Datenschutz-Checkliste für Zoom

basierend auf der *DSK-Checkliste für Videokonferenzsysteme*
vom 11. November 2020

V 1.1
(15.02.2021)

Hinweis zur Nutzung dieses Dokuments

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) hat am 23. Oktober 2020 eine Orientierungshilfe zum Datenschutz bei Videokonferenzsystemen veröffentlicht. Darauf aufbauend erschien am 11. November 2020 eine Checkliste.

Zoom begrüßt die Orientierungshilfe und die Checkliste, da sie Transparenz und einen verlässlichen Rahmen für die Bewertung von Videokonferenzsystemen bieten. Um es Zoom-Kunden so einfach wie möglich zu machen, diese Maßstäbe anzulegen, veröffentlichen wir den vorliegenden Kommentar. In der linken Spalte finden Sie die Kriterien der Checkliste, die wir unverändert übernommen haben. Auf der rechten Seite finden Sie Hinweise von Zoom zu den Einstellungsmöglichkeiten und weiterführenden Informationen bzw. den rechtlich verbindlichen Dokumenten von Zoom zum Thema Datenschutz.

Um das Lesen zu vereinfachen, haben wir die Tabellenfelder farblich markiert:

[ ]: Zoom kann dem Controller dabei helfen, dieses Kriterium zu erfüllen

[ ]: Dieses Kriterium richtet sich direkt an den Controller

[ ]: Dieses Kriterium betrifft keine der von Zoom erbrachten Dienste

Wir werden dieses Dokument kontinuierlich weiterentwickeln. Wir hoffen, dass Ihnen dieser Zoom-Leitfaden hilft und freuen uns über Ihr Feedback.

Erreichen können Sie uns am besten über privacy@zoom.us

V 1.0: Release November 2020
V 1.1: Einarbeitung von Anregungen des Hamburgische Beauftragten für Datenschutz und Informationsfreiheit (Februar 2021)

DSK-Checkliste	Zoom-Kommentar
3. Rechtliche Anforderungen Rollen und Verantwortlichkeiten der Beteiligten sind klar verteilt und eindeutig festgelegt (Art. 4 Nr. 7 DS-GVO i.V.m. Art. 28 Abs. 3 und/oder Art. 26 DS-GVO).	Zoom sieht sich im Verhältnis zu seinen Kunden als Auftragsdatenverarbeiter.
3.1 Selbst betriebener Dienst […] **3.2 Betrieb durch einen externen Dienstleister** […]	Die Themen in den Kapiteln 3.1 und 3.2 beziehen sich nicht auf die von Zoom angebotenen Dienste.
3.3 Online-Dienst Im Falle einer Verarbeitung zu eigenen Zwecken durch den Anbieter verfügt der Veranstalter für jede Offenlegung personenbezogener Daten an den Anbieter über eine Rechtsgrundlage.	
Der Anbieter verfügt für jede Verarbeitung personenbezogener Daten in eigener Verantwortlichkeit über eine Rechtsgrundlage.	Soweit Zoom personenbezogene Daten für seine eigenen Zwecke verarbeitet, findet dies ausschließlich statt, wenn eine rechtliche Grundlage existiert. Weitere Informationen hierzu finden Sie im Zoom Privacy Statement im Kapitel "Personal Data We Process & How We Use It".
Die Notwendigkeit einer Vereinbarung zur gemeinsamen Verantwortlichkeit von Anbieter und Verantwortlichem nach Art. 26 Abs. 1 DS-GVO wurde geprüft.	Aus Zoom's Sicht besteht keine gemeinsame Verantwortlichkeit zwischen Zoom und Verantwortlichem nach Art. 26 Abs 1 DS-GVO.
Der Verantwortliche hat die vom Auftragsverarbeiter vorgelegten Auftragsverarbeitungsverträge, Nutzungsbedingungen und Sicherheitsnachweise sowie dessen Datenschutzerklärung geprüft.	Zoom stellt auf Anfrage dem Verantwortlichen alle notwendigen Dokumente zu Verfügung. Ein Muster des Global Data Processing Addendums kann hier eingesehen werden, welches in Exhibit B die technischen und organisatorischen Maßnahmen seitens Zoom darlegt. Die Nutzungsbedingungen finden Sie hier und wie Zoom Daten verarbeitet erläutern wir hier.
Der Verantwortliche hat bei der Auswahlentscheidung für einen Anbieter darauf geachtet, dass dieser geeignete technische und organisatorische Maßnahmen ergreift, dass die Verarbeitung im Einklang mit den Anforderungen der DS-GVO erfolgt und der Anbieter hierfür hinreichende Garantien bietet.	Zoom ist dem Schutz der Daten seiner Kunden und der Nutzer seiner Dienste verpflichtet. Zoom's aktuellen technischen und organisatorischen Maßnahmen finden Sie unter anderem im "Zoom Global Data Privacy Addendum" (Exhibit B).
Die Konfigurationsoptionen des eingesetzten Dienstes wurden hinsichtlich datenschutzrechtlicher Aspekte geprüft und bei Bedarf angepasst.	

	Zoom stellt den Nutzern und den Teilnehmern von Videokonferenzen mehrere Einstellungsmöglichkeiten zur Verfügung. Eine leicht verständliche Einführung findet sich im Zoom Help Center.
Gegenüber den betroffenen Personen wird transparent gemacht, wer in welcher Rolle personenbezogene Daten verarbeitet.	Soweit Zoom personenbezogene Daten verarbeitet, stehen alle Details der Datenverarbeitung im Zoom Privacy Statement zu Verfügung.
Die Kontaktdaten des Verantwortlichen und – falls im jeweiligen Nutzungsszenario anwendbar – des Anbieters sind klar für den Nutzer auffindbar.	Die Kontaktdaten des Verantwortlichen sollten im Rahmen der Datenschutzrichtlinien des verantwortlichen Unternehmens bereitgestellt werden. Zoom's Kontaktdaten sind im Zoom Privacy Statement gelistet.
3.4 Rechtsgrundlage und Zweckbindung Für die Veranstaltung einer Videokonferenz liegt eine Rechtsgrundlage des Veranstalters und, soweit er Daten nicht alleine im Rahmen der Auftragsverarbeitung empfängt, des Anbieters gemäß Art. 6 DS-GVO vor.	
3.4.1 Zur Struktur der Rechtsgrundlage Eine einschlägige Befugnisnorm nach Art. 6 Abs. 1 lit a, b, e, f DS-GVO, gegebenenfalls auch in Verbindung mit dem nationalen Recht, ist vorhanden.	
3.4.2 Einwilligung Sollte die Verarbeitung personenbezogener Daten in einer Videokonferenz auf Basis von Einwilligungen legitimiert werden, so sind diese in informierter Weise und freiwillig abgegeben worden (Art. 4 Nr. 11 DS-GVO und Art. 6 Abs. 1 lit. a i.V.m. Art. 7 DS-GVO).	
Ausreichende Datenschutzinformationen wurden erteilt, damit die Einwilligung informiert abgegeben werden kann.	Zoom kann dem Verantwortlichen helfen, die notwendigen Informationen zur Verfügung zu stellen. Die im Rahmen der Nutzung der Dienste von Zoom einschlägigen Datenschutzinformationen können in Zooms Datenschutzerklärung eingesehen werden.
Es besteht eine echte Wahlmöglichkeit hinsichtlich der Teilnahme an der Videokonferenz.	
3.4.3 Arbeitgeber als Verantwortliche Die Erforderlichkeit der Übertragung auch von Bilddaten wurde überprüft, insbesondere, wenn die Rechtsgrundlage für die Datenverarbeitung auf § 26 Abs. 1 Satz 1 BDSG oder entsprechenden landesrechtlichen Vorschriften im öffentlichen Bereich beruht.	
3.4.4 Verarbeitung besonderer Kategorien personenbezogener Daten	

Sofern bei der Videokonferenz besondere Kategorien personenbezogener Daten thematisiert werden, ist diese Datenverarbeitung auch nach Art. 9 Abs. 2 DS-GVO, ggf. in Verbindung mit einem nationalen Gesetz, zulässig.	
Soweit bei der Videokonferenz besondere Kategorien personenbezogener Daten verarbeitet werden, kann nach Art. 9 Abs. 2 lit. a DS-GVO eine ausdrückliche gesonderte Einwilligung erforderlich sein. Diese Einwilligung wurde ausdrücklich, informiert, freiwillig, vorherig, aktiv, für den konkreten Einzelfall und separat erklärt und ist jederzeit zumutbar widerruflich.	
3.4.5 Teilnahme aus Privatwohnungen Soweit Beschäftigte aus ihrem Home-Office teilnehmen, hat der Arbeitgeber durch technische und organisatorische Maßnahmen sichergestellt, dass Einblicke in deren Privatsphäre durch Bild und Ton nicht möglich sind.	Zoom kann Arbeitgebern helfen, ihren Angestellten eine sicheres Home-Office-Umgebung zu Verfügung zu stellen. Dies beinhaltet zum Beispiel die Möglichkeit, Video- und Audioaufnahmen auszustellen oder die Verwendung von Hintergrundbildern. Eine Anleitung hierzu findet sich hier.
Unter Sicherstellung der Freiwilligkeit ist eine gesonderte Einwilligung in diese Einblicke denkbar. Die Freiwilligkeit wird in diesem Falle zugesichert und die betroffenen Beschäftigten wurden vom Verantwortlichen über die diesbezüglichen Risiken informiert.	
3.4.6 Verarbeitung durch Anbieter zu eigenen Zwecken Sofern ein Anbieter personenbezogene Daten zu eigenen Zwecken verarbeitet hat dieser selbst – als Verantwortlicher im datenschutzrechtlichen Sinne (Art. 4 Nr. 7 DS-GVO) – eine Rechtsgrundlage.	Zoom verarbeitet personenbezogene Daten nur dann zu eigenen Zwecken, wenn eine Rechtsgrundlage existiert. Weitere Informationen zu den Daten, die Zoom verarbeitet, finden Sie hier.
Gegenüber einem Auftragsverarbeiter wird im Auftragsverarbeitungsvertrag sichergestellt, dass dieser die personenbezogenen Daten der teilnehmenden Personen nur auf Weisung des Verantwortlichen und nicht für eigene Zwecke verarbeitet (Art. 28 Abs. 3 DS-GVO).	Zoom verarbeitet personenbezogene Daten nur auf Anweisung des Verantwortlichen. Siehe auch Abschnitt 3 des "Zoom Global Data Privacy Agreement".
3.4.7 Verarbeitung von Daten Dritter Für die Verarbeitung personenbezogener Daten Dritter, die nicht an der Videokonferenz teilnehmen, werden die allgemeinen Rechtsgrundlagen herangezogen	
3.4.8 Transparenz, Aufzeichnungen von Videokonferenzen Art und Zweck der Verarbeitung personenbezogener Daten sind klar definiert.	Die Datenverarbeitung durch Zoom ist im Zoom Privacy Statement beschrieben. Zusätzlich sollten Nutzer von Videokonferenzdiensten die Datenschutzregeln des Veranstalters eines Zoom Phone Calls oder Videokonferenz lesen.
Die Verarbeitung ist auf den Zweck der Videokonferenz beschränkt.	Zoom verarbeitet personenbezogene Daten ausschließlich, um Videokonferenzdienste und unmittelbar damit verbundene Dienste (wie zum

	Beispiel die Abrechnung) zu erbringen. Welche Daten zu welchen zwecken verarbeitet werden, können Sie detailliert in Zooms Datenschutzerklärung nachlesen.
Die Rechtsgrundlage für Aufzeichnungen wurde erfolgreich geprüft.	
Wirksame Einwilligungen in die Aufzeichnung und die weitere Verarbeitung liegen vor.	
Aufzeichnungsmöglichkeiten werden bei der Erfüllung der Informationspflichten erwähnt.	
Bestehende Aufzeichnungsfunktionen wurden in der Voreinstellung deaktiviert.	Zoom-Videokonferenzsysteme haben bei Installation als “default” keine automatische Aufzeichnungsfunktionen aktiviert. Weitere Informationen zu den Einstellungs- und Konfigurationsmöglichkeiten finden sich im Zoom Help Center.
Die Nutzer werden darüber belehrt, dass das (gerade auch heimliche) Mitschneiden von Video- und/oder Audiodaten, das Speichern und das Verbreiten solcher Aufnahmen strafbar sein kann.	Heimliche Video- oder Audioaufnahmen sind in den meisten Ländern verboten. Der Verantwortliche sollte die Teilnehmer dementsprechend informieren. Vgl. hierzu auch die Einstellungsmöglichkeiten, die in Abschnitt 4.2 beschrieben werden.
Audio- und Videodaten werden nur solange und soweit verarbeitet, wie es für die Übermittlung der Nachrichten durch einen Dienstleister oder im Rahmen einer notwendigen Dokumentation erforderlich ist.	Zoom zeichnet keine Videokonferenzen seiner Kunden für eigene Zwecke auf.
3.5 Pflichten des Verantwortlichen **3.5.1 Informationspflichten und Betroffenenrechte** Den an der Konferenz teilnehmenden Personen werden klare und eindeutige Informationen über die mit der Nutzung des Dienstes verbundene Datenverarbeitung zur Verfügung gestellt (Art. 13 und 14 DS-GVO).	Die Datenverarbeitung durch Zoom ist en detail im Zoom Privacy Statement beschrieben. Zusätzlich sollten Nutzer von Videokonferenzdiensten die Datenschutzhinweise des Veranstalters eines Telefonats oder Videokonferenz lesen.
Die Informationen werden so dargestellt, dass sie für einen durchschnittlichen Nutzer des Dienstes ohne übermäßigen Aufwand verständlich sind (Art. 12 und Art. 5 Abs. 1 lit. a DS-GVO).	Zoom bemüht sich, alle Datenschutzregelungen so einfach wie möglich darzustellen.
Werden die Daten auf Grund eines berechtigten Interesses (Art. 6 Abs. 1 lit. f DS-GVO) verarbeitet, so werden diese Interessen konkret benannt und die wesentlichen Gesichtspunkte der Abwägung mit den Interessen und Grundrechten der Betroffenen dargestellt.	
Die teilnehmenden Personen werden über die Zwecke und die Rechtsgrundlagen der einzelnen Verarbeitungsvorgänge informiert (Art. 13, 14 DS-GVO).	Die Datenverarbeitung durch Zoom ist en detail im Zoom Privacy Statement beschrieben. Der Verantwortliche kann diese Informationen in seine eigenen Datenschutzhinweise integrieren.

Die teilnehmenden Personen werden ggf. auf ihr Widerspruchsrecht hingewiesen (Art. 21 Abs. 4 DS-GVO).	
Der Veranstalter der Videokonferenz informiert die teilnehmenden Personen über Verarbeitungstätigkeiten des Anbieters des Dienstes, die dieser – soweit das überhaupt zulässig ist – zu eigenen Zwecken vornimmt.	Dies liegt in der Hand des Verantwortlichen. Die Datenverarbeitung durch Zoom ist en detail im Zoom Privacy Statement beschrieben. Der Verantwortliche kann diese Informationen in seine eigenen Datenschutzregelungen integrieren.
Der Veranstalter informiert die teilnehmenden Personen darüber, welche Möglichkeiten für sie bestehen, im Rahmen der Privatsphäre-Einstellungen des Dienstes selbst auf den Schutz ihrer personenbezogenen Daten hinzuwirken (z. B. Nutzung eines Synonyms, Einstellen eines künstlichen Hintergrunds).	Dies liegt in der Hand des Verantwortlichen. Zoom stellt hier wichtige Informationen zu den Einstellungsmöglichkeiten im Zoom Help Center zu Verfügung, unter anderem FAQs.
Die Betroffenenrechte aus Art. 15 bis 21 DS-GVO sind gewährleistet.	Dies liegt in der Hand des Verantwortlichen. Zoom stellt wichtige Informationen im Zoom Global DPA zu Verfügung, um ihn dabei zu unterstützen, einschließlich der Informationen zu den Betroffenenrechten gegenüber Zoom.
Die Löschung der Inhalts- und Rahmendaten der beendeten Konferenz erfolgt auch unabhängig von einem Antrag der betroffenen Personen nach Art. 17 DS-GVO regelmäßig unverzüglich nach dem Abschluss der Videokonferenz.	Zoom speichert keinerlei “data in transit” von Videokonferenzen. Dateien und Bilder, die während eines Meetings hochgeladen oder geteilt wurden, werden nach 31 Tage nach Beendigung des Meetings gelöscht.
3.5.2 Auftragsverarbeitungsvertrag Wenn das Videokonferenzsystem durch den Anbieter betrieben wird oder dieser die Möglichkeit hat, auf personenbezogene Daten zuzugreifen, wurde mit ihm ein gültiger Auftragsverarbeitungsvertrag abgeschlossen (Art. 28 DS-GVO).	Siehe "Zoom Global DPA".
3.5.3 Verarbeitungsverzeichnis Die Veranstaltung der Videokonferenz(en) wurde in das Verzeichnis der Verarbeitungstätigkeiten gemäß Art. 30 DS-GVO aufgenommen.	
3.5.4 Meldepflichten bei Datenpannen Im Fall einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit der Videokonferenz werden die Pflichten aus Art. 33 und 34 DS-GVO eingehalten.	Dies ist hauptsächlich eine Pflicht des Verantwortlichen. Als Auftragsdatenverarbeiter hat Zoom hierauf keinen Einfluss. Zoom kann dem Verantwortlichen in seinen Pflichten gemäß Art. 33 und 34 DS-GVO unterstützen - Details finden sich im Zoom Global DPA.
3.5.5 Datenschutz-Folgeabschätzung Der Verantwortliche hat überprüft, ob eine Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO durchzuführen ist und diese bei Bedarf durchgeführt.	Zusätzlich zu den Anforderungen von Art. 35 DS-GVO haben die deutschen Datenschutzaufsichtsbehörden ein Kurzpapier zur Datenschutz-Folgenabschätzung veröffentlicht (“Kurzpapier Nr. 5”) sowie spezifische Verfahren gelistet, für die aus Sicht der Aufsichtsbehörden eine DSFA zwingend notwendig sind (öffentliche Einrichtungen sowie private Einrichtungen).

3.5.6 Besonderheiten bei Übermittlungen an Drittländer Werden Videokonferenzsysteme von Anbietern ausgewählt, die zu Datenübermittlungen in Drittländer führen, so hält die Übermittlung besondere Bedingungen (vgl. Kapitel V, Art. 44 ff. DS-GVO, siehe dazu auch Kurzpapier Nr. 4 der Datenschutzkonferenz sowie Veröffentlichungen des EDSA) ein.	Zoom übermittelt personenbezogene Daten im Einklang mit denen in Kapitel 5 der DS-GVO beschriebenen Regelungen. Für die folgenden Länder bezieht sich Zoom auf Standardvertragsklauseln nach Art. 46 Abs. 2 der DS-GVO: USA, Philippinen, Malaysia und Australien. Datenübermittlungen nach Kanada werden nach Art. 45 Abs 1 DS-GVO getätigt.
4 Technische und organisatorische Anforderungen **4.1 Sicherheit der Übertragung** Für die Übertragung der Videokonferenzdaten werden mindestens Transportverschlüsselungen nach dem Stand der Technik, entsprechend den einschlägigen Technischen Richtlinien des BSI, genutzt.	Zoom bietet zwei verschiedene Verschlüsselungsmethoden für “data in transit” an: **Verschlüsselung GCM AES-256:** Als Standardeinstellung verschlüsselt Zoom Meeting- und Webinar-Inhalte auf der Applikationsebene mit TLS 1.2 und Advanced Encryption Standard (AES) 256-bit-Algorithmus für den Desktop-Client. Audiosignale von Dial-In-Teilnehmer, die mit dem Telefon teilnehmen, werden beim Transfer ab Zoom’s Datenzentren verschlüsselt. Für Teilnehmer, die sich per Telefon einwählen, wird die Audiospur verschlüsselt, bis sie die Datenzentren von Zoom verlässt und an das Telefonnetz des Teilnehmers übertragen wird.Die Verschlüsselung kann für H.323- und SIP-Geräte, die an Zoom-Meetings teilnehmen, erforderlich sein. Diese Einstellung wird auf Kontoebene, Gruppen- oder Benutzerebene konfiguriert. **Ende-zu-Ende-Verschlüsselung (E2EE):** Zoom bietet E2EE für Nutzer mit verifizierten Zoom-Accounts und Telefonnummern an. Die Schlüssel und die Meeting-Inhalte werden ausschließlich auf den Endgeräten gespeichert - Zoom hat keinen Zugang hierzu. Die E2EE-Funktion hat keinen Einfluss auf den Ort und die Art der Datenspeicherung von Zoom-Dienstleistungen. E2EE wird zurzeit vom Zoom Desktop Client, mobile app, Zoom Rooms und der Virtual Desktop Infrastructure unterstützt. Die Browser-Version unterstützt E2EE derzeit noch nicht.Eine detaillierte Dokumentation von Zoom E2EE-Ansatz findet sich in diesem White Paper. Eine kurze Übersicht in deutsch findet sich hier.
Sollte ein hohes Risiko bestehen, werden geeignete technische und organisatorische Maßnahmen zur Sicherstellung der Vertraulichkeit der Inhaltsdaten ergriffen (bspw. über Ende-zu-Ende-Verschlüsselung oder über TLS-Verbindungen mit zusätzlichen technischen und organisatorischen Maßnahmen).	Die Frage, ob ein hohes Risiko besteht, kann nur vom Verantwortlichen beantwortet werden. Zu den Verschlüsselungsstandards vgl. unsere Antwort oben.
Die einzelnen Funktionalitäten des eingesetzten Videokonferenzsystems wurden separat betrachtet, insbesondere hinsichtlich der Risiken ihres Einsatzes für Rechte und Freiheiten der betroffenen Personen.	Zoom stellt Kunden und Teilnehmern verschiedene Optionen zur Verfügung. Die Bewertung, welche Einstellungen sinnvoll und notwendig sind, obliegt dem Verantwortlichen. Weitere Informationen zu den Optionen finden sich im Zoom Help Center.

Es wurden Funktionalitäten des Dienstes unterbunden, für die ein unbefugter Abfluss personenbezogener Daten zu befürchten ist.	Das Zoom's Privacy Statement führt alle Fälle von Datenverarbeitungen auf, die für die Bereitstellung von Zoom-Meetings und Webinaren notwendig sind.
Über die Protokollierung der Inanspruchnahme von Funktionalitäten wird für die teilnehmenden Personen Transparenz gewahrt.	Zoom verwendet Logging- und Monitoring-Software, um Daten der produktiven Server zu analysieren hinsichtlich der Performanz, Sicherheit und Lastverteilung.
Es wird sichergestellt, dass der Hersteller und andere Dritte keinen Zugriff auf die verarbeiteten Daten, wie bspw. Nutzungsdaten, erhalten.	Zoom stellt durch technische und organisatorische Maßnahmen sicher, dass kein unautorisierter Dritter Zugang zu Nutzungsdaten erhält. Zoom's Unterauftragnehmer sind abschließend hier gelistet.
4.2 Nutzerauthentifizierung Es wird sichergestellt, dass nur berechtigte Personen auf eine Videokonferenzsitzung und deren Daten zugreifen können.	Die folgenden Funktionen helfen sicherzustellen, dass nur autorisierte Personen Zugang zu einer Videokonferenz und den dort geteilten Daten haben: • **Erlaube nur den Zugang authentifizierter Teilnehmer:** Der Account-Administrator oder der Meeting-Host können die Teilnahme auf authentifizierte Nutzer (also solche, die in einen Zoom-Account eingeloggt sind) beschränken. Dadurch können Personen, die zwar den Meeting-Link, aber nicht eingeloggt sind, nicht am Meeting teilnehmen. • **Erlaube Zugang nur mit Passcode:** Der Account-Administrator oder der Meeting-Host können den Zugang nur nach Eingabe eines Passcodes gewähren. • **Erlaube Zugang nur von bestimmter Domain:** Der Account-Administrator oder der Meeting-Host können den Zugang auf Teilnehmer aus einer bestimmten Web-Domain erlauben - zum Beispiel Nutzer mit einer email-Adresse einer bestimmten Organisation. • **Warteraum:** Der Meeting-Host kann über den Warteraum den Zugang zu einer Videokonferenz oder Webinar steuern - Teilnehmer können dann vom Host entweder einzeln oder alle auf einmal zum Meeting zugelassen werden. Hier können entweder alle Teilnehmer zunächst in den Warteraum geführt werden oder aber eine Ausnahme von der Warteraum-Regel für die Teilnehmer aus einer bestimmten Domain eingerichtet werden. • **Meeting schließen:** Es ist darüber hinaus möglich, ein Meeting zu "schließen", so dass keine weiteren Teilnehmer dazu kommen können. • **Verhindere Teilnahme aus bestimmten Ländern / Regionen:** Account-Administratoren können die Teilnahme aus bestimmten Ländern oder Regionen über eine "approved vs. blocked list" managen. Weitere Informationen finden sich im Zoom Help Center.
4.2.1 Normale Risiken	Account-Administratoren können eine Zwei-Faktor-Authentifizierung von Teilnehmern verlangen. Account-Administratoren können einen Reset für existierende Zwei-Faktor-Authentifizierungen durchführen, falls ein Nutzer den Zugang hierzu verloren hat.

Die Nutzer werden mittels Nutzername und Passwort authentisiert oder mittels eines stärkeren Verfahrens, beispielsweise Zwei-Faktor-Authentisierung.	Beim Erstellen einer Videokonferenz-Einladung kann der Account-Administrator die Verwendung eines Meeting-Passworts vorschreiben. Das Meeting-Passwort muss folgende Eigenschaften aufweisen: ● Mindestens 10 Zeichen ● Klein-/Großbuchstaben-sensitiv ● Empfohlen wird die Verwendung von Zahlen und Sonderzeichen @ * _ - Weitere Informationen hierzu finden sich im Zoom Help Center.
Die Authentisierung mittels Nutzername und geeignetem Passwort ist so ausgestaltet, dass Passwörter weder übertragen noch bei dem Dienstleister gespeichert werden.	Zoom erlaubt Single Sign-On (SSO) und ermöglicht damit den Zugang von Nutzern mit ihren Unternehmens-Kontodaten. Zoom SSO basiert auf SAML 2.0. Zoom arbeitet mit Okto sowie anderen Enterprise Identify Management-Platformen wie Centrify, Microsoft Active Directory, Gluu, OneLogin, PingOne, Shibboleth und anderen. Zoom fungiert hier als Service Provider (SP) und stellt eine automatische Nutzer-Provision zu Verfügung. Nutzer müssen sich damit nicht bei Zoom registrieren. Sobald Zoom eine SAML-Antwort vom Identity-Provider (IdP) erhält, prüft Zoom, ob bereits ein Nutzer-Account existiert. Ist dies nicht der Fall, erstellt Zoom automatisch einen Nutzeraccount für die erhaltene Identität. Mehr Informationen zum Thema SSO finden sich hier.
Dem Stand der Technik entsprechende Authentifizierungsverfahren verhindern, dass aus dem Passwort abgeleitete Daten, die im Zuge eines Authentifizierungsvorgangs übertragen wurden, für einen zweiten Authentifizierungsvorgang verwendet werden können.	Siehe oben.
4.2.2 Hohe Risiken Bei hohem Risiko wird eine Zwei-Faktor-Authentisierung nach dem Stand der Technik eingesetzt. Dafür kommen je nach Höhe des Risikos insbesondere Softwaretoken bzw. Hardwaretoken in Frage.	Siehe oben.
4.2.3 Authentifizierungsdienst Die Nutzerauthentifizierung wird nach erfolgter Risikoabwägung auf ein Verfahren gestützt, das bereits für andere Verfahren genutzt wird. Der Identity Provider gewährleistet die Integrität des Authentifizierungsvorgangs und die Nichtverkettung verschiedener Nutzungsvorgänge.	Siehe oben.
Bei Anwendungsfällen, die eine vorherige Identifikation der Nutzer erfordern, werden geeignete Verfahren implementiert, um die Authentizität der Nutzer im Nachhinein nachvollziehen zu können.	Siehe oben.

4.2.4 Gastteilnahme Der Gastzugang ist für den Anwendungsfall erforderlich.	Ein Gastzugang ist erhältlich - Nutzer müssen sich nicht bei Zoom registrieren, sondern nur einen Namen eingeben, bevor sie an ein Meeting oder Webinar teilnehmen können. SSO-Nutzer müssen sich ebenfalls nicht bei Zoom registrieren.
Die Risiken für betroffene Personen, die durch eine nicht autorisierte Teilnahme entstehen, sind geringfügig.	Dies hängt von den Einstellungen ab, die der Meeting-Host vorgibt. Wie oben dargelegt, können Meetings so konfiguriert werden, dass nur autorisierte Nutzer teilnehmen können. Vgl. hierzu unsere Antwort unter 4.2.1 und 2.
Es ist gewährleistet, dass nur Personen teilnehmen, die untereinander bekannt sind.	Der Meeting-Host kann zahlreiche Einstellungen vornehmen, um dies zu gewährleisten: ● **Erlaube nur den Zugang authentifizierter Teilnehmer:** Der Account-Administrator oder der Meeting-Host können die Teilnahme auf authentifizierte Nutzer (also solche, die in einen Zoom-Account eingeloggt sind) beschränken. Dadurch können Personen, die zwar den Meeting-Link, aber nicht eingeloggt sind, nicht am Meeting teilnehmen. ● **Erlaube Zugang nur mit Passcode:** Der Account-Administrator oder der Meeting-Host können den Zugang nur nach Eingabe eines Passcodes gewähren. ● **Erzwinge zufallsgenerierten Passcode:** Der Account-Administrator kann die Verwendung eines Zufallscodes erzwingen, so dass derselbe Passcode nicht für mehrere Meetings verwendet werden kann. ● **Erlaube Zugang nur von bestimmter Domain:** Der Account-Administrator oder der Meeting-Host können den Zugang auf Teilnehmer aus einer bestimmten Web-Domain erlauben - zum Beispiel Nutzer mit einer email-Adresse einer bestimmten Organisation. ● **Warteraum:** Der Meeting-Host kann über den Warteraum den Zugang zu einer Videokonferenz oder Webinar steuern - Teilnehmer können dann vom Host entweder einzeln oder alle auf einmal zum Meeting zugelassen werden. Hier können entweder alle Teilnehmer zunächst in den Warteraum geführt werden oder aber eine Ausnahme von der Warteraum-Regel für die Teilnehmer aus einer bestimmten Domain eingerichtet werden. ● **Meeting schließen:** Es ist darüber hinaus möglich, ein Meeting zu “schließen”, so dass keine weiteren Teilnehmer dazu kommen können. ● **Verhindere Teilnahme aus bestimmten Ländern / Regionen:** Account-Administratoren können die Teilnahme aus bestimmten Ländern oder Regionen über eine “approved vs. blocked list” managen. ● **TOR-Blocking:** Zoom verhindert die Teilnahme über “The Onion Router (TOR) und andere IP-Anonymisierungs-Services. Weitere Informationen finden sich im Zoom Help Center.

Nicht autorisierte Personen werden erkannt und können aktiv ausgeschlossen werden, noch bevor sie aktiv an der Videokonferenz teilnehmen können.	Es ist nicht möglich, unerkannt an einem Videokonferenz-Meeting teilzunehmen. Darüber hinaus ist es möglich, bestimmte Teilnehmer aus laufenden Meetings zu entfernen. Diese Teilnehmer können sich anschließend nicht wieder in das gleiche Meeting einwählen wenn die Option “Allow removed participants to rejoin” vom Meeting-Host nicht aktiviert ist. Darüber hinaus stellt Zoom einen **“At Risk Meeting Notifier”** zu Verfügung der Notifier scannt öffentliche Webseiten und social media-Inhalte bezüglich eingestellter Links zu Zoom-Meetings (also Links to Meetings, die eine Zoom-URL enthalten). Wird eine solche URL gefunden, informiert Zoom den Account-Owner. Zoom hat bis heute über 100.000 Emails and Account-Owner versendet, um sie vor möglichen Problemen mit ihren Meetings zu warnen.
Die Empfänger eines Einladungslinks werden auf die Folgen einer nicht autorisierten Weitergabe des Links hingewiesen.	Der Meeting-Host hat im Admin-Portal die Möglichkeit, individualisierte Einladungs-E-Mails zu verfassen. Hier können Warnungen wie die hier beschriebene eingefügt werden. Darüber hinaus können solche Warnungen auch auf dem Bildschirm vor Betreten eines Meetings angezeigt werden.
Die Übergabe des Links wahrt die Vertraulichkeit auf angemessenem Niveau.	
4.3 Installierung and Software-Update Technische Schwachstellen und sonstige Sicherheitslücken in Videokonferenzsystemen werden in einem angemessenen Zeitraum behoben.	**Schwachstellen-Management** Alle entdeckten Sicherheitsschwachstellen werden bis zum Patching kontinuierlich von Zoom-Sicherheitsexperten beobachtet. Zoom lässt darüber hinaus regelmäßig Pen-Tests von unabhängigen Dritten durchführen. Während des 90-Tage-Planes zu Datenschutz und IT-Sicherheit (April-Juni 2020) wurden weitere Pen-Tests durchgeführt. Identifizierte Probleme werden mit Hilfe eines Ticketing-Systems bis zum Patching gemanaged. **Server-Monitoring und Evaluation** Zoom beobachtet fortlaufend die Entwicklung und die Vorhersagen der Server-Verfügbarkeit. Zoom’s Enterprise Monitoring Application versendet Warnhinweise sobald vorab definierte Grenzwerte überschritten werden. In diesen Fällen werden das Network Operations Center (NOC) und das Security Operations Center (SOC) eingeschaltet. Zoom hat darüber hinaus Kontrollpunkte für das Management von Denial of Service (DoS)- und Distributed Denial of Service (DDoS)-Attacken eingerichtet. **Sicherheits-Monitoring**

	Zoom's Logging- und Monitoring-Software analysiert Daten der produktiven Server hinsichtlich ihrer Leistungsfähigkeit, möglichen Sicherheitsschwachstellen und Ressourcenoptimierung. Im Falle von Auffälligkeiten wird das für die Infrastruktur zuständige Personal benachrichtigt. **Störungsmanagement** Im Falle eines Sicherheitsvorfalles stellt Zoom seinen Kunden detaillierte Eskalationsprozesse zu Verfügung, die von der Validierung, Klassifizierung, Priorisierung bis zur Berichterstattung über den Verlust vertraulicher Daten reichen.
Alle Komponenten, die für die Teilnahme an einer Videokonferenz auf einem Client installiert werden, können einfach und vollständig deinstalliert werden. Auch bei einer nur einmaligen Nutzung eines nativen Clients ist sichergestellt, dass keine ungewartete Software auf dem System verbleibt.	Eine vollständiges Löschen aller Komponenten ist möglich. Das Removal Tool und eine Beschreibung der Löschoptionen findet sich hier (ganz unten auf der Webseite).
Sofern webbasierte Videokonferenzsysteme genutzt werden, wird für einen sicheren Betrieb stets eine aktuelle Webbrowser-Version eingesetzt. Dasselbe gilt für ggf. erforderliche Browser-Erweiterungen.	
4.4 Rollentrennung Das Videokonferenzsystem ermöglicht die Einrichtung administrierender, moderierender, präsentierender und teilnehmenden Personen bzw. andere Zuschnitte, soweit die Verantwortung für die Steuerung der implizit vorgenommenen Verarbeitung von personenbezogenen Daten klar zugewiesen bleibt.	Es stehen verschiedene Rollen zu Verfügung: Host, Co-Host, alternativer Host und Teilnehmer. Die Rollenverteilung wird durch den Host des Meetings bestimmt. Einen Überblick zu den Rollen und den damit verbundenen Rechten findet sich hier.
Die teilnehmenden Personen können ihr Mikrofon und ihre Kamera jederzeit deaktivieren. Ohne die Zustimmung der teilnehmenden Person kann deren Mikrofon und deren Kamera nicht aktiviert werden.	Teilnehmer können Mikrofon und Kamera jederzeit ausschalten und die Grundeinstellung sieht auch vor, dass Mikrofon und Kamera per default ausgeschaltet sind. Der Meeting-Host hat keine Möglichkeit, ein ausgeschaltetes Mikrofon oder Kamera ohne Einwilligung des Teilnehmers zu (re)aktivieren. Der Host kann entweder die Option "Ask All to Unmute" verwenden (in diesem Fall müssen alle Teilnehmer ihre Geräte selber aktivieren), oder aber er kann ein Meeting mit der Option "Request permission to unmute participants" aufsetzen. In diesem Fall müssen die Teilnehmer vor der Reaktivierung zustimmen. Mehr Details hierzu finden sich hier.
Bei Anwendungen mit hohem Risiko ist eine Nutzerverwaltung vorgesehen, die die Autorisierung der teilnehmenden Personen zur Übernahme einer der o.g. Rollen sicherstellt.	

4.5 Datensparsamkeit Es werden für die Bereitstellung des Dienstes nur die zwingend erforderlichen technischen und sonstigen Informationen verarbeitet.	Zoom verarbeitet personenbezogene Daten ausschließlich, um Videokonferenzdienste und unmittelbar damit verbundene Dienste (wie zum Beispiel die Abrechnung) zu erbringen.
Die Protokolldaten werden nur für den Zweck der Konferenz verarbeitet.	Zoom verarbeitet personenbezogene Daten ausschließlich um Videokonferenzdienste und unmittelbar damit verbundene Dienste (wie zum Beispiel die Abrechnung) zu erbringen.
Das Videokonferenzsystem erfüllt die Grundsätze Datenschutz durch Technikgestaltung sowie datenschutzfreundlicher Voreinstellungen.	Zoom-Meetings können vom Meeting-Host nach den Maßgaben der Datensparsamkeit konfiguriert werden. Alle Zoom-Dienste werden in Kooperation mit dem Zoom-Datenschutz-Team entwickelt. Dieser Prozess beinhaltet eine detaillierte Analyse der Sammlung und Verarbeitung personenbezogener Daten und der damit verbundenen Prozesse. In Fällen, in denen Drittanbieter Teil des Dienstes sind, werden sie einer detaillierten Prüfung unterzogen, um Konformität mit Zoom's Anforderungen zu garantieren.
Vor Eintritt in die Konferenz sind Funktionen von Kamera, Mikrofon und das Teilen des Bildschirms deaktiviert und müssen erst von der teilnehmenden Person aktiviert werden.	Teilnehmer sind beim Betreten eines Meetings grundsätzlich stumm geschaltet. Teilnehmer können die Stummschaltung nach Beitritt selber aufheben. Die Standard-Einstellung für die Videofunktion ist ebenfalls „off". Beim Erstellen des Meetings kann der Host bestimmen, ob alle Teilnehmer zunächst ohne Videofunktion beitreten sollen.
4.6 Transparenz Der Hersteller des Videokonferenzsystems stellt, zusätzlich zu den rechtlich gebotenen Hinweisen in den Datenschutzbestimmungen, Informationen zur technischen Implementierung, den eingesetzten Standards, genutzten Software-Bibliotheken und Lizenzen bereit.	Detaillierte Informationen zu Zooms Verschlüsselungsansatz können im Zoom Security White Paper, dem Zoom Encryption Whitepaper und dem E2EE White Paper entnommen werden.
Es ist teilnehmenden Personen leicht möglich und an prominenter Stelle erkennbar, ob und ggf. welche Datenverarbeitungsvorgänge über den eigentlichen Anwendungszweck der Videokonferenz hinaus erfolgen.	Sofern Zoom Daten verarbeitet, sind alle Informationen hierzu im Zoom Privacy Statement einsehbar.
Berichte zu Sicherheitsprüfungen werden frei zugänglich veröffentlicht.	Zoom stellt Berichte zu Sicherheitsprüfungen grundsätzlich offen zu Verfügung. Sollten jedoch vertrauliche Informationen enthalten sein, die die IT-Sicherheit des Systems beeinträchtigen können, werden solche Sicherheits-Audits Zoom-Kunden unter einem Non-Disclosure-Agreement (NDA) zu Verfügung gestellt.
4.7 Aufzeichnungen Aufzeichnungen werden technisch unterbunden, sofern diese nicht aus sonstigen Gründen zulässig sind.	Administratoren können die Aufzeichnungsfunktion für Meeting Hosts (lokal und/oder in der Cloud) sowohl auf der Account-, Group- oder individuellen Ebene verwalten. Meeting Hosts können Teilnehmern die Aufzeichnung einer Videokonferenz untersagen.

Die notwendige Konfigurationseinstellung kann nur von einem Administrator zurückgenommen werden.	Ja, dies ist aufgrund der Administratorenrollen-Konfiguration der Fall.
Die an der Videokonferenz teilnehmenden Personen werden darauf hingewiesen, dass eine Aufzeichnung unzulässig ist.	Dies ist der Fall. Sollte ein Teilnehmer den Aufnahmeknopf betätigen, erscheint eine Botschaft “Please ask the host for recording permissions”.
Im Falle einer zulässigen Aufzeichnung können ausschließlich besonders privilegierte Nutzer diese Funktion aktivieren.	Grundsätzlich können nur Host oder Co-Host eine Aufnahme starten.
Alle teilnehmenden Personen werden durch einen expliziten und durch einen durch die teilnehmende Person zu bestätigenden Hinweis oder durch Kennzeichnung innerhalb der Benutzerschnittstelle darauf hingewiesen, dass die Videokonferenz ganz oder in Teilen aufgezeichnet wird.	Teilnehmer werden immer informiert, wenn ein Meeting aufgezeichnet wird. Der Host hat außerdem die Möglichkeit, einen Recording Disclaimer als Pop-Up einzuschalten. Die Aktivierung des Recording Disclaimers wird im Zoom Support Center erklärt. Weitere Informationen finden sich hier.
Aufzeichnungen von Videokonferenzen werden wenn möglich verschlüsselt gespeichert. Bei hohem Risiko ist dies zwingend vorgesehen.	Der Verantwortliche kann verschiedene Datenspeicherungssoptionen für Aufnahmen (lokal und/oder in der Cloud) wählen. Falls der Verantwortliche die Datenspeicherungsoption Cloud auswählt, werden diese mittels AES-256 und einem Cloud-basierten Key Management System (KMS) verschlüsselt.
4.8 Intervenierbarkeit Die teilnehmenden Personen haben die technische Möglichkeit, zumindest zeitweise an Konferenzen lediglich passiv (empfangend), aber nicht aktiv (sendend) teilzunehmen. Dies beinhaltet auch das separate Abschalten von jeweils der Kamera und des Mikrofons durch die teilnehmende Person.	Teilnehmer können ihr Mikrofon und ihre Kamera jederzeit ausstellen. Zoom stellt darüber hinaus die Zoom Webinar-Lösung zu Verfügung, in der die Mikrofone und Kameras aller Teilnehmer standardmäßig ausgeschaltet sind.