Übersicht zur datenschutzkonformen Nutzung des Videokonferenz-Programms „Zoom“

Zoom ist ein Softwareprogram 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.

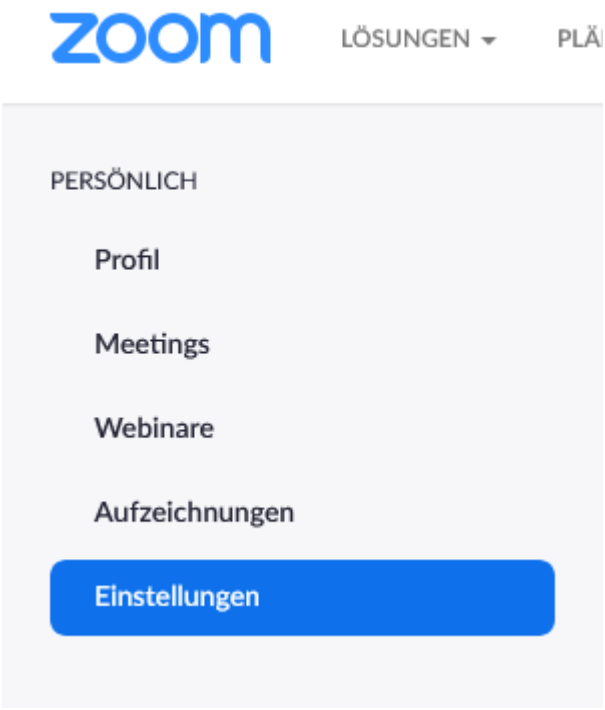
Erste Erwägungen zum datenschutzkonformen Umgang mit Zoom:

- 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 mitverifizierten 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 informiert und ihr Einwilligung eingeholt werden.
- Sie können ferner Teilnehmer auf „unsichtbar“ stellen, sofern dies gewünscht ist.
- Eine Vorlage für die Datenschutzinformation/-einwilligung finden Sie auf der Website der AA, diese kann auch im Wartebereich eines Meetings implementiert werden

Konkrete Handlungsschritte:

A. Vor Beginn Ihres Zoom-Meetings

- „Einstellungen“ aufrufen



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

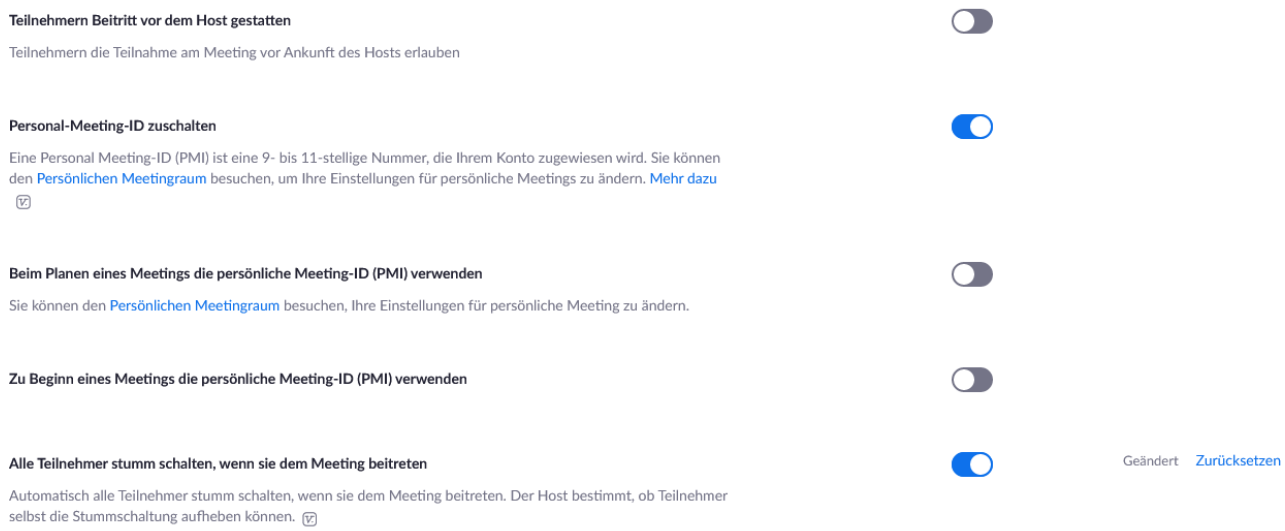
- Sicherheitsrelevante Einstellung
- Auffindbar unter: „Einstellungen“ -> „Sicherheit“

II. EU-Server auswählen

- Zunächst wählen Sie bitte die Region der Server für die Datenverarbeitung aus. Hier wählen Sie dann ausschließlich die EU-Server in den Einstellungen aus. Das geht allerdings nur mit der kostenpflichtigen Pro-Version. Bei geschäftlichem Einsatz daher unbedingt empfehlenswert (Pro-, Business-, Enterprise oder Bildungskonto)
- Einstellungsmöglichkeit auffindbar unter: Kontoverwaltung -> Kontoeinstellungen -> „Im Meeting (Erweitert)“ -> Rechenzentrumsregionen für durch Ihr Konto gehostete Meetings/Webinare auswählen“

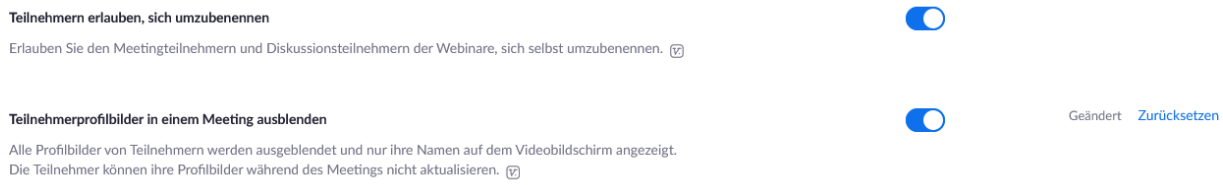
III. „Alle Teilnehmer stumm schalten, wenn sie dem Meeting beitreten“

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



IV. „Teilnehmerprofilbilder in einem Meeting ausblenden“

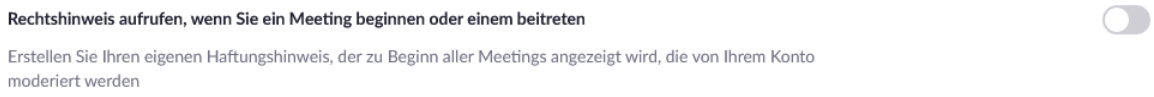
- Dient ebenfalls dem Schutz der Privatsphäre der Teilnehmer
- Auffindbar unter: „Einstellungen“ -> „In Meeting (Grundlage)“



V. Einladung zum Zoom-Meeting

- Es empfiehlt sich, in der Einladung an Ihre Teilnehmer bereits einen Link zu Ihrer Datenschutzinformation/-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 Datenschuztinformation/-einwilligung eingefügt werden

- Auffindbar unter: „Einstellungen“ -> „In Meeting (erweitert)“



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 berechtige 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 „Warteraum“ 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 Nutzername 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.