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 Auftragsverarbeitungs-vertrag

Einzelheiten der Verarbeitung – TeamViewer Produkte

Stand vom 27. Juli 2026

1 Gegenstand der Verarbeitung

Gegenstand der Datenverarbeitung im Rahmen dieses AVV ist die Bereitstellung und Nutzung der TeamViewer-Software und -Services, wie in der TeamViewer Endnutzer-Lizenzvereinbarung („**EULA**“) sowie in sonstigen anwendbaren Vereinbarungen („**Vertrag**“) und der jeweils geltenden Produktspezifikation beschrieben.

2 Dauer der Verarbeitung

Die Verarbeitung personenbezogener Daten erfolgt für die Dauer der Vereinbarung. Nach Beendigung der Vereinbarung darf TeamViewer personenbezogene Daten verarbeiten, soweit dies zur Erfüllung anwendbarer gesetzlicher Verpflichtungen oder dokumentierter Weisungen des Kunden erforderlich ist.

3 Art und Zweck der Verarbeitung

TeamViewer wird personenbezogene Daten als Auftragsverarbeiter des Kunden verarbeiten, um die Nutzung der im Rahmen des Vertrags 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.

Die weitere Spezifikation der Software und Services finden Sie auf der Produktspezifikationsseite. Die Verarbeitung außerhalb des Geltungsbereichs dieses Vertrags wird in der jeweiligen Datenschutzinformation beschrieben.

TeamViewer wird je nach den vom Kunden genutzten TeamViewer Produkten die folgenden Verarbeitungstätigkeiten im Auftrag des Kunden durchführen:

- **Zugriffs- und Sitzungsmanagement.** Ermöglichung, Aufbau und Durchführung von Remote-Zugriffs-, Support-, Kollaborations- und Kommunikationssitzungen zwischen Geräten, Systemen und Benutzern

- **Daten- und Inhaltsverarbeitung.** Übermittlung, Anzeige, Hosting, Speicherung und Synchronisierung von Daten und Inhalten, die durch den Service verarbeitet werden, insbesondere Bildschirminhalte, Audio- und Videostreams, Chatnachrichten, Dateien und sonstige Kollaborationsartefakte

- **Identitäts- und Berechtigungsmanagement.** Bereitstellung, Administration und Absicherung von Benutzerkonten, Identitäten, Rollen, Berechtigungen und kundenspezifischen Konfigurationen

- **Geräte- und Endpoint-Management.** Unterstützung der Remote-Erkennung, Überwachung, Konfiguration, Administration und Verwaltung von Endpoints, Geräten sowie zugehörigen IT-Assets und Umgebungen

- **Verarbeitung operativer Daten.** Erhebung und Verarbeitung technischer, diagnostischer und operativer Daten, die für den Betrieb der Services erforderlich sind
- **Reporting.** Bereitstellung kundenbezogener Dashboards, Berichte und Ansichten in Bezug auf die Umgebung des Kunden
- **Integrationen und Datenaustausch.** Ermöglichung von Integrationen und Datenaustausch, die vom Kunden mit Drittsystemen oder -services konfiguriert werden
- **Support und Professional Services.** Bereitstellung von Kundensupport, Professional Services, Wartung, Fehlerbehebung und damit verbundener Serviceunterstützung auf Anfrage des Kunden
- **Protokollierungs- und Audit-Funktionen.** Unterstützung von Sitzungsberichten, Protokollierungs- und Audit-Funktionen, die vom Kunden konfiguriert werden
- **Künstliche Intelligenz und automatisierte Verarbeitung.** Verarbeitung von durch Benutzer übermittelten Eingaben und kontextbezogenen Sitzungsdaten für automatisierte oder KI-unterstützte Funktionalitäten, soweit diese in den Services enthalten sind
- **Analysen und Erkenntnisse.** Ermöglichung von Leistungsanalysen für Endpunkt-Geräte und Erkenntnissen zur Benutzer-Geräte-Interaktion, soweit vom Kunden lizenziert

4 Art der personenbezogenen Daten

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

Produkt & Service	Art der verarbeiteten personenbezogenen Daten (Details unten)
TeamViewer Remote (Business, Corporate, Premium)	Konten- und Identitätsdaten; Sitzungs- und Verbindungsdaten; Geräte- und Endpunkte-Daten; Inhaltsdaten; Integrations- und Konfigurationsdaten; KI-Eingabe- und Ausgabedaten (soweit aktiviert)
TeamViewer Tensor	Konten- und Identitätsdaten; Sitzungs- und Verbindungsdaten; Geräte- und Endpunkte-Daten; Inhaltsdaten; Integrations- und Konfigurationsdaten; KI-Eingabe- und Ausgabedaten (soweit aktiviert)

Produkt & Service	Art der verarbeiteten personenbezogenen Daten (Details unten)
TeamViewer Remote Management	Konten- und Identitätsdaten; Sitzungs- und Verbindungsdaten; Geräte- und Endpunkte-Daten
TeamViewer ONE	Konten- und Identitätsdaten; Sitzungs- und Verbindungsdaten; Geräte- und Endpunkte-Daten; Inhaltsdaten; DEX-Daten; Integrations- und Konfigurationsdaten; KI-Eingabe- und Ausgabedaten (soweit aktiviert)
TeamViewer DEX	Konten- und Identitätsdaten; Geräte- und Endpunkte-Daten; DEX-Daten; Integrations- und Konfigurationsdaten; KI-Eingabe- und Ausgabedaten (soweit aktiviert)
TeamViewer Frontline	Konten- und Identitätsdaten; Sitzungs- und Verbindungsdaten; Geräte- und Endpunkte-Daten; Inhaltsdaten; Integrations- und Konfigurationsdaten
TeamViewer Engage	Konten- und Identitätsdaten; Sitzungs- und Verbindungsdaten; Inhaltsdaten
TeamViewer Co-Browsing	Konten- und Identitätsdaten; Sitzungs- und Verbindungsdaten; Inhaltsdaten
TeamViewer Classroom	Konten- und Identitätsdaten; Sitzungs- und Verbindungsdaten; Inhaltsdaten
TeamViewer Meeting	Konten- und Identitätsdaten; Sitzungs- und Verbindungsdaten; Inhaltsdaten
TeamViewer Assist AR	Sitzungs- und Verbindungsdaten; Geräte- und Endpunkte-Daten; Inhaltsdaten; KI-Eingabe- und Ausgabedaten (soweit aktiviert)
TeamViewer IoT	Geräte- und Endpunkte-Daten; Integrations- und Konfigurationsdaten

Produkt & Service	Art der verarbeiteten personenbezogenen Daten (Details unten)
TeamViewer Support, Service Level Support & Professional Services	Support- und Servicedaten

4.1 Konten- und Identitätsdaten

Personenbezogene Daten im Zusammenhang mit Benutzerkonten und Identitäten, insbesondere:

- Namen und Anzeigenamen
- Benutzernamen und Benutzer-IDs
- E-Mail-Adressen
- Authentifizierungsdaten
- Kontokennungen
- Rollen- und Berechtigungszuweisungen
- Kontaktlisten
- Informationen zum Unternehmensprofil

4.2 Sitzungs- und Verbindungsdaten

Personenbezogene Daten, die im Zusammenhang mit dem Aufbau und der Durchführung von Sitzungen entstehen, insbesondere:

- Sitzungskennungen
- Zeitstempel
- IP-Adressen
- Verbindungsmetadaten
- Gerätekennungen
- Meeting-Kennungen
- Authentifizierungs- oder Sitzungstoken
- Verbindungsberichte und Audit-Protokolle

4.3 Geräte- und Endpunkte-Daten

Technische Daten in Bezug auf vom Kunden verwaltete oder vom Kunden genutzte Geräte, insbesondere:

- Gerätenamen und Gerätekennungen
- Hardware- und Softwareinventar
- Betriebssysteminformationen
- Konfigurationsstatus
- Patch-Status
- Sicherheitswarnungen
- Daten zur virtuellen Desktop-Umgebung
- IoT-Gerätekennungen

4.4 Inhaltsdaten

Inhalte, die von Benutzern während Sitzungen oder Kommunikation übertragen oder bereitgestellt werden, insbesondere:

- Bildschirminhalte
- Audio- und Videostreams
- Chatnachrichten
- Übertragene Dateien
- Anmerkungen
- Whiteboard-Inhalte
- Workflow-Dokumente
- Visuelle Augmented-Reality-Daten
- Aufzeichnungen, Transkripte, Zusammenfassungen und sonstige Inhalte, die aus Sitzungen generiert werden oder mit Sitzungen verbunden sind

4.5 Support- und Servicedaten

Personenbezogene Daten, die im Zusammenhang mit vom Kunden initiierten Supportanfragen, Fehlerbehebungsmaßnahmen oder Professional-Services-Leistungen verarbeitet werden, insbesondere:

- Supportanfragen und Ticketinhalte
- Hochgeladene Diagnosedateien, Protokolle oder Berichte
- Sitzungsaufzeichnungen, Screenshots oder sonstige vom Kunden bereitgestellte Materialien
- Geräte- oder Verbindungsmetadaten, die zur Problemanalyse übermittelt werden
- Serviceberichte
- Sonstige personenbezogene Daten, die vom Kunden im Rahmen von Supportanfragen bereitgestellt werden

4.6 Digital Employee Experience (DEX)-Daten

Technische und Nutzungsdaten, die von vom Kunden verwalteten Geräten im Zusammenhang mit Funktionen der Digital Employee Experience (**DEX**) generiert werden, insbesondere:

- Geräteleistungsmetriken
- Betriebssystem- und Netzwerkleistungsdaten
- Anwendungsleistungs- oder Absturzberichte
- Software-Interaktionsdaten
- Metriken zur virtuellen Desktop-Erfahrung
- Analysen zur Benutzer-Geräte-Interaktion
- Antworten auf Experience-Umfragen

4.7 Integrations- und Konfigurationsdaten

Personenbezogene Daten, die im Zusammenhang mit vom Kunden konfigurierten Integrationen oder Automatisierungen verarbeitet werden, insbesondere:

- Daten, die mit angebundenen Drittsystemen ausgetauscht werden
- Integrationsmetadaten
- Jeweils anwendbare Zugangsdaten
- Konfigurationsdaten der SaaS-Lösung

4.8 KI-Eingabe- und Ausgabedaten

Soweit KI-unterstützte Funktionalitäten durch den Kunden aktiviert werden:

- Interaktionen der Benutzer während der Sitzung
- Kontextbezogene Sitzungsdaten
- Von Benutzern eingegebene Daten
- Von Benutzern hochgeladene Dateien
- Generierte Ausgaben, die aus vom Benutzer initiierten Eingaben abgeleitet werden

5 Kategorien von betroffenen Personen

TeamViewer verarbeitet im Auftrag des Kunden, abhängig von dessen Konfiguration und Nutzung der TeamViewer Produkte und Services, personenbezogene Daten der folgenden Kategorien betroffener Personen:

- Mitarbeiter, Auftragnehmer und andere vom Kunden autorisierte Nutzer
- Endnutzer von Geräten, die vom Kunden verwaltet, unterstützt oder genutzt werden
- Teilnehmer von Verbindungen, Sitzungen oder Meetings, die mit dem Kunden interagieren
- Administratoren, die im Auftrag des Kunden handeln
- Nutzer sowie sonstige Dritte, die über Kommunikationsfunktionen mit dem Kunden interagieren
- Dritte, deren personenbezogene Daten auf dokumentierte Weisung des Kunden verarbeitet werden

TeamViewer

Übersicht der technisch-organisatorischen Maßnahmen

Stand vom 17. März 2025

Inhalt

1 Zugangskontrolle 2

1.1 Datenzentren 2

1.2 TeamViewer-Büros 3

2 System-Zugangs- und Zugriffskontrolle 3

2.1 Netzwerk- und Hardwaresicherheit 3

2.2 Einstellung (“Onboarding”) und Austritt (“Offboarding”) von Mitarbeitern 4

2.3 Datenzugriffskontrolle 4

2.4 Datentrennung 4

2.5 Pseudonymisierung 5

3 Maßnahmen zur Herstellung der Integrität 5

3.1 Weitergabekontrolle 5

3.2 Dateneingangsteuerung 5

4 Datenverfügbarkeit und Belastbarkeit der Systeme 5

4.1 Incident Response Management 6

5 Datenschutzmanagement 6

5.1 Unterauftragsverarbeiter 7

6 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen 7

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

TeamViewer

Anlage 3 zum Auftragsverarbeitungsvertrag

Liste der Unterauftrag-nehmer

Stand vom 27. Juli 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, Deutschland	Hosting
MongoDB, Inc. (*nur für Assist AR*)	1633 Broadway, 38th Floor, New York, NY 10019, USA	Database Hosting (*EU Hosting-Standort*)
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
Lansweeper NV (*gilt nur für Asset Management und Discovery*)	Fraterstraat 212, 9820 Merelbeke, Belgien	Asset Management und Discovery
Ivanti UK Limited *(gilt nur für Mobile Device Management)*	3 Arlington Square Downshire Way, Bracknell, RG12 1WA, Großbritannien	Mobile Device Management
1E Limited	2nd Floor Midas House, 62 Goldsworth Road, Woking, Surrey, GU21 6LQ, Großbritannien	DEX- Dienste (*Hosting-Standort wie vereinbart*)
Workato, Inc.	215 Castro St., Suite 300, Mountain View, CA 94041, USA	Workflow Automations (*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
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.	375 Beale Street, Suite 300, San Francisco, Kalifornien 94105, USA	Video- und Audio-Streaming
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

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
MongoDB, Inc.	1633 Broadway, 38th Floor, New York, NY 10019, USA	Database Hosting (*EU Hosting-Standort)*
TeamViewer Austria GmbH	Graben 5, 4020 Linz, Österreich	Hosting
TeamViewer Germany GmbH	Bahnhofsplatz 2, 73033 Göppingen, Deutschland	TeamViewer Produkte und Services

4. Unterauftragnehmer für TeamViewer DEX-Dienste

Name	Standort	Leistung
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,	Entwicklungsplattform

	Boston MA 02210, USA	für Design und die Bereitstellung von DEX-Diensten
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	Integrierte Analytik für Tia 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