Datenschutz-Checkliste für Zoom

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

Version 3.0
(März 2025)

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)
V 2.0: Umfassende Aktualisierung (August 2022)
V 3.0: Umfassende Aktualisierung (März 2025)

Vorgaben 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 agiert im Verhältnis zu seinen Kunden als Auftragsdatenverarbeiter.
3.1 Selbst betriebener Dienst [...] **3.2 Betrieb durch einen externen Dienstleister** [...]	
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.	Zoom verarbeitet personenbezogene Daten ausschließlich zu eigenen Zwecken soweit dies zur Erfüllung des Dienstleistungsvertrages erforderlich ist oder aus berechtigtem Interesse zur Verbesserung der Service und Angebote. Weitere Informationen finden Sie im "Zoom Privacy Data Sheet".
Der Anbieter verfügt für jede Verarbeitung personenbezogener Daten in eigener Verantwortlichkeit über eine Rechtsgrundlage.	Soweit Zoom personenbezogene Daten in eigener Verantwortlichkeit 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 Zooms 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).

Vorgaben DSK-Checkliste	Zoom-Kommentar
Die Konfigurationsoptionen des eingesetzten Dienstes wurden hinsichtlich datenschutzrechtlicher Aspekte geprüft und bei Bedarf angepasst.	Ja. Die Funktion "Daten und Datenschutz" bietet Kontobesitzern/Administratoren die notwendigen Werkzeuge zur effizienten Verwaltung von Nutzerdaten in Bezug auf Meetings, Webinare und Chats. Sie haben die Möglichkeit, den Export oder die Löschung von Nutzerdaten zu beantragen, einschließlich der Daten von Teilnehmern, die innerhalb eines bestimmten Zeitraums an Ihren Meetings teilgenommen haben. Sie können die Daten von bis zu 50 Benutzer gleichzeitig exportieren. Darüber hinaus haben Sie die Möglichkeit, den Status dieser Anfragen zu verfolgen und ausstehende Anfragen, die noch nicht bearbeitet wurden, zu stornieren. Mehr Informationen Jeder Zoom Benutzer kann über das Menü "Daten und Datenschutz" einsehen, welche Daten zu welchem Grund verarbeitet werden. Dieses Menü gibt Administratoren und Benutzern mehr Kontrolle über die Arten von Daten, die Zoom sammelt und verwendet. Mehr Informationen
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.	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.	Zoom's Kunde und Veranstalter einer Videokonferenz ist Verantwortlicher bzw. Controller.
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.	Zooms Kunde trifft hierzu notwendige Vorkehrungen.

Vorgaben DSK-Checkliste	Zoom-Kommentar
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).	**Option zur Anzeige von Disclaimer/Haftungsausschlüssen/Einwilligung (Beitritt, Anmeldung, Aufzeichnung)** Administratoren können einen benutzerdefinierten Haftungsausschluss einblenden, wenn Benutzer ein Meeting oder ein Webinar starten oder daran teilnehmen oder sich über das Webportal, den Desktop Client und die mobile App bei ihrem Konto anmelden. Benutzer müssen dem Haftungsausschluss zustimmen. Andernfalls können sie, wenn sie im Haftungsausschluss auf Abbrechen klicken, nicht an der Sitzung teilnehmen, sie nicht starten oder sich anmelden. Den Benutzern werden jedes Mal Haftungsausschlüsse angezeigt, wenn ein Kontoinhaber oder Administrator einen Haftungsausschluss aktualisiert, und dann wieder in der angegebenen Häufigkeit. Beim Beitritt zu einem Meeting, das bereits aufgezeichnet wird, oder wenn der Host mit der Aufzeichnung beginnt, werden die Teilnehmer um ihre Zustimmung zur Aufzeichnung gebeten. Je nach Konto können Administratoren diese Zustimmungsbenachrichtigung so einstellen, dass sie nur externe Teilnehmer betrifft oder für alle Meeting-Teilnehmer gilt, egal ob intern oder extern. Diese Benachrichtigung kann auch mit zusätzlichen Informationen und einem Link, z. B. zu einer Datenschutzrichtlinie, angepasst werden. Video Meetings können so vorkonfiguriert werden, dass Kamera und Mikrofon der Teilnehmer bei Beitritt deaktiviert sind. Teilnehmer können dann frei entscheiden ob Kamera oder Mikrofon aktiviert wird.
Ausreichende Datenschutzinformationen wurden erteilt, damit die Einwilligung informiert abgegeben werden kann.	
Es besteht eine echte Wahlmöglichkeit hinsichtlich der Teilnahme an der Videokonferenz.	**Option zur Anzeige von Disclaimer/Haftungsausschlüssen/Einwilligung (Beitritt, Anmeldung, Aufzeichnung)**

Vorgaben DSK-Checkliste	Zoom-Kommentar
	Administratoren können einen benutzerdefinierten Haftungsausschluss/Einwillgung einblenden, wenn Benutzer ein Meeting oder ein Webinar starten oder daran teilnehmen oder sich über das Webportal, den Desktop Client und die mobile App bei ihrem Konto anmelden. Benutzer müssen dem Haftungsausschluss/Einwilligung zustimmen. Andernfalls können sie, wenn sie im Haftungsausschluss auf Abbrechen klicken, nicht an der Sitzung teilnehmen, sie nicht starten oder sich anmelden.
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.	Zooms Kunde trifft hierzu notwendige Vorkehrungen.
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.	Zooms Kunde trifft hierzu notwendige Vorkehrungen.
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.	Zooms Kunde trifft hierzu notwendige Vorkehrungen.
3.4.5 Teilnahme aus Privatwohnungen Soweit Beschäftigte aus ihrem Home-Office teilnehmen, hat der Arbeitgeber durch technische und	Zoom bietet einige technische und organisatorische Maßnahmen, die den Zweck dient, die Privatsphäre von Teilnehmenden zu

Vorgaben DSK-Checkliste	Zoom-Kommentar
organisatorische Maßnahmen sichergestellt, dass Einblicke in deren Privatsphäre durch Bild und Ton nicht möglich sind.	schützen. Dazu gehören die Möglichkeit, Video- und Audioaufnahmen auszustellen oder die Verwendung von Hintergrundbildern, um die Umgebung im Hintergrund zu maskieren. Eine Anleitung, plus weitere Support Infos stehen hier zur Verfügung.
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.	Administratoren können einen benutzerdefinierten Haftungsausschluss einblenden, wenn Benutzer ein Meeting oder ein Webinar starten oder daran teilnehmen oder sich über das Webportal, den Desktop Client und die mobile App bei ihrem Konto anmelden. Benutzer müssen dem Haftungsausschluss zustimmen. Andernfalls können sie, wenn sie im Haftungsausschluss auf Abbrechen klicken, nicht an der Sitzung teilnehmen, sie nicht starten oder sich anmelden. Den Benutzern werden jedes Mal Haftungsausschlüsse angezeigt, wenn ein Kontoinhaber oder Administrator einen Haftungsausschluss aktualisiert, und dann wieder in der angegebenen Häufigkeit. Weitere Details sind im Zoom Support Center zu finden
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	Zooms Kunde trifft hierzu notwendige Vorkehrungen.

Vorgaben DSK-Checkliste	Zoom-Kommentar
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 für die beauftragte Videokonferenzdienstleistung und damit verbundene Dienste, wie etwa zur Abrechnung oder zur Übersicht der Nutzung für den Kunden sowie zusätzliche beauftragte Dienste aus Zoom's Produktpalette. Welche Daten zu welchen Zwecken verarbeitet werden, können Sie detailliert in Zooms Datenschutzerklärung oder in den Privacy Data Sheets zu den einzelnen Dienstleistungen nachlesen.
Die Rechtsgrundlage für Aufzeichnungen wurde erfolgreich geprüft.	Der Hinweis auf die Zustimmung zur Aufzeichnung fordert die Teilnehmer von Meetings oder Webinaren auf, ihre Zustimmung zur Aufzeichnung zu geben. Teilnehmer erhalten eine Benachrichtigung, wenn eine Aufzeichnung beginnt oder wenn sie einer Sitzung beitreten, die bereits aufgezeichnet wird. Der Teilnehmer kann entweder zustimmen, in der Sitzung zu bleiben, oder sie verlassen. Nach der Sitzung kann der Host einen Bericht mit einer Liste der Teilnehmer erstellen, die ihre Zustimmung gegeben haben.
Wirksame Einwilligungen in die Aufzeichnung und die weitere Verarbeitung liegen vor.	Der Hinweis auf die Zustimmung zur Aufzeichnung fordert die Teilnehmer von Meetings oder Webinaren auf, ihre Zustimmung zur Aufzeichnung zu geben. Teilnehmer erhalten eine Benachrichtigung, wenn eine Aufzeichnung beginnt oder wenn sie einer Sitzung beitreten, die bereits aufgezeichnet wird. Der Teilnehmer kann entweder zustimmen, in der Sitzung zu bleiben, oder sie verlassen. Nach der Sitzung kann der Host einen Bericht mit einer Liste der Teilnehmer erstellen, die ihre Zustimmung gegeben haben. Support-Artikel

Vorgaben DSK-Checkliste	Zoom-Kommentar
Aufzeichnungsmöglichkeiten werden bei der Erfüllung der Informationspflichten erwähnt.	Der Hinweis auf die Zustimmung zur Aufzeichnung fordert die Teilnehmer von Meetings oder Webinaren auf, ihre Zustimmung zur Aufzeichnung zu geben. Teilnehmer erhalten eine Benachrichtigung, wenn eine Aufzeichnung beginnt oder wenn sie einer Sitzung beitreten, die bereits aufgezeichnet wird. Der Teilnehmer kann entweder zustimmen, in der Sitzung zu bleiben, oder sie verlassen. Nach der Sitzung kann der Host einen Bericht mit einer Liste der Teilnehmer erstellen, die ihre Zustimmung gegeben haben. Support-Artikel
Bestehende Aufzeichnungsfunktionen wurden in der Voreinstellung deaktiviert.	Zoom-Videokonferenzsysteme haben bei Installation als “default” keine automatischen Aufzeichnungsfunktionen aktiviert. Weitere Informationen zu den Einstellungs- und Konfigurationsmöglichkeiten finden sich im Zoom Support 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.	Der Hinweis auf die Zustimmung zur Aufzeichnung fordert die Teilnehmer von Meetings oder Webinaren auf, ihre Zustimmung zur Aufzeichnung zu geben. Teilnehmer erhalten eine Benachrichtigung, wenn eine Aufzeichnung beginnt oder wenn sie einer Sitzung beitreten, die bereits aufgezeichnet wird. Der Teilnehmer kann entweder zustimmen, in der Sitzung zu bleiben, oder sie verlassen. Nach der Sitzung kann der Host einen Bericht mit einer Liste der Teilnehmer erstellen, die ihre Zustimmung gegeben haben. Weitere Informationen
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 und in den Privacy Data Sheets beschrieben. Zusätzlich sollten Nutzer von Videokonferenzdiensten die Datenschutzhinweise des Veranstalters eines Telefonats oder Videokonferenz lesen.

Vorgaben DSK-Checkliste	Zoom-Kommentar
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. Jeder Zoom Benutzer kann über das Menü "Daten und Datenschutz" einsehen, welche Daten zu welchem Grund verarbeitet werden. Dieses Menü gibt Administratoren und Benutzern mehr Kontrolle über die Arten von Daten, die Zoom sammelt und verwendet. Das Zoom Trust Center bietet auch eine Vielzahl an Informationen zu den Themen: ● Datenschutz ● Zertifizierungen & Compliance ● Sicherheit ● Trust & Safety ● Rechtliche Bestimmungen
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.	Zooms Kunde trifft hierzu notwendige Vorkehrungen.
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).	Optional kann ein Disclaimer beim Starten oder Teilnehmen eines Meetings gezeigt werden. Administratoren können frei editieren welcher Content hier zu sehen ist.
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	Dies liegt in der Hand des Verantwortlichen. Zoom stellt hier wichtige Informationen zu den

Vorgaben DSK-Checkliste	Zoom-Kommentar
selbst auf den Schutz ihrer personenbezogenen Daten hinzuwirken (z. B. Nutzung eines Synonyms, Einstellen eines künstlichen Hintergrunds).	Einstellungsmöglichkeiten im Zoom Help Center zu Verfügung, unter anderem FAQs.
Die Betroffenenrechte aus Art. 15 bis 21 DS-GVO sind gewährleistet.	Die Funktion "Daten und Datenschutz" bietet Kontobesitzern/Administratoren die notwendigen Werkzeuge zur effizienten Verwaltung von Nutzerdaten in Bezug auf Meetings, Webinare und Chats. Sie haben die Möglichkeit, den Export oder die Löschung von Nutzerdaten zu beantragen, einschließlich der Daten von Teilnehmern, die innerhalb eines bestimmten Zeitraums an Ihren Meetings teilgenommen haben. Sie können die Daten von bis zu 50 Benutzer gleichzeitig exportieren. Darüber hinaus haben Sie die Möglichkeit, den Status dieser Anfragen zu verfolgen und ausstehende Anfragen, die noch nicht bearbeitet wurden, zu stornieren. Mehr Informationen Jeder Zoom Benutzer kann über das Menü “Daten und Datenschutz” einsehen, welche Daten zu welchem Grund verarbeitet werden. Dieses Menü gibt Administratoren und Benutzern mehr Kontrolle über die Arten von Daten, die Zoom sammelt und verwendet. Mehr Informationen Das Zoom Trust Center bietet auch eine Vielzahl an Informationen zu den Themen: ● Datenschutz ● Zertifizierungen & Compliance ● Sicherheit ● Trust & Safety ● Rechtliche Bestimmungen
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 Echtzeit Customer Content Data nicht zu eigenen Zwecken und nicht über die Dauer der Videokonferenz hinaus. Dateien und Bilder, die während eines Meetings hochgeladen oder geteilt wurden, werden regelmäßig nach Beendigung des Meetings gelöscht, es sei denn, Dateien werden im Continuous Chat optional gespeichert.
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	Siehe "Zoom Global DPA".

Vorgaben DSK-Checkliste	Zoom-Kommentar
gültiger Auftragsverarbeitungsvertrag abgeschlossen (Art. 28 DS-GVO).	
3.5.3 Verarbeitungsverzeichnis Die Veranstaltung der Videokonferenz(en) wurde in das Verzeichnis der Verarbeitungstätigkeiten gemäß Art. 30 DS-GVO aufgenommen.	Zooms Kunde trifft hierzu notwendige Vorkehrungen.
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). Zoom unterstützt seine Kunden bei der Erstellung von DSFA.
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 den 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: Philippinen, Indien, Malaysia und Australien. Datenübermittlungen nach Kanada und in die USA 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 "Echtzeit Daten" 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.

Vorgaben DSK-Checkliste	Zoom-Kommentar
	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. **Post-Quantum Ende-zu-Ende Verschlüsselung (PQ E2EE):** Wenn Benutzer die Ende-zu-Ende-Verschlüsselung (E2EE) für ihre Zoom Meetings aktivieren, ist das System von Zoom so konzipiert, dass nur die Teilnehmer Zugriff auf die Verschlüsselungsschlüssel haben, die zur Verschlüsselung des Meetings verwendet werden. Dies gilt sowohl für die Post-Quantum E2EE als auch für die Standard-E2EE. Da die Server von Zoom den notwendigen Entschlüsselungsschlüssel nicht besitzen, sind die verschlüsselten Daten, die über die Server von Zoom geleitet werden, unlesbar. Um sich gegen „harvest now, decrypt later“-Angriffe zu schützen, verwendet die Post-Quantum E2E-Verschlüsselung von Zoom Kyber 768, einen Algorithmus, der vom National Institute of Standards and Technology (NIST) als *Module Lattice-based Key Encapsulation Mechanism* standardisiert wird. Mehr Informationen
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).	Bei Zoom werden den entsprechenden technischen und organisatorischen Maßnahmen ergriffen, um die Vertraulichkeit der Inhaltsdaten zu schützen. Dazu gehören Maßnahmen wie der Einsatz von TLS 1.2 AES256 GCM für Echtzeit-Medien Verbindungen, sowie AES256 Verschlüsselung von gespeicherten Inhaltsdaten.
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 Teilnehmenden verschiedene Optionen zur Sicherheit und Datenschutz zur Verfügung. Die Bewertung, welche Einstellungen sinnvoll und notwendig sind, obliegt dem

Vorgaben DSK-Checkliste	Zoom-Kommentar
	Kunden/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. Administratoren können einschränken, welche In-Meeting-Funktionen verfügbar sind, wenn sie einem internen Meeting beitreten oder es veranstalten. Mit der "Follow User In-Meeting"-Richtlinie können Administratoren jedoch auch Richtlinien aktivieren, die bestimmte In-Meeting-Funktionen einschränken, selbst wenn sie einem externen Meeting beitreten. Dazu gehören die Einschränkung der Übertragung von Dateien, die Freigabe des eigenen Bildschirms, die Verwendung/Anzeige des Chats im Meeting, das Hinzufügen von Anmerkungen während einer Bildschirmfreigabe, die Freigabe eines Whiteboards, die Aufzeichnung eines Meetings, die Anzeige/Eingabe von Untertiteln und vieles mehr. Sobald die Richtlinie aktiviert ist, folgt sie dem Benutzer, unabhängig davon, mit welchem Gerät er sich bei Zoom anmeldet, um an Meetings teilzunehmen oder diese zu leiten. Support-Artikel
Über die Protokollierung der Inanspruchnahme von Funktionalitäten wird für die teilnehmenden Personen Transparenz gewahrt.	Zoom hat eine Reihe von integrierten Datenschutzbenachrichtigungen eingeführt, damit Sie besser ermitteln können, wer Ihre Inhalte auf Zoom sehen, speichern und freigeben kann. Diese funktionsspezifischen Benachrichtigungen sollen Sie dabei unterstützen, fundierte Entscheidungen darüber zu treffen, wie Sie Zoom verwenden. Außerdem stellen sie robuste Datenschutzeinstellungen und Sicherheit für unsere Produkte bereit. Weitere Informationen
Es wird sichergestellt, dass der Hersteller und andere Dritte keinen Zugriff auf die verarbeiteten Daten, wie bspw. Nutzungsdaten, erhalten.	Zoom setzt technische und organisatorische Maßnahmen ein, um Zugänge von unautorisierten Dritten zu verhindern.

Vorgaben DSK-Checkliste	Zoom-Kommentar
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. **Zoom Authenifizierungsprofile:** Authentifizierungsprofile ermöglichen es Hosts, die Teilnahme an Meetings und Webinaren auf angemeldete Benutzer zu beschränken. Eine

Vorgaben DSK-Checkliste	Zoom-Kommentar
	weitere Einschränkung auf Zoom Benutzer, deren E-Mail-Adresse zu einer bestimmten Domäne gehört, ist ebenfalls möglich. Dies kann sich als nützlich erweisen, wenn Sie Ihre Teilnehmerliste auf verifizierte Benutzer oder Benutzer eines bestimmten Unternehmens beschränken möchten. Darüber hinaus können Sie verhindern, dass Benutzer in bestimmten Domänen an Meetings oder Webinaren teilnehmen. Weitere Informationen Die **Zwei-Faktor-Authentifizierung (2FA)** ist ein zwei Schritte umfassender Anmeldeprozess, bei dem zusätzlich zur Hauptanmeldung bei Zoom ein einmaliger Code von einer mobilen App oder einer Textnachricht abgefragt wird. So werden Konten zusätzlich geschützt, da Benutzer Zugriff auf ihr Smartphone benötigen, um sich beim Zoom Web Portal, Desktop Client, der mobilen App oder bei Zoom Room anmelden zu können. Weitere Informationen Zoom empfiehlt es, alle Online Videokonferenzsitzungen vor unautorisierten Teilnehmenden zu schützen und bietet einige Sicherheitsfunktionen dafür an. Dazu gehören Meeting Passcodes, die Warteraum-Funktion, und die Möglichkeit, eine Sitzung zu verriegeln. Weitere Informationen finden sich im Zoom Help Center.
4.2.1 Normale Risiken Die Nutzer werden mittels Nutzername und Passwort authentisiert oder mittels eines stärkeren Verfahrens, beispielsweise Zwei-Faktor-Authentisierung.	Zoom bietet beide Optionen an. Zoom Admins können 2FA für Benutzer aktivieren, sodass sie diese einrichten und nutzen müssen. Administratoren können auch bereits eingerichtete 2FAs zurücksetzen, wenn ein Benutzer den Zugriff auf seine 2FA-App verloren hat.
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 Okta sowie anderen Enterprise Identify Management-Platformen wie Centrify, Microsoft Active Directory, Gluu, OneLogin, PingOne, Shibboleth und anderen.

Vorgaben DSK-Checkliste	Zoom-Kommentar
	Zoom fungiert hier als Service Provider (SP) und stellt eine automatische Nutzer-Provision zu Verfügung. 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.	Zoom empfiehlt die Nutzung von SSO. 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 Okta sowie anderen Enterprise Identify Management-Platformen wie Centrify, Microsoft Active Directory, Gluu, OneLogin, PingOne, Shibboleth und anderen. Mehr Informationen zum Thema SSO finden sich hier.
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.	Zoom Admins können 2FA für Benutzer aktivieren, sodass sie diese einrichten und nutzen müssen. Administratoren können auch bereits eingerichtete 2FAs zurücksetzen, wenn ein Benutzer den Zugriff auf seine 2FA-App verloren hat. Weitere Informationen
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.	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 Okta sowie anderen Enterprise Identify Management-Platformen wie Centrify, Microsoft Active Directory, Gluu, OneLogin, PingOne, Shibboleth und anderen. Mehr Informationen zum Thema SSO finden sich hier.
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.

Vorgaben DSK-Checkliste	Zoom-Kommentar
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.

Vorgaben DSK-Checkliste	Zoom-Kommentar
	● **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. Darüber hinaus bietet Zoom auch die Möglichkeit “Zoom Node” im eigenen Rechenzentrum zu installieren. Auf “Zoom Node” können Produkt-spezifische Module installiert werden. Das Module “Zoom Meetings Hybrid” ermöglicht es Zoom Benutzern ein Meeting zu planen (“Private Meeting”) an dem nur Zoom Benutzer des eigenen Accounts und innerhalb des Firmennetzwerkes teilnehmen können. Des Weiteren kann das Modul auch so konfiguriert werden, dass auch externe Teilnehmer bei jedem Meeting über das Modul im Rechenzentrum verbunden werden.
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. Mithilfe der Funktion „Warteraum“ kann der Host steuern, wann ein Teilnehmer einem Meeting beitritt. Authentifizierungsprofile ermöglichen es Hosts, die Teilnahme an Meetings und Webinaren auf angemeldete Benutzer zu beschränken. Eine weitere Einschränkung auf Zoom Benutzer, deren E-Mail-Adresse zu einer bestimmten Domäne gehört, ist ebenfalls möglich.

Vorgaben DSK-Checkliste	Zoom-Kommentar
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.	**Zoom bietet für besonders sensitive Meetings von Authentifizierungsprofilen.** Authentifizierungsprofile ermöglichen es Hosts, die Teilnahme an Meetings und Webinaren auf angemeldete Benutzer zu beschränken. Eine weitere Einschränkung auf Zoom Benutzer, deren E-Mail-Adresse zu einer bestimmten Domäne gehört, ist ebenfalls möglich. Folgende Methoden stehen zur Verfügung.
4.3 Installierung and Software-Update Technische Schwachstellen und sonstige Sicherheitslücken in Videokonferenzsystemen werden in einem angemessenen Zeitraum behoben.	**Schwachstellen-Management** Es gibt Informationssicherheitsstandards für die Behebung von Produktschwachstellen. Erkannte Schwachstellen werden nachverfolgt und im Einklang mit diesen Standards behoben.
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.	Ein 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 Web-Browser-Version eingesetzt. Dasselbe gilt für ggf. erforderliche Browser-Erweiterungen.	Eine aktuelle Liste mit den unterstützen Web-Browsern ist hier zu finden.

Vorgaben DSK-Checkliste	Zoom-Kommentar
	Generell gilt: **Desktop** Innerhalb von 2 Versionen der aktuellen Version • Chrome: Innerhalb von 2 Versionen der aktuellen Version • Firefox: Innerhalb von 2 Versionen der aktuellen Version • Edge: Innerhalb von 2 Versionen der aktuellen Version • Safari: Innerhalb von 2 Versionen der aktuellen Version **Mobile** • Safari: Innerhalb von 2 Versionen der aktuellen Version • Chrome: Innerhalb von 2 Versionen der aktuellen Version • Firefox: Innerhalb von 2 Versionen der aktuellen Version
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 zur 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 ist hier zu finden.
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. Mehr Details hierzu finden sich hier und hier.
Bei Anwendungen mit hohem Risiko ist eine Nutzerverwaltung vorgesehen, die die Autorisierung der teilnehmenden Personen zur Übernahme einer der o.g. Rollen sicherstellt.	Über die Benutzerverwaltung können Kontoinhaber und Admins ihre Benutzer verwalten und z. B. Rollen und Add-on-Funktionen hinzufügen, löschen und zuweisen.
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 die beauftragten Dienstleistungen und unmittelbar damit verbundene Dienste (wie zum Beispiel die Abrechnung) zu erbringen.

Vorgaben DSK-Checkliste	Zoom-Kommentar
Die Protokolldaten werden nur für den Zweck der Konferenz verarbeitet.	Zoom verarbeitet personenbezogene Daten ausschließlich, um die beauftragten Dienstleistungen und unmittelbar damit verbundene Dienste (wie zum Beispiel die Abrechnung) zu erbringen. Weiter Details werden im Data Processing Addendum und dem Privacy Data Sheet aufgeführt.
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. Weitere Informationen zum Thema Sicherheit und Datenschutz finden sich im Zoom Trust Center.

Vorgaben DSK-Checkliste	Zoom-Kommentar
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 zur 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) zur Verfügung gestellt. Sicherheitsmeldungen (Security Bulletins) werden online veröffentlicht.
4.7 Aufzeichnungen Aufzeichnungen werden technisch unterbunden, sofern diese nicht aus sonstigen Gründen zulässig sind.	Wenn Sie Cloud-Aufzeichnungen deaktivieren und diese Einstellung für das gesamte Konto sperren, werden alle Verwaltungseinstellungen für Cloud-Aufzeichnungen deaktiviert. Direkt zur Verwaltung der Einstellungen
Die notwendige Konfigurationseinstellung kann nur von einem Administrator zurückgenommen werden.	Kontoinhaber und Administratoren können Funktionen und Einstellungen über Kontoeinstellungen verwalten.
Die an der Videokonferenz teilnehmenden Personen werden darauf hingewiesen, dass eine Aufzeichnung unzulässig ist.	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. Beim Beitritt zu einem Meeting, das bereits aufgezeichnet wird, oder wenn der Host mit der Aufzeichnung beginnt, werden die Teilnehmer um ihre Zustimmung zur Aufzeichnung gebeten. Diese Benachrichtigung kann auch mit zusätzlichen Informationen und einem Link, zB. zu einer Datenschutzrichtlinie, angepasst werden. Support-Artikel

Vorgaben DSK-Checkliste	Zoom-Kommentar
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.	Beim Beitritt zu einem Meeting, das bereits aufgezeichnet wird, oder wenn der Host mit der Aufzeichnung beginnt, werden die Teilnehmer um ihre Zustimmung zur Aufzeichnung gebeten. Diese Benachrichtigung kann auch mit zusätzlichen Informationen und einem Link, zum Beispiel zu einer Datenschutzrichtlinie, angepasst werden. Darüber hinaus werden Benutzer visuell (oben links im Zoom Meeting Fenster) und mittels Audio-Benachrichtigung informiert, dass ein Recording/Aufnahme läuft oder gestartet wurde.
Aufzeichnungen von Videokonferenzen werden wenn möglich verschlüsselt gespeichert. Bei hohem Risiko ist dies zwingend vorgesehen.	Wenn ein Meeting-Host die Cloud-Aufzeichnung und Audioaufzeichnungen aktiviert, werden beide verschlüsselt gespeichert. Der Kontoinhaber sowie alle von ihm genehmigten Benutzer und Apps können auf die in der Zoom Cloud gespeicherten verschlüsselten Inhalte zugreifen.
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 individuell ausstellen. Zoom stellt darüber hinaus die Zoom Webinar-Lösung zur Verfügung, in der die Mikrofone und Kameras aller Teilnehmer standardmäßig ausgeschaltet sind. Weiterhin sind zusätzliche Meeting-Sicherheitsoptionen verfügbar.