Handreichung zur Verwendung von Zoom im Hochschulkontext
Stand: 22. Juni 2023
Studium Digitale, Burg Giebichenstein Kunsthochschule Halle

Diese Empfehlung orientiert sich an der deutschen Datenschutz-Grundverordnung (DSGVO) „Hessischen Modell“ und an der Empfehlung des Österreichischen Bundesministeriums für Bildung, Wissenschaft und Forschung zur Nutzung von Zoom als Video-Kommunikationsmittel.

In der Vergangenheit wurde insbesondere die fehlende Ende-zu-Ende-Verschlüsselung des Anbieters kritisiert. Weiterhin konnte die DSVGO-Konformität nicht gewährleistet werden, da die Server von Zoom in den USA und teilweise in China angesiedelt waren. Inzwischen können in beiden Punkten alternative, DSGVO-konforme Einstellungen vorgenommen werden.

AES-256-Ende-zu-Ende-Verschlüsselung[1]

Meetings können mit der AES-256-Verschlüsselung gesichert werden, die als maximal sicher gilt. Mit AES-256 wird für jede Sitzung ein einmaliger Verschlüsselungsschlüssel erstellt und auf den Servern von Zoom verwaltet. Das bedeutet aber auch, dass die Schlüssel kompromittiert werden können, wenn Zoom Opfer eines Cybersicherheitsangriffs wird.

- muss extra aktiviert werden
- Ende-zu-Ende-Verschlüsselung, die Schlüssel werden auf den Rechnern der Nutzer*innen erstellt
- In E2EE kein Streaming oder Cloud-Aufnahme möglich

Datenverarbeitung

Bei Business-Accounts kann der Serverstandort eingestellt werden: Europa, USA, Australien, China, Indien, Japan/Hongkong, Kanada, Lateinamerika.
Personenbezogene Daten werden u.a. für Marketingzwecke und Produktforschung und -entwicklung verwendet. Meeting-, Webinar- und Chatinhanlte werden nicht verarbeitet.
Verarbeitete Meeting-Metadaten sind[2]:

- Titel des Meetings
- Beschreibung (optional)
- Start- und Endzeit
- Teilnehmer*innen-IP-Adressen
- Geräte/Hardware-Informationen (z.B. Browser, Audiogeräte, Verbindungsqualität), Start- und Endzeit

Die Daten werden in der ausgewählten Rechenzentrumsregion verarbeitet und nach 7 Tagen anonymisiert gespeichert.

1 https://support.zoom.us/hc/de/articles/360048660871-End-to-End-Verschlüsselung-E2EE-für-Meetings
2 https://www.bmbwf.gv.at/Ministerium/Datenschutz/Zoom.html

Zoom DSGVO-konform verwenden[3]:

- Beschränkung der Rechenzentrumsregionen von Zoom auf EU-Standorte (nur
- Regelmäßig Aktualisieren, um Updates mit behobenen Sicherheitslecks zu laden[4]
- Aufzeichnung und Streaming nur mit eindeutiger Einwilligung der Teilnehmer*innen
- Speicherung von Aufzeichnungen nur auf internen Laufwerken/Datenträgern, Löschungspflicht beachten
- Datentausch mit anderen Plattformen, wie Office 365, deaktivieren

Zusätzliche Empfehlungen im „Hessisches Modell“ [5]:

- Alle Inhalte Ende-zu-Ende-Verschlüsseln
- Nur für Lehrveranstaltungen nutzen, sensible Einzelgespräche über andere Anbieter abwickeln
- Hochschulen müssen alternatives datenschutzkonformes Videokonferenzsystem für andere Zwecke oder für Lehrpersonen, die nicht mit Zoom arbeiten wollen, anbieten

Weitere Tipps:

- Datenschutzsichere Umgebung: Alexa, Siri usw. nicht zuhören lassen
- Hintergrund im Video ausblenden, um Privatsphäre zu schützen
- Meeting-ID niemals öffentlich bekannt machen
- Warteraum-Funktion und ggf. unbekannte Nutzer*innen blockieren
- Meetings mit eindeutigem, starken Passwort schützen
- Automatische Speicherung von Inhalten, wie der Chat-Kommunikation oder Whiteboard-Inhalten deaktivieren

3 https://nordvpn.com/de/blog/zoom-datenschutz/#:~:text=Mit%20den%20richtigen%20Einstellungen%2C%20wie,Verbesserungen%2C%20ist%20Zoom%20zurzeit%20datenschutzkonform.
4 https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/TW/2022/04/warnmeldung_tw-t22-0101.html
5 https://www.datenschutz.de/mit-schutzmassnahmen-ist-zoom-fuer-lehrveranstaltungen-an-hessischen-hochschulen-nutzbar/