Zoom X

Whitepaper Datenschutz und Sicherheit

Version 1.0
07. September 2022

Erleben,
was verbindet.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

Neben der Telefonie sind Videokonferenzen für viele Unternehmen und Behörden zu einem unverzichtbaren Bestandteil der Kommunikation geworden. Geschäftspartner, Kunden und Projektteams, die sich an unterschiedlichen Orten befinden, können gemeinsam arbeiten und Ergebnisse effizient erzielen. So können beispielsweise in Videokonferenzen Dokumente gemeinsam diskutiert und bearbeitet werden.

Zeitaufwendige Terminabsprachen und kostenintensive Anreisen werden dank der modernen Kommunikationskanäle minimiert. Vielmehr werden spontane Entscheidungen sowie schnelle Ergebnisse ermöglicht, um die Effizienz des Unternehmens nachhaltig zu steigern. Zudem schont diese innovative Art Konferenzen und Meetings durchzuführen die Umwelt, da die Videokonferenzen der Telekom CO2-neutral angeboten werden.

Moderne Kommunikationstools, wie Zoom, sind spätestens seit der pandamiebedingten Einschränkungen aus dem Arbeitsalltag der Verwaltungen und Unternehmen nicht mehr wegzudenken. Daher hat die Deutsche Telekom gemeinsam mit Zoom eine Lösung entwickelt, die einerseits den Bedarf der Anwender nach einer intuitiven und innovativen App und anderseits die Anforderungen der Datenschützer und IT-Sicherheitsveranwortlichen adressiert.

Das hier vorliegende Whitepaper beschreibt detailliert die Videokonferenzlösung von Zoom X powered by Telekom. Im einzelnen sind es die Applikationen Zoom X One (Meetings), Zoom X Phone, Zoom X Rooms, Zoom X CRC, Zoom X Education, Zoom X Webinare. Die einzelnen Angebote unterscheiden sich durch verschiedene Leistungsmerkmale.

Dieses Whitepaper für Zoom X beschreibt die Verarbeitung von Informationen von oder über eine identifizierte oder identifizierbare Person ("Persönliche Daten") durch Zooms X One, Zoom X Webinar und Zoom X Phone (zusammenfassend "Zoom X"). Dieses Whitepaper gilt für Organisationen und Einzelpersonen, die durch den Erwerb eines Zoom-Kontos ("Kunden") Zoom X Dienste nutzen.

Dieses Whitepaper spezifiziert unsere Datenschutzerklärung, und beschreibt die Verarbeitung von personenbezogenen Daten, um die Dienstleistungen für unsere Kunden zu erbringen, sowie andere Datenschutzangelegenheiten wie internationale Datenübertragungen und Datenstandort. Es schafft keine zusätzlichen Rechte oder Rechtsmittel und sollte nicht als verbindliche Vereinbarung ausgelegt werden. Bitte kontaktieren Sie uns unter datenschutz@telekom.de, wenn Sie Fragen oder Anmerkungen haben.

2 Zoom X - Architektur

2.1 Zoom X High Level Architektur

Das High Level Architekturschaubild veranschaulicht in vereinfachter Weise die speziell von Telekom und Zoom aufgebaute Back-End Infrastruktur von Zoom X einschließlich der Zoom-Services, die außerhalb der bereitgestellten Installation genutzt werden.

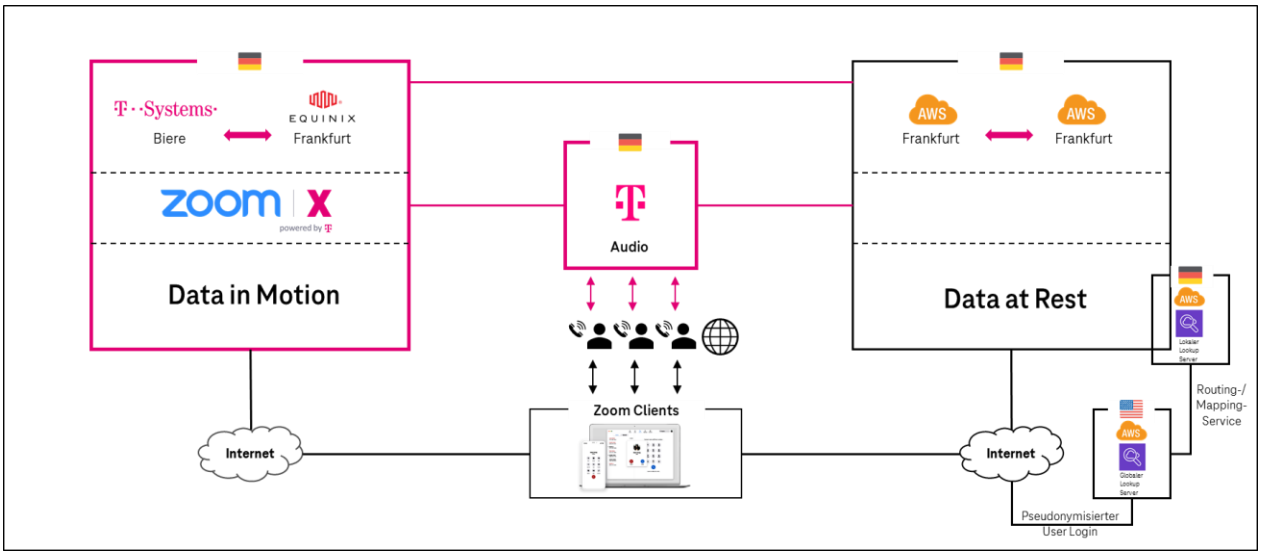

Abbildung 1: High Level Architektur von Zoom X

Data in Motion - Zoom Real-Time Media & Signalling

Die Verarbeitung der, während eines Meetings erzeugten, Real-Time Daten findet im T-Systems Rechenzentrums in Biere bei Magdeburg statt. Als georedundantes Rechenzentrum für den Disaster-Recovery-Verbund erfolgt ein Housing im Equinix Rechenzentrum in Frankfurt. In den Rechenzentren der T-System und bei Equinix sind Services für Zoom Real-Time Media & Signalling installiert. Das sind die „Data in Motion“ für Zoom X One, Webinare, Rooms, CRC & Phone, wie z. B. Recording, Audio.

Data at Rest - Zoom (Services für Web & Data)

Die sog. Data-at-Rest werden durch Zoom in Amazon Web-Services (AWS) Rechenzentren (redundant) in Frankfurt verarbeitet. In diesen Rechenzentren werden selektive Backend Systeme Web- und Data-Service verwendet. Das sind die „Data at Rest“ für Zoom X One & Phone – wie z. B. Benutzerprofile, Meeting-Aufzeichnungen, Meeting Meta- & Telemetriedaten, Dashboards/ Berichte und persistente Chats.

Audio

Die Audiozuführungen für Zoom X One und Zoom X Phone stellt die Telekom zur Verfügung. Die Audionutzung wird überwiegend aus dem Zoom Client vom Nutzer angesteuert. Bei Zoom X One werden Einwahlrufnummern für über 50 Ländern bereitgestellt, die bei der Telekom zusammengeführt werden. Bei Zoom X Phone kommt es je nach Nutzung des Audioprodukts - Company Flex oder C SIP Germany/International - darauf an, welche Plattform angesteuert wird:

1. Company Flex, Telekom nutzt eine Plattform in den Niederlanden
2. CSIP-Germany (CSIP-G) / CSIP-International (CSIP-I)
    a. CSIP-Germany Telekom nutzt eine Plattform in Frankfurt und/oder

b. C SIP International Telekom nutzt eine Plattform in Österreich.

Zoom Clients & globaler und lokaler Lookup Service

Aus der Abbildung 1: High Level Architektur von Zoom X wird im untenstehendem Sequenzdiagramm der Ablauf zwischen den Lookup Servern detaillierter dargestellt. Um das richtige Rechenzentrum (Biere/Frankfurt) via Internet anzusteuern, verbindet sich der Zoom Client vorab über das Internet mit einem Lookup-Service in den USA. Die Telekom arbeitete mit der Firma Zoom ein Konzept aus, das garantiert, dass keine persönlichen Klartextinformationen in die USA gesendet werden, sondern diese vorab pyseudonymisiert werden und damit nicht von Zoom USA ausgelesen werden können.

Zoom verfügt über einen Lookup-Service, der sowohl in den USA (global) als auch in Deutschland (lokal) ansässig ist. Dabei handelt es sich um einen Routing-/Mapping-Service, der dabei hilft, festzustellen, in welchem Cluster sich ein Nutzer befindet oder von wo aus ein Meeting stattfindet. Zoom verfügt über ein Backend-System, in dem die Daten sowohl in den USA und Deutschland als auch in anderen Ländern gespeichert sind, um die Daten im jeweiligen Land zu halten. Dies wird bei Zoom als Cluster bezeichnet.

Das Diagramm stellt den Ablauf bezogen auf den regulären Login-Prozess dar. Dies ist nicht auf SSO anwendbar.

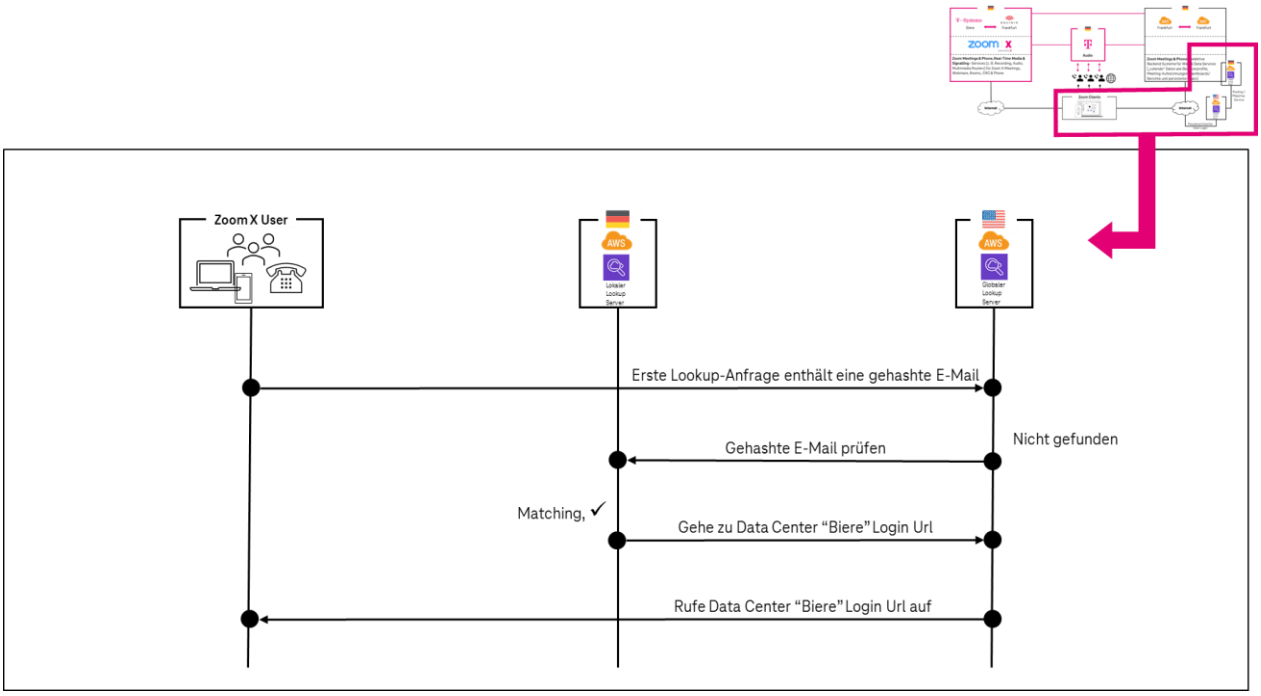

Abbildung 2: Zoom X Lookup Sequenzdiagramm

2.2 Zoom X Besonderheiten

Die Funktionen in der untendargestellten Tabelle weisen Besonderheiten auf, die zu beachten sind und ggf. manuell für ein Unternehmen angepasst werden müssen.

Funktion	Besonderheiten	Anmerkungen
Marketplace Anwendungen und APIs	Marketplace & APIs sind derzeit US-basierte Komponenten.	Die Nutzung von Marketplace Anwendungen und API's kann „per default" deaktiviert sein (Vorkonfiguration beim Roll-Out).
Mobile Push-Mitteilungen (Mobile Push Notifications)	Nur bei Nutzung der Zoom App auf mobilen Endgeräten relevant. Es gelten die gültigen Datenschutzhinweise von Google und Apple.	Push-Notifications können für Nutzer vom Admin aktiviert bzw. deaktiviert werden.
In der Zoom Cloud gehostete Meetings/Webinare	Zoom X-Nutzer, die als Gast bzw. Teilnehmer einem Zoom Cloud-Meeting beitreten, profitieren nicht vom erweiterten Datenschutz der Zoom X Lösung.	
Firmenübergreifender persistenter Chat	Wenn der Initiator des Chats ein Zoom X User ist, dann verbleiben die Chat-Nachrichten innerhalb der Zoom X Rechenzentren. Wird ein Nicht-Zoom X User in den Chat-Raum eingeladen, sind die Chat-Nachrichten natürlich auch außerhalb der Zoom X Architektur verfügbar. Gleiches gilt wenn ein Nicht-Zoom X User einen Zoom X in den Chat einlädt.	
Für Vertrauen und Sicherheit gemeldete Probleme (Issues reported for Trust & Safety)	Wenn ein Teilnehmer während oder nach dem Meeting das Zoom Trust & Safety Center aktiviert, um Missbrauch zu melden, werden die entsprechenden Informationen in die USA geleitet.	Ein Datentransfer in die USA findet nur statt, wenn es eine Meldung durch einen User gibt.
User Feedbacks (NPS, ...)	Derzeit wird dieses optionale Feedback an ein US-basiertes System gesendet.	Die Abfrage zum Nutzer Feedback kann durch den Admin aktiviert bzw. deaktiviert werden.

Tabelle 1: Zoom X Besonderheiten

2.3 Zoom X Updates/Upgrades/Bugfixing

Zoom X und Zoom sind auf der Client-Seite identisch. Daher werden neue Funktionen und Sicherheitspatches zeitgleich zur Verfügung stehen.

3 Sicherheit & Datenschutz

3.1 Datenschutzrollen und Verarbeitungszwecke

Der Schutz Ihrer persönlichen Daten hat für die Telekom Deutschland GmbH einen hohen Stellenwert. Es ist uns wichtig, Sie darüber zu informieren, welche persönlichen Daten erfasst werden, wie diese verwendet werden und welche Gestaltungsmöglichkeiten Sie dabei haben.

Alle Daten, die Sie der Telekom anvertrauen, werden auf Basis gültiger Rechtsgrundlagen wie beispielsweise dem Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) oder der Europäischen Datenschutzgrundverordnung (EU-DSGVO) verarbeitet und von unseren Mitarbeitenden zur Erbringung bestimmter Leistungen vertraulich behandelt.

Grundsätzlich gelten für die Verarbeitung bei der Telekom die allgemeinen Datenschutzhinweise unter sowie ergänzend weitere produktspezifische Hinweise wie bspw. die für Mehrwertlösungen.

Bei einigen Produkten – dazu gehört auch Zoom X - verarbeiten wir Ihre personenbezogenen Daten (z. B. die Ihrer Mitarbeiter oder Kunden) in Ihrem Auftrag. Dazu ist ein gesonderter Vertrag zur Auftragsverarbeitung nach Artikel 28 Datenschutz-Grundverordnung erforderlich. Diesen Vertrag haben wir nach den Anforderungen der Datenschutz-Grundverordnung angepasst.

Für individuelles Vertragsgeschäft erhalten Sie als Auftraggeber automatisch einen auf das Produkt Zoom X passend zugeschnittenen Auftragsverarbeitungsvertrag (AVV). Dieser enthält alle relevanten Angaben zur Datenverarbeitung durch die Telekom und nachgelagerter Unterauftragsverarbeiter.

Die Verträge zu AGB-Produkten haben wir hier als „Ergänzende Bedingungen Auftragsverarbeitung (AV)“ (ErgBAV) veröffentlicht. Das bedeutet: die veröffentlichten Regelungen gelten automatisch als ergänzende Bedingungen.

Warum die Deutsche Telekom persönliche Daten verarbeitet
Die Deutsche Telekom verarbeitet personenbezogene Daten als Auftragsverarbeiter nur für die folgenden Zwecke:

- Bereitstellung und Aktualisierung der lizenzierten, konfigurierten und von unseren Kunden und ihren Nutzern verwendeten Zoom-Dienste, die von unseren Kunden und ihren Nutzern genutzt werden, einschließlich der Nutzung von Zoom-Einstellungen, Administratorsteuerungen oder anderen Servicefunktionen,
- um die Zoom-Dienste zu sichern und zu schützen,
- um Probleme und Fehler zu beheben,
- Unterstützung der Kunden auf Anfrage, einschließlich der Anwendung von Erkenntnissen aus individuellen Kundenanfragen zum Nutzen aller Zoom-Kunden, jedoch nur in dem Maße, wie diese Erkenntnisse anonymisiert sind,
- zur Ausführung von Anweisungen, die vom Kunden ausdrücklich in einem schriftlichen Dokument genehmigt wurden.

Die Deutsche Telekom verarbeitet personenbezogene Daten, die durch die Bereitstellung der Dienste als Verantwortlicher (wie in der DSGVO definiert) nur für folgende Zwecke:

- zur Verwaltung der Geschäftskonten des Kunden (z. B. Rechnungsstellung, Marketingkommunikation mit Beschaffungs- oder Vertriebsmitarbeitern) und damit verbundene Kundenkorrespondenz (z. B. Kommunikation über notwendige Aktualisierungen),

- zur Erfüllung und Lösung rechtlicher Verpflichtungen, einschließlich der Beantwortung von Datenanfragen zu personenbezogenen Daten, die von Zoom als Controller verarbeitet werden (z. B. Website-Daten), steuerliche Anforderungen, Vereinbarungen und Streitigkeiten,
- zur Erkennung, Verhinderung und zum Schutz von Missbrauch (z. B. automatisches Scannen nach Übereinstimmungen mit Kennungen von bekanntem Material über sexuellen Kindesmissbrauch ("CSAM"), Viren und Scannen zur Erkennung von Verstößen gegen die Nutzungsbedingungen (z. B. Urheberrechtsverletzungen, SPAM und Handlungen, die gegen Zoom Community Standards und Zoom Nutzungsbedingungen verstoßen).

Zoom verarbeitet pseudonymisierte Daten oder aggregierte Daten als Verantwortlicher für:

- die Verbesserung und Optimierung der Leistung und der Kernfunktionalitäten,
- der Zugänglichkeit, des Datenschutzes, der Sicherheit und der Effizienz der IT-Infrastruktur der Dienste, einschließlich zoom.us, explore.zoom.us, und support.zoom.us,
- interne Berichterstattung, Finanzberichterstattung, Umsatzplanung, Kapazitätsplanung und Prognosemodellierung (einschließlich Produktstrategie),
- Empfang und Nutzung von Feedback für die allgemeine Verbesserung der Dienstleistungen von Zoom.

Unabhängig davon, ob Telekom bzw. Zoom als Auftragsverarbeiter oder Verantwortlicher handelt, verarbeitet Telekom bzw. Zoom personenbezogene Daten nur dann, wenn diese angemessen und relevant sind.

3.2 Persönliche Daten, die zur Erbringung der Dienstleistungen verarbeitet werden

Es erfolgt eine Verarbeitung von persönlichen Daten folgender Kategorien:

- Kundeninhaltsdaten (Customer Content Data),
- Diagnosedaten (Diagnostic Data),
- Kontodaten Endnutzer (Account Data (end users)),
- Kontoinhaberdaten (Account Holder Business Data),
- Supportdaten (Support Data),
- Website-Daten (Website Data),
- Feedback-Daten (Feedback Data).

3.2.1 Kundeninhaltsdaten

Kundeninhaltsdaten sind Informationen, die vom Kunden durch die Nutzung der Dienste bereitgestellt werden, einschließlich aller Daten, die der Kunde während eines Meetings oder Webinars aufzeichnen oder freigeben möchte, einschließlich Cloud-Aufzeichnungen, Meeting-Protokolle, Chat-Protokolle (In-Meeting & persistent) und Dateien, die während eines Meetings oder im persistenten Chat-Kanal ausgetauscht werden.

Kommunikationsinhalte für Sitzungen und Webinare
Dies beinhaltet:

- Video, Audio, Whiteboard, Untertitel und Präsentationen;
- Fragen und Antworten während der Sitzung, Umfragen und Informationen zu Umfragen;
- Untertitel (Live-Transkription);

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

Vom Kunden initiierte Cloud-Aufnahmen.
Dazu gehören die folgenden Aufzeichnungen (wenn der Administrator des Kundenkontos eine solche Aufzeichnung zulässt und die Funktion von einem Meeting-Gastgeber oder -Teilnehmer genutzt wird):

- Videoaufzeichnung von Video, Audio, Whiteboard, Untertiteln und Präsentationen;
- Audioaufnahme;
- Textdatei-Dokument aller Gruppenchats während der Sitzung;
- Textdatei der Audiotranskription;
- Fragen und Antworten während der Sitzung, Umfragen und Informationen zu Umfragen;
- Abschriften für geschlossene Untertitel.

Informationen für Meeting- und Webinar-Teilnehmer
Diese enthalten:

- Name und Kontaktdaten des registrierten Teilnehmers sowie alle Daten, die der Kunde optional in Verbindung mit der Registrierung erhebt, wie z. B. eine E-Mail-Adresse;
- Status des Teilnehmers (als Gastgeber, als Teilnehmer an einem Chat oder als Teilnehmer);
- Raumnamen (falls verwendet);
- Benutzerkategorien (falls verwendet);
- Verfolgungsfelder wie Abteilung oder Gruppe (falls verwendet);
- geplante Zeit für ein Treffen;
- Themenbezogene Namen.

Gespeicherte Chat-Informationen
Dies sind Daten im Ruhezustand (im Speicher) und umfassen:

- Chat-Nachrichten,
- über den Chat ausgetauschte Dateien,
- über Chat ausgetauschte Bilder,
- über den Chat ausgetauschte Videos,
- Titel des Chat-Kanals.

Adressbuch-Informationen
Dazu gehören optionale Kontaktinformationen, die durch kundengesteuerte Integrationen (z. B. Outlook) zur Verfügung gestellt werden.

Kalenderinformationen
Dazu gehören optionale Kalenderinformationen, die vom Kunden (z. B. Outlook, Google) zur Verfügung gestellt werden.

3.2.2 Diagnosedaten

Zu den Diagnosedaten gehören alle automatisch generierten oder gesammelten Daten über die Nutzung des Meeting- und Webinar-Produkts von Zoom X. Zu den Diagnosedaten gehören nicht der Name eines Zoom-Benutzers, seine E-Mail-Adresse oder Kundeninhaltsdaten. Diagnosedaten umfassen drei Kategorien von Daten: Meeting-Metadaten, Telemetriedaten und andere vom Dienst generierte Daten. Die Diagnosedaten gehören zu “Data at Rest” und werden damit von AWS in Frankfurt gespeichert. Diese Daten werden nicht außerhalb Deutschlands verarbeitet. Eine Auswertung zu eigenen Zwecken erfolgt zu keiner Zeit durch Zoom oder Telekom. Alle Diagnosedaten werden im AWS Rechenzentrum nach aktuellen Standards (AES-256 GCM) verschlüsselt gespeichert.

Meeting-Metadaten

Meeting-Metadaten sind Metriken über die Nutzung von Zoom X, einschließlich der Frage, wann und wie Besprechungen stattgefunden haben.

Diese Kategorie umfasst:

- Ereignisprotokolle (einschließlich durchgeführter Aktion, Ereignistyp und -untertyp, Ort des In-App-Ereignisses, Zeitstempel, Client-UUID),
- userID und Besprechungs-ID,
- Informationen über Besprechungssitzungen, einschließlich Häufigkeit, durchschnittliche und tatsächliche Dauer, Quantität, Qualität, Netzwerkaktivität und Netzwerkkonnektivität,
- Anzahl der Sitzungen,
- Anzahl der Sitzungen mit und ohne Bildschirmfreigabe,
- Anzahl der Teilnehmer,
- Informationen zum Gastgeber der Veranstaltung,
- Hostname,
- URL (Uniform Resource Locator) des Veranstaltungsorts,
- Beginn/Ende der Sitzung,
- Beitrittsmethode,
- Informationen zu Leistung, Fehlersuche und Diagnose.

Telemetrie-Daten

Telemetriedaten sind Informationen, die von der Zoom-Client-Software, die auf dem Gerät eines Endbenutzers läuft, an Zoom gesendet werden. Es handelt sich um Informationen darüber, wie Zoom X genutzt wird oder funktioniert (z. B. Produktnutzung und Systemkonfiguration). Telemetriedaten enthalten keine Kundeninhalte oder Informationen über andere Benutzer, Meeting-Namen oder andere vom Benutzer eingegebene Werte wie Profilnamen.
Zoom verarbeitet Telemetriedaten, die einer ähnlichen Struktur folgen: einige Felder beschreiben den Client und das Betriebssystem, den Typ und den Untertyp des Ereignisses, die Stelle in der App, an der das Ereignis aufgetreten ist, einen Zeitstempel und einige pseudonyme Identifikatoren, einschließlich einer UUID, userID und meeting_id.

Gemeinsame Telemetrie-Datenfelder für alle Ereignisse

Diese Daten werden für alle Events auf dem Zoom Client verarbeitet:

- Zeit der Veranstaltung,
- Typ des Kunden,
- Ort der Veranstaltung,
- Veranstaltung,
- Unterereignis,
- UUID,
- Client-Version,
- Benutzer-ID,
- Client-Betriebssystem,
- Besprechungs-ID.

Telemetrie-Ereignistypen und Unterereignistypen

Bitte besuchen Sie die Support-Seite für Telemetrie-Ereignisse von Zoom für eine detailliertere Dokumentation über Ereignistypen und Unterereignistypen. Bitte beachten Sie, dass die Liste der Telemetrie-Ereignisse dynamisch ist und aktualisiert wird. Zoom unterhält Datenschutz- und Sicherheitsprozesse, um den Inhalt und den Zweck von vorgeschlagenen neuen Ereignissen zu genehmigen, bevor solche Ereignisse hinzugefügt werden können.

Andere vom Dienst generierte Daten
Hiebei handelt es sich um Daten, die Zoom verwendet, um einen vom Endnutzer oder Kunden angeforderten Dienst bereitzustellen, wie z. B. die Bereitstellung von Spam-Warnungen oder Push-Benachrichtigungen. Andere vom Dienst generierte Daten umfassen auch einen "Unique Identifier“ der von Zoom’s Trust and Safety Team genutzt wird, um Missbrauch zu verhindern und Teilnehmer zu identifizieren bzw. zu blocken, die gegen Richtlinien und ggfs. Gesetze verstoßen. Zugang zu diesen Daten haben nur ausgewählte Mitarbeiter*innen, die speziell ausgebildet und geschult sind.

3.2.3 Kontodaten Endbenutzer

Dies sind Informationen, die mit Endnutzern eines Zoom Enterprise- oder Education-Kontos verbunden sind. Je nachdem, wie der Kontoadministrator das Zoom Enterprise- oder Education-Konto konfiguriert hat, umfassen diese Informationen:

- Zoom eindeutige Benutzer-ID,
- Anmeldung bei sozialen Medien (optional),
- Profilbild (optional),
- Anzeigename,
- Daten zur Kundenauthentifizierung, es sei denn, es wird Single Sign On (SSO") verwendet.

3.2.4 Geschäftsdaten des Kontoinhabers

Dies sind Informationen, die mit der/den Person(en) verbunden sind, die der Vertriebskontakt für ein Zoom Enterprise- oder Education-Konto für die Bereitstellung und Registrierung eines Kontos sind, einschließlich:

- Firmenname,
- Firmenadresse,
- Daten im Zusammenhang mit dem Kundenkonto, wie z. B. Abonnementplan und ausgewählte Kontrollen.

3.2.5 Supportdaten

Supportdaten in Zoom X sind Informationen, die Zoom von der Deutschen Telekom im Zusammenhang mit Support-Aktivitäten zur Verfügung gestellt werden, die nicht durch den Tier 1 und 2 Support der Deutschen Telekom gelöst werden können. Die Anfrage kann Anhänge, wie z.B. Screenshots, enthalten. Solche Screenshots können Kundeninhaltsdaten oder Diagnosedaten enthalten.

Endnutzer in der EU und Cookies
Zoom setzt auf seinen öffentlichen Websites standardmäßig nur unbedingt notwendige Cookies für Endnutzer aus der EU. Bitte lesen Sie unsere Cookie-Erklärung für weitere Informationen über Ihre Wahlmöglichkeiten.

3.2.6 Feedback-Daten

Feedback-Daten sind Informationen über die Zufriedenheit der Endbenutzer mit den Zoom-Diensten. Es gibt zwei Arten von Feedback-Daten: (1) Post-Meeting-Bewertungen und (2) In-Meeting-Umfragen.
Post-Meeting-Bewertungen sind ein Modul, das unmittelbar nach einem Zoom-Meeting oder -Webinar erscheint und den Endbenutzer auffordert, seine Zoom-Erfahrung zu bewerten, indem er ein Daumen-hoch- oder Daumen-runter-Symbol auswählt. Je nachdem, wie der Kunde sein Zoom-Konto konfiguriert, kann er die Post-Meeting-Bewertung aktivieren, um nur die Daumen-hoch/Daumen-runter-Informationen zu sammeln, oder der Kunde kann zusätzliche Informationen anfordern, indem er ein Freitextfeld anzeigt. Die Post-Meeting-Bewertung ist standardmäßig nicht aktiviert.
Eine In-Meeting-Umfrage ist ein Tool, das von Zoom eingesetzt wird, um einen Zoom Net Provider Score ("NPS") zu ermitteln. Dieses Umfragetool ist für Endnutzer in der EU standardmäßig deaktiviert. Alle anderen Endnutzer können es deaktivieren, indem sie in der Cookie-Verwaltung von Zoom, die Sie durch Auswahl von "Cookies" in der Fußzeile der Zoom-Webseiten finden, nur "Strictly Necessary Cookies" auswählen.

3.3 Internationaler Datentransfer

Zoom ist bestrebt, personenbezogene Daten gemäß den geltenden Datenschutzgesetzen zu übertragen. Wenn beispielsweise personenbezogene Daten außerhalb des Europäischen Wirtschaftsraums ("EWR") übertragen werden, in die Schweiz oder in das Vereinigte Königreich, erfolgt dies auf der Grundlage der entsprechenden EU-Standardvertragsklauseln ("SCC") und gegebenenfalls mit zusätzlichen Sicherheitsvorkehrungen, so dass die personenbezogenen Daten gemäß dem erforderlichen Standard geschützt sind.

3.4 Regierungsanfragen zu persönlichen Daten

Telekommunikationsunternehmen sind gesetzlich verpflichtet, Sicherheitsbehörden bei Überwachungsmaßnahmen oder durch die Herausgabe von Daten zur Strafverfolgung zu unterstützen. Dabei ist uns wichtig, dass wir unsere Tätigkeiten im Rahmen dieser gesetzlichen Verpflichtungen so transparent wie möglich gestalten. Als erstes Unternehmen hat die Deutsche Telekom bereits im Jahr 2014 einen Transparenzbericht für Deutschland veröffentlicht. Weitere Infos sind auf der Webseite Datenschutz der Telekom zu finden.

Ebenso verpflichtet sich unser Partner Zoom die Privatsphäre seiner Kunden und Endnutzer zu schützen, und gibt Nutzerdaten nur auf begründete und rechtmäßige Anfragen an Regierungen weiter, wobei Zoom den Leitfaden für Regierungsanfragen und die entsprechenden rechtlichen Richtlinien beachtet. Weitere Informationen darüber, wie Zoom auf staatliche Anfragen reagiert, finden Sie in in Transparenzberichten, im Trust Center.

3.5 Auftragsverarbeitung (AVV)

Weitere Zulieferer, die mit der Verarbeitung personenbezogener Daten beauftragt werden, sind im „Vertragsanhang Auftragsverarbeitung (AVV)“ dokumentiert. Ebenso sind dort die Technischen und organisatorischen Maßnahmen (TOMs) dokumentiert.

Die Verträge zu AGB-Produkten haben wir hier als „Ergänzende Bedingungen Auftragsverarbeitung (AV)“ (ErgBAV) veröffentlicht. Das bedeutet: die veröffentlichten Regelungen gelten automatisch als ergänzende Bedingungen.

4 Technische Parameter

4.1 Systemanforderungen

Unter https://support.zoom.us/hc/de/articles/201362023 sind die Zoom Systemanforderungen für Windows, macOS, Linux zu finden.
Unter https://support.zoom.us/hc/de/articles/201179966 sind die Systemanforderungen für iOS, iPadOS und Android zu finden.

4.2 Firewall-Kompatibilität

Während des Sitzungsaufbaus verbindet sich der Zoom-Client über HTTPS (Port 443/TLS) mit den Zoom X Servern, um Informationen zu erhalten, die für die Verbindung mit dem jeweiligen Meeting oder Webinar erforderlich sind, und um die aktuelle Netzwerkumgebung zu bewerten, wie z. B. den zu verwendenden Multimedia-Router, welche Ports offen sind und ob ein SSL-Proxy verwendet wird. Anhand dieser Metadaten bestimmt der Zoom-Client die beste Methode für die Echtzeitkommunikation und versucht, sich automatisch über die bevorzugten UDP- und TCP-Ports 8801, 8802 und 8804 zu verbinden. Zur Verbesserung der Kompatibilität und Unterstützung von SSL-Proxys in Unternehmen kann die Verbindung auch über HTTPS (Port443/TLS) hergestellt werden. Eine HTTPS-Verbindung wird auch für Benutzer hergestellt, die sich über den Zoom X - Webbrowser-Client mit einem Meeting verbinden.

4.3 Client-Anwendung - rollenbasierte Benutzersicherheit

Die folgenden Sicherheitsfunktionen stehen dem Meetingveranstalter vor dem Meeting zur Verfügung:

- Sichere Anmeldung mit Standard-Benutzername und Passwort oder SAML Single Sign-On,
- Start eines gesicherten Meetings mit Passcode,
- Planen eines gesicherten Meetings mit Passcode.

Selektive Meeting-Einladung
Der Gastgeber kann Teilnehmer selektiv per E-Mail, IM oder SMS einladen. Dies ermöglicht eine bessere Kontrolle über die Verteilung der Meeting-Zugangsinformationen. Der Gastgeber kann das Meeting auch so einrichten, dass nur Mitglieder aus einer bestimmten E-Mail-Domäne teilnehmen können.

Sicherheit der Meeting-Details
Die Event-Details einer Sitzung werden zu Berichtszwecken speichert. Die Event-Details werden in der gesicherten Datenbank in Deutschland gespeichert und stehen dem Administrator des Kundenkontos zur Überprüfung auf der Kundenportalseite zur Verfügung, sobald er sich sicher angemeldet hat.

Anwendungssicherheit
Zoom verschlüsselt alle Echtzeit-Medieninhalte auf der Anwendungsebene mit dem Advanced Encryption Standard (AES).

Zoom-Client-Gruppenrichtlinienkontrolle
Speziell für den Zoom Meetings-Client für Windows und Zoom Rooms für Windows können Administratoren eine breite Palette von Client-Konfigurationseinstellungen definieren, die über Active Directory-Gruppenrichtlinienkontrollen durchgesetzt werden.

Erweiterte Verschlüsselung
Die erweiterte Chat-Verschlüsselung ermöglicht eine sichere Kommunikation, bei der nur der vorgesehene Empfänger die gesicherte Nachricht lesen kann.

Ende-zu-Ende-Verschlüsselung
Wenn die Ende-zu-Ende-Verschlüsselung aktiviert ist, wird die Kommunikation zwischen allen Teilnehmern eines Meetings mit kryptografischen Schlüsseln verschlüsselt, die nur den Geräten dieser Teilnehmer bekannt sind. Dadurch wird sichergestellt, dass keine dritte Partei - auch nicht Zoom oder Telekom - Zugang zu den privaten Schlüsseln des Meetings hat. Die Ende-zu-Ende-Verschlüsselung ist als technische Vorschau für alle Kunden verfügbar.

4.4 Meeting Sicherheit - Rollenbasierte Benutzersicherheit

Die folgenden Sicherheitsfunktionen stehen dem Meeting-Gastgeber während des Meetings zur Verfügung:
- Warteraum,
- Wartezeit für Gastgeber aktivieren,
- Einen Teilnehmer oder alle Teilnehmer ausschließen,
- Besprechung beenden,
- Sperren eines Meetings,
- Chat mit einem Teilnehmer oder allen Teilnehmern,
- Stummschaltung eines Teilnehmers oder aller Teilnehmer aktivieren/deaktivieren,
- Wasserzeichen für die Bildschirmfreigabe,
- Audio-Signaturen,
- Aufzeichnung eines Teilnehmers oder aller Teilnehmer aktivieren/deaktivieren,
- Vorübergehende Unterbrechung der Bildschirmfreigabe, wenn ein neues Fenster geöffnet wird.

Die folgenden Sicherheitsfunktionen stehen den Besprechungsteilnehmern während der Besprechung zur Verfügung:
- Audio stummschalten/stummschalten,
- Video ein-/ausschalten,
- Schnappschuss im iOS-Task-Switcher verwischen.

Host- und Client-authentifiziertes Meeting
Ein Gastgeber muss sich (über HTTPS) mit seinen Benutzerdaten (ID und Passwort) bei der Zoom X Website authentifizieren, um ein Meeting zu starten. Der Client-Authentifizierungsprozess verwendet ein eindeutiges Token pro Client und pro Sitzung, um die Identität jedes Teilnehmers zu bestätigen, der versucht, einem Meeting beizutreten. Jede Sitzung hat ein eindeutiges Set von Sitzungsparametern, die von Zoom generiert werden. Jeder authentifizierte Teilnehmer muss Zugang zu diesen Sitzungsparametern in Verbindung mit dem eindeutigen Sitzungs-Token haben, um dem Meeting erfolgreich beitreten zu können.

Offenes oder passwortgeschütztes Meeting
Der Gastgeber kann von den Teilnehmern verlangen, dass sie einen Passcode eingeben, bevor sie dem Meeting beitreten. Dies bietet eine bessere Zugangskontrolle und verhindert, dass ungebetene Gäste einem Meeting beitreten.

Meeting bearbeiten oder löschen
Der Gastgeber kann ein bevorstehendes oder vorheriges Meeting bearbeiten oder löschen. Dies ermöglicht eine bessere Kontrolle über die Verfügbarkeit von Meetings.

Vom Gastgeber kontrollierte Teilnahme an Meetings
Für eine bessere Kontrolle der Meetings kann der Gastgeber verlangen, dass die Teilnehmer dem Meeting erst dann beitreten, wenn der Gastgeber es gestartet hat. Für mehr Flexibilität kann der Gastgeber den Teilnehmern erlauben, dem Meeting vor dem Gastgeber beizutreten.

Sicherheit während des Meetings
Während des Meetings liefert Zoom Rich-Media-Inhalte in Echtzeit und auf sichere Weise an jeden Teilnehmer eines Zoom-Meetings. Alle Inhalte, die mit den Teilnehmern eines Meetings geteilt werden, sind nur eine Darstellung der Originaldaten. Dieser Inhalt wird kodiert und für die Freigabe mit einer sicheren Implementierung wie folgt optimiert:

- ist das einzig mögliche Mittel, um einem Zoom-Meeting beizutreten,
- ist vollständig abhängig von Verbindungen, die auf Sitzungsbasis hergestellt werden,
- führt ein proprietäres Verfahren durch, das alle gemeinsam genutzten Daten verschlüsselt,
- verschlüsselt alle Echtzeitmedien (Audio, Video, Bildschirmfreigabe) mit dem AES-Verschlüsselungsstandard,
- verschlüsselt andere Daten mit dem Verschlüsselungsstandard TLS,
- stellt eine visuelle Identifikation jedes Teilnehmers in der Besprechung bereit.

Authentifizierung
Zu den Authentifizierungsmethoden gehören Passwort oder Single Sign-On (SSO) mit SAML oder OAuth. Benutzer, die sich mit Benutzername und Kennwort authentifizieren, können auch die Zwei-Faktor-Authentifizierung (2FA) als zusätzliche Sicherheitsebene für die Anmeldung aktivieren. Mit SSO meldet sich ein Benutzer einmal an und erhält Zugriff auf mehrere Anwendungen, ohne sich bei jeder einzelnen erneut anmelden zu müssen. Zoom unterstützt SAML 2.0, das eine webbasierte Authentifizierung und Autorisierung einschließlich SSO ermöglicht. SAML 2.0 ist ein XML-basiertes Protokoll, das Sicherheits-Token verwendet, die Behauptungen enthalten, um Informationen über einen Benutzer zwischen einer SAML-Autorität (einem Identitätsanbieter) und einem Webdienst (wie Zoom) zu übermitteln. Zoom arbeitet mit verschiedenen Identitätsmanagement-Lösungen von Drittanbietern zusammen. Zoom kann Attribute zuordnen, um einen Benutzer verschiedenen Gruppen mit Funktionskontrollen zuzuordnen. OAuth-basiertes Provisioning funktioniert mit Google oder Facebook OAuth für sofortiges Provisioning. Zoom bietet auch einen API-Aufruf für die Vorabbereitstellung von Benutzern aus einem beliebigen Datenbank-Backend. Sobald Ihr Antrag für die zugehörige Domäne genehmigt ist, können alle bestehenden und neuen Benutzer mit Ihrer E-Mail-Adressdomäne zu Ihrem Konto hinzugefügt werden.

4.5 Administrative Kontrollmechanismen

Dem verantwortlichen Kontoverwalter stehen die folgenden Sicherheitsfunktionen zur Verfügung:

- sichere Anmeldeoptionen mit Standard-Benutzername und -Passwort (mit der Option, die Zwei-Faktor-Authentifizierung (2FA) als zusätzliche Sicherheitsebene zu aktivieren) oder SAML SSO,
- Hinzufügen von Benutzern und Administratoren zum Konto,
- Hoch- oder Herunterstufen der Abonnement-Stufe des Kontos,
- Benutzer aus dem Konto löschen,
- Berichte einsehen,
- Konto-Dashboard und Cloud-Aufzeichnungen verwalten.

Sie haben noch Fragen?

Weitere Informationen erhalten Sie online unter
www.telekom.de/datenschutzhinweise oder
per E-Mail an datenschutz@telekom.de.

Erleben,
was verbindet.