere Menge an personenbezogenen Daten verarbeitet wird, mit Ausnahme der Kernfunktionalitäten. Die Entwicklungsteams arbeiten eng mit dem Datenschutzteam zusammen, um sicherzustellen, dass die Datenschutzanforderungen in den Produkten von TeamViewer umgesetzt werden.

In Bezug auf die Änderungskontrolle unterhält TeamViewer dokumentierte Richtlinien und Verfahren des Software Development Life Cycle (SDLC), um das Personal bei der Dokumentation und Implementierung von Anwendungs- und Infrastrukturänderungen anzuleiten. Zu den Änderungskontrollverfahren gehören: Änderungsanforderungs- und -einleitungsprozesse, Dokumentationsanforderungen, Entwicklungspraktiken, Qualitätssicherungs-Testanforderungen und erforderliche Genehmigungsverfahren.

Ein Ticketingsystem wird verwendet, um die Änderungen in der Anwendung und die Implementierung neuer Änderungen zu dokumentieren (sog. Änderungskontrollverfahren).

Qualitätssicherungsprüfungen und -ergebnisse werden dokumentiert und zusammen mit der entsprechenden Änderungsanforderung gepflegt. Entwicklung und Tests werden in einer Umgebung durchgeführt, die logisch von der Produktionsumgebung getrennt ist. Das Management genehmigt die Änderungen vor der Migration in die Produktionsumgebung und dokumentiert diese Genehmigungen im Ticketing-System. Versionskontrollsoftware wird eingesetzt, um Quellcodeversionen zu verwalten und Quellcode durch den Entwicklungsprozess in die Produktionsumgebung zu migrieren. Die Versionskontrollsoftware verwaltet eine Historie der Codeänderungen, um Rollback-Funktionen zu unterstützen, und verfolgt die Änderungen für die Entwickler.

Alle Infrastrukturänderungen an der Umgebung werden vom Change Advisory Board (CAB) geprüft und genehmigt. Das CAB besteht mindestens aus dem Leiter der "IT-Infrastruktur", dem Leiter der "Anwendungs- und Bedarfsverwaltung", einem Mitglied des IT-Sicherheitsteams und dem Antragsteller der Änderung. Dadurch wird sichergestellt, dass alle Änderungen überprüft werden und die Qualität der Implementierung erhalten bleibt.

TeamViewer Germany GmbH

Bahnhofsplatz 2

73033 Göppingen

Deutschland

Anlage 3 zum Auftragsverarbeitungsvertrag

Liste der Unterauftragnehmer

Stand vom 9. März 2026

Die folgenden Unternehmen können Ihre personenbezogenen Daten als Unterauftrags-verarbeiter oder weitere Unterauftragsverarbeiter verarbeiten, je nach Vertragspartner.

1. Unterauftragnehmer für TeamViewer Produkte (außer Frontline, Engage/Co-Browsing und Classroom, siehe separaten Abschnitt unten)

Name	Standort	Leistung
Anexia Internetdienstleistungs GmbH	Feldkirchnerstraße 140, 9020 Klagenfurt, Österreich	Hosting
Amazon Web Services EMEA Sarl *(nicht für AssistAR)*	38 Avenue John F. Kennedy, L-1855 Luxemburg	Hosting
Microsoft Ireland Ltd.	South County Business Park, One Microsoft Place, Carmanhall and Leopardstown, Dublin, D18 P521, Irland	Hosting
Google Ireland Ltd.	Gordon House, Barrow Street, Dublin 4, Irland	Hosting
Schwarz Digits IT KG	Stiftsbergstraße 1, 74172 Neckarsulm, Germany	Hosting
TeamViewer Greece EPE	Leoforos Dodonis 147, 45221 Ioannina, Griechenland	Wartung und Entwicklung
TeamViewer Portugal, Unipessoal Lda	Rua Manuel Pinto de Azevedo, 860, 7º, 4100-320 Porto, Portugal	Wartung und Entwicklung
TeamViewer Austria GmbH	Graben 5, 4020 Linz, Österreich	Wartung und Hosting
TeamViewer Germany GmbH	Bahnhofsplatz 2, 73033 Göppingen, Deutschland	TeamViewer Produkte und Services

Zusätzliche Funktionen bei separater Bestellung oder Aktivierung der jeweiligen Funktionsmodule		
Malwarebytes Inc. (*gilt nur für die Funktionsmodule Threatdown Endpoint Protection/ Endpoint Detection & Response*)	3979 Freedom Circle, Santa Clara, CA 95054, USA	Threatdown Endpoint Protection; Endpoint Detection & Response *(optional)*
Lansweeper NV (*gilt nur für Asset Management und Discovery*)	Fraterstraat 212, 9820 Merelbeke, Belgien	Asset Management und Discovery *(optional)*
Ivanti UK Limited *(gilt nur für Mobile Device Management)*	3 Arlington Square Downshire Way, Bracknell, RG12 1WA, Großbritannien	Mobile Device Management *(optional)*
1E Limited	2nd Floor Midas House, 62 Goldsworth Road, Woking, Surrey, GU21 6LQ, Großbritannien	DEX-Dienste (*optional*, Hosting-Standort wie vereinbart)
Workato, Inc.	215 Castro St., Suite 300, Mountain View, CA 94041, USA	Automations (*optional*, EU Hosting-Standort)
Ausschließlich für Verbindungen nach und von China		
Alibaba.com (Europe) Limited	Herengracht 448, 1017 CA, Amsterdam, die Niederlande	Hosting

2. Unterauftragnehmer für TeamViewer Frontline

Name	Standort	Leistung
Microsoft Ireland Ltd.	South County Business Park, One Microsoft Place, Carmanhall and Leopardstown, Dublin, D18 P521, Irland	Hosting
TeamViewer Greece EPE	Leoforos Dodonis 147, 45221 Ioannina, Griechenland	Wartung und Entwicklung
TeamViewer Portugal, Unipessoal Lda	Rua Manuel Pinto de Azevedo, 860, 7º, 4100-320 Porto, Portugal	Wartung und Entwicklung
Google Ireland Ltd.	Gordon House, Barrow Street, Dublin 4, Irland	Hosting

TeamViewer Germany GmbH	Bahnhofsplatz 2, 73033 Göppingen, Deutschland	TeamViewer Produkte und Services
Zusätzliche Funktionen, nur auf spezielle Anfrage oder unter besonderen Umständen		
Twilio Inc. (*nur auf Wunsch des Kunden*)	375 Beale Street, Suite 300, San Francisco, Kalifornien 94105, USA	Hosting von Video- und Audio-Stream (*optional*)
Business Objects Software Limited (“**SAP**”) (*gilt nur für Kunden, die das SAP Global Partner Support Center nutzen*)	1012 - 1014 Kingswood Avenue, Citywest Business Campus, Dublin 24, Irland	Hosting des Kunden-Support-Portals (*optional*)

3. Unterauftragnehmer für TeamViewer Engage/ Co-Browsing/ Classroom

Name	Standort	Leistung
Amazon Web Services EMEA Sarl	38 Avenue John F. Kennedy, 1855 Luxemburg	Hosting
Hetzner Online GmbH	Industriestraße 25, 91710 Gunzenhausen, Deutschland	Hosting
TeamViewer Greece EPE	Leoforos Dodonis 147, 45221 Ioannina, Griechenland	Wartung und Entwicklung
TeamViewer Portugal, Unipessoal Lda	Rua Manuel Pinto de Azevedo, 860, 7º, 4100-320 Porto, Portugal	Wartung und Entwicklung
TeamViewer Austria GmbH	Graben 5, 4020 Linz, Österreich	Wartung und Hosting. Hosting-Standorte für Engage/ Co-Browsing: für alle Kunden – EU; nur für japanische Kunden – Japan Hosting-Standorte für Classroom: EU

TeamViewer Germany GmbH	Bahnhofsplatz 2, 73033 Göppingen, Deutschland	TeamViewer Produkte und Services

4. Unterauftragnehmer für TeamViewer DEX-Dienste

Name	Standort	Leistung
Atlassian Pty Ltd.	350 Bush Street Floor 13 San Francisco, CA 94104 USA	Kundensupport, KI-Dienste
Datadog Inc.	620 8th Ave 45th Floor, New York, NY 10018, USA	Monitoring und Logging
Microsoft Ireland Ltd.	South County Business Park, One Microsoft Place, Carmanhall and Leopardstown, Dublin, D18 P521, Irland	Hosting
Outsystems Inc.	55 Thomson Place, 2nd floor, Boston MA 02210, USA	Entwicklungsplattform für Design und die Bereit-stellung von DEX-Diensten
Pendo.io, Inc.	Raleigh, 301 Hillsborough St, Suite 1900, USA	1E Anwendung UI
1E Limited	2nd Floor Midas House, 62 Goldsworth Road, Woking, Surrey, GU21 6LQ, Großbritannien	DEX-Dienste (Hosting-Standort wie vereinbart)
ThoughtSpot Inc.	444 Castro Street, Suite 1000 Mountain View, CA 94041, USA	Anpassbares Reporting
Project Hosts Inc.	201 N. Spence Ave. STE 101 Goldsboro, NC 27534, USA	Hosting (nur für FedRAMP Instanzen)

5. Professional Services und Support

Name	Standort	Leistung
TeamViewer Affiliates	Affiliated Companies	Professional Services, Service Level Support und Kunden-Support