

Übersicht zur datenschutzkonformen Nutzung des Videokonferenz-Programms „Zoom“

Zoom ist ein Softwareprogramm für Videotelefonie. Im Verhältnis zu seinen Kunden tritt Zoom als Auftragsdatenverarbeiter auf. Eine gemeinsame Verantwortlichkeit nach Art. 26 DSGVO besteht nicht. Den Auftragsdatenverarbeitungsvertrag erhält jeder Nutzer mit Abschluss des Registrierungsvorgangs bei Zoom.

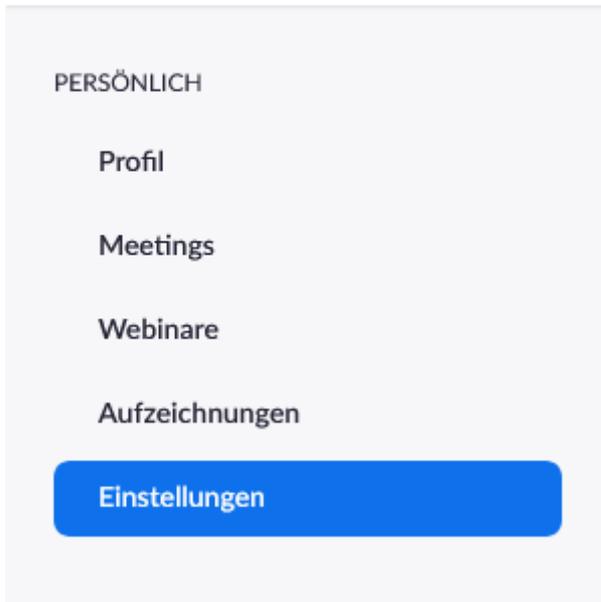
Erste Erwägungen zum datenschutzkonformen Umgang mit Zoom:

- Bitte wählen Sie zunächst die EU-Server in den Einstellungen aus, diese Funktionalität bietet jedenfalls die kostenpflichtigen Pro-Version.
- Sie können mittels aktiviertem Passwortschutz und geschlossene Gruppe steuern wer den Gruppen-Meetings beitreten kann
- Bitte aktivieren Sie die Ende-zu-Ende-Verschlüsselung (E2EE) (<https://>)
 - 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.
 - ACHTUNG: wird nicht von der Web-Version unterstützt.
- Bitte deaktivieren Sie Einstellungen bei Zoom, die
 - Ein Tracking des Nutzerverhaltens bei der Konferenz
 - Eine Beobachtung des Nutzerverhaltens anlässlich der Konferenz oder
 - Eine Aufzeichnung ermöglichen.
- Die Auswahl von EU-Server in den Einstellungen, verhindert leider nicht die Übertragung von sog. Betriebsdaten (Operation Data)
 - Zu den Betriebsdaten gehören Konfigurationsdaten, Meeting-Metadaten, Nutzungsdaten, Leistungsdaten und Dienst-Protokolle
- Aufzeichnung sind wie bei Offline-Meeting üblich nicht gestattet, sollte dies widererwarten der Fall sein, so müssen alle Teilnehmer im Vorfeld darüber informieren werden.
- Sie können ferner Teilnehmer auf „unsichtbar“ stellen, sofern dies gewünscht ist.
- Eine Vorlage für die Datenschutzhinweis/-einwilligung finden Sie auf der Website der AA, diese kann auch als „Rechthinweis mit Zustimmungsfunktion“ als Voraussetzung zum Betreten eines Meetings implementiert werden.

Konkrete Handlungsschritte:

A. Vor Beginn Ihres Zoom-Meetings

- „Einstellungen“ aufrufen



I. „End-to-End-Verschlüsselung nutzen“

- Sicherheitsrelevante Einstellung
- Auffindbar unter: „Einstellungen“ -> „Sicherheit“

End-to-End-Verschlüsselung nutzen



Beim Anmelden oder Starten eines Meetings wählen Sie zwischen der erweiterten und der End-to-End-Verschlüsselung. Im letzteren Fall sind einige Funktionen (z. B. Cloud-Aufzeichnung, Telefon/SIP/H.323-Einwahl) stillgelegt. [Mehr erfahren](#)

II. Rechenzentrumsregionen für die Verarbeitung der Daten während der Übertragung auswählen

Um Rechenzentrumsregionen für alle Benutzer in Ihrem Konto auszuwählen:

- Melden Sie sich im Zoom Web Portal als Administrator mit der Berechtigung zur Bearbeitung von Kontoeinstellungen an.
- Klicken Sie im Navigationsbereich auf Kontoverwaltung und anschließend auf Kontoprofil.
- Vergewissern Sie sich im Abschnitt Transitdaten, dass die Option Rechenzentrumsregionen für im Transit befindliche Meeting-/Webinardaten anpassen aktiviert ist.
- Ist die Einstellung deaktiviert, klicken Sie auf die Status-Umschaltfläche, um sie zu aktivieren. Wird ein Bestätigungsdialog angezeigt, wählen Sie Einschalten, um die Änderung zu bestätigen.
- Markieren Sie die Regionen, durch die Sie Ihre Daten im Transit während Meetings und Webinaren weiterleiten möchten.

- (Optional) Wenn diese Einstellung für alle Benutzer Ihres Kontos verbindlich sein soll, klicken Sie erst auf das Schlosssymbol und anschließend auf Sperren, um die Einstellung zu bestätigen.

Vereinigte Staaten kann nicht ausgewählt werden, da dies der Bereich ist über den das Konto bereitgestellt wird. D.h. ich kann nicht ausschließlich einen EU-Server wählen, sondern nur die Rechenzentrumsregion über die Daten während der Übertragung verarbeitet werden.

III. „Alle Teilnehmer stumm schalten, wenn sie dem Meeting beitreten“

- Dies dient dem Privatsphäre-Schutz des Einzelnen
- Auffindbar unter: „Einstellungen“ -> „Besprechung planen“

<p>Teilnehmern Beitritt vor dem Host gestatten</p> <p>Teilnehmern die Teilnahme am Meeting vor Ankunft des Hosts erlauben</p>	<input type="checkbox"/>
<p>Personal-Meeting-ID zuschalten</p> <p>Eine Personal Meeting-ID (PMI) ist eine 9- bis 11-stellige Nummer, die Ihrem Konto zugewiesen wird. Sie können den Persönlichen Meetingraum besuchen, um Ihre Einstellungen für persönliche Meetings zu ändern. Mehr dazu</p> <p></p>	<input checked="" type="checkbox"/>
<p>Beim Planen eines Meetings die persönliche Meeting-ID (PMI) verwenden</p> <p>Sie können den Persönlichen Meetingraum besuchen, Ihre Einstellungen für persönliche Meeting zu ändern.</p>	<input type="checkbox"/>
<p>Zu Beginn eines Meetings die persönliche Meeting-ID (PMI) verwenden</p>	<input type="checkbox"/>
<p>Alle Teilnehmer stumm schalten, wenn sie dem Meeting beitreten</p> <p>Automatisch alle Teilnehmer stumm schalten, wenn sie dem Meeting beitreten. Der Host bestimmt, ob Teilnehmer selbst die Stummschaltung aufheben können. </p>	<input checked="" type="checkbox"/>

[Geändert](#) [Zurücksetzen](#)

IV. „Teilnehmerprofilbilder in einem Meeting ausblenden“

- Dient ebenfalls dem Schutz der Privatsphäre der Teilnehmer
- Auffindbar unter: „Einstellungen“ -> „In Meeting (Grundlage)“

<p>Teilnehmern erlauben, sich umzubenennen</p> <p>Erlauben Sie den Meetingteilnehmern und Diskussionsteilnehmern der Webinare, sich selbst umzubenennen. </p>	<input checked="" type="checkbox"/>
<p>Teilnehmerprofilbilder in einem Meeting ausblenden</p> <p>Alle Profilbilder von Teilnehmern werden ausgeblendet und nur ihre Namen auf dem Videobildschirm angezeigt. Die Teilnehmer können ihre Profilbilder während des Meetings nicht aktualisieren. </p>	<input checked="" type="checkbox"/>

[Geändert](#) [Zurücksetzen](#)

V. Einladung zum Zoom-Meeting

- Es empfiehlt sich, in der Einladung an Ihre Teilnehmer bereits einen Link zu Ihrer Datenschutzzinformation/-einwilligung sowie zum Auftragsverarbeitungsvertrag mit Zoom zu hinterlegen.

- Holen Sie sich außerdem die Einwilligung der Teilnehmer ein. Es muss in diesem Kontext darauf hingewiesen werden, dass zumindest Betriebsdaten in den USA verarbeitet werden können und dass dort kein gleichwertiges Datenschutzniveau existiert.
- „Rechtshinweis“
 - Hier kann die Datenschutzinformation/-Einwilligung eingefügt werden
 - Auffindbar unter: „Einstellungen“ -> „In Meeting (erweitert)“

Rechtshinweis aufrufen, wenn Sie ein Meeting beginnen oder einem beitreten

Erstellen Sie Ihren eigenen Haftungshinweis, der zu Beginn aller Meetings angezeigt wird, die von Ihrem Konto moderiert werden



VI. Geben Sie den Mitgliedern bzw. Teilnehmern Ihrer Konferenz eine echte Wahlmöglichkeit hinsichtlich der Teilnahme an der Videokonferenz

- Da die Meetings stets freiwillig sind, darf jeder entscheiden ob und wie lange er an dem Meeting teilnehmen möchte.
- Bei Meetings ohne Einladung ist darauf zu achten, dass Störer vom Host des Meetings gemutet bzw. aus dem Meeting entfernt werden.

VII. Stellen Sie sicher, dass nur berechtigte Personen auf die Videokonferenz zugreifen können

- Beschränken Sie den Zugang nur auf authentifizierte Teilnehmer. Das sind all diejenigen Nutzer, die einen Zoom-Account haben.
- Der Zugang zu Ihrem Zoom-Meeting sollte mit einem Passcode abgesichert sein.
- Es ist auch möglich, den Zugang auf Teilnehmer mit einer bestimmten E-Mail-Domain zu beschränken. Dann müssten aber alle Ihre Mitglieder eine geschäftliche bzw. dem Verein zuzuordnenden E-Mail-Adresse besitzen.
- Im „Wartezimmer“ kann der Meeting-Host die Zugänge steuern. Es ist möglich, alle Teilnehmer auf einmal zuzulassen oder einzeln nacheinander.
- Es besteht auch die Möglichkeit, ein Meeting zu schließen. Sodass bei Vollständigkeit der Gruppe keine weiteren Teilnehmer mehr hinzukommen können.

B. Während des Zoom-Meetings

- Teilnehmer dürfen selbst entscheiden, ob sie die Kamera- und Mikrofonfunktion nutzen wollen oder nicht. Auch der Nutzernamen ist frei vom Teilnehmer wählbar.
- Der Meeting-Host hat zudem die Möglichkeit, alle Teilnehmer auf „unsichtbar“ zu stellen. Dann ist für jeden Teilnehmer nur der Meeting-Host zu sehen.

