Aktuelle Stellungnahmen zum Datenschutz bei Zoom

Durch die aktuelle Situation steigt die Nachfrage von Videokonferenzsoftware enorm. Auch der Deutsche Fundraising Verband e.V. hat sich im Hinblick auf unsere Veranstaltungs- und Vernetzungsformate intensiv mit den unterschiedlichen Softanbietern befasst und diese verglichen.

Verschiedene Parameter wie Funktionalität, Stabilität, Sicherheit und Datenschutz wurden bei der Auswahl miteinbezogen. Die Entscheidung fiel letztendlich auf den Anbieter Zoom, da sich die Software als eine verlässliche Lösung mit hoher Konferenzqualität etabliert hat.

Bedingt durch die sehr große Nachfrage steht der Anbieter Zoom seit einiger Zeit unter Beobachtung von Sicherheitsexpert*innen weltweit. Auch Zoom wurde von den Entwicklungen im Umfeld von Corona überrascht und nun gefordert ist, in kurzer Zeit auf die vielfältigen Anforderungen sowohl technisch, als auch organisatorisch zu reagieren.

Untenstehend finden Sie eine Übersicht der Stellungsnahmen von Zoom zu den wichtigsten Fragestellungen.

Privacy Policy

Die Privacy-Policy von Zoom wurde am 29.3.2020 aktualisiert, um einige Aussagen deutlicher herauszuarbeiten.

https://zoom.us/privacy?zcid=1231

Stellungnahmen von Zoom

Zoom kommentiert mittlerweile regelmäßig neue Problembereiche unter

https://blog.zoom.us/

Aufzeichnung

Aufzeichnungen von Veranstaltungen werden im Nachgang auf einer passwortgeschützten Seite nur Teilnehmer*innen der jeweiligen Veranstaltung bereitgestellt. In den Protokollen werden die Teilnehmer*innen anonymisiert.

Zoom und Data-Mining

Zoom beschreibt zur Frage des Umgangs mit Data-Mining:

"Importantly, Zoom does not mine user data or sell user data of any kind to anyone."

https://theintercept.com/2020/03/31/zoom-meeting-encryption/

Senden von Daten an Facebook bei iOS-App

Auf die Datenschutzlücke vom 26.3.2020, bei der bekannt wurde, dass der Zoom-Client unter iOS auch ohne Facebook-Account Daten an Facebook schickt (https://www.vice.com/en_us/article/k7e599/zoom-ios-app-sends-data-to-facebook-even-if-you-dont-have-a-facebook-account),

hat Zoom innerhalb weniger Tage reagiert und diese Lücke geschlossen (https://blog.zoom.us/wordpress/2020/03/27/zoom-use-of-facebook-sdk-in-ios-client/)

Sicherheitslücken im Mac-Zoom-Client

Am 30.3.2020 wurden Sicherheitsprobleme im Mac-Zoom-Client erkannt, die u.a. mittels Phishing ausnutzbar waren (https://techcrunch.com/2020/04/01/zoom-doom/, https://heise.de/-4695129).

Zoom gibt im Blog unter https://blog.zoom.us/wordpress/2020/04/01/a-message-to-our-users/ am 1.4.2020 an, diesen Fehler geschlossen zu haben: ”Released fixes for both Mac-related issues raised by Patrick Wardle.”

Eine detaillierte, technische Beschreibung der Probleme gibt Patrick Wardle unter der Primärquelle https://objective-see.com/blog/blog_0x56.html.

Nachweislich wurden beide beanstandeten Sicherheitsprobleme im aktuell herunterladbaren Mac-Zoom-Client behoben (Zeitstempel des Codesigning für den Installer: 2. Apr 2020 at 15:15:06).

Wurden Accounts und Passwörter von Zoom angegriffen?

Es wurden ca. 500.000 Accounts mit Klartextpasswörtern publiziert, die anscheinend auch bei Zoom funktionieren
https://www.bleepingcomputer.com/news/security/over-500-000-zoom-accounts-sold-on-hacker-forums-the-dark-web/
Es wird vermutet, dass diese Accounts aus früheren Hacks anderer Webseiten stammen.

Ende-zu-Ende Verschlüsselung

Zoom bietet immer eine TLS-basierte Transportverschlüsselung (sofern Sie nicht mit normalem Telefon teilnehmen), jedoch eine Ende-zu-Ende-Verschlüsselung (End-to-End Encryption, E2EE) für Video-Gruppenkonferenzen nur mit Endpunkten, die bei Zoom liegen. Entsprechend nutzte Zoom diesen Begriff anders, als er normalerweise benutzt wird, in dem die Endpunkte die Geräte der Videokonferenzteilnehmer sind (https://theintercept.com/2020/03/31/zoom-meeting-encryption/).

Eine in den USA eingereichten Klage soll klären, ob durch die unübliche Verwendung des Begriffes “End-to-End-Verschlüsselung” für Zoom ein unzulässiger Wettbewerbsvorteil erlangt wurde. Prinzipiell sind auch die Pexip-Konferenzen, die wir vom DFN einsetzten, nicht End-to-End verschlüsselt.

Zoom hat mittlerweile eine Stellungnahme bzgl. End-to-End-Verschlüsselung veröffentlicht (https://blog.zoom.us/wordpress/2020/04/01/facts-around-zoom-encryption-for-meetings-webinars/), worin dargestellt wird:

“To be clear, in a meeting where all of the participants are using Zoom clients, and the meeting is not being recorded, we encrypt all video, audio, screen sharing, and chat content at the sending client, and do not decrypt it at any point before it reaches the receiving clients.”

Wenn der Zoom-Client eingesetzt wird und das Meeting nicht aufgezeichnet wird, werden demnach gemäß der Aussage von Zoom alle Inhalte verschlüsselt und nicht mitgeschnitten.

Abwägung zum Einsatz von Zoom mit einem Browser oder mit dem Zoom-Client

Wenn Sie Zoom mit einem Browser einsetzen, sprechen wir uns, wie bei fast allen Videokonferenz-Systemen über das Web für die Verwendung von Google Chrome aus, da dieser Browser derzeit die beste Umsetzung der hierfür notwendigen WebRTC-Standards implementiert. Bei Verwendung des Browsers werden weniger Daten, z.B. in Bezug auf die für die Konferenz verwendeten Geräte, erhoben. Die Funktion “Virtueller Hintergrund”, mit der in Bezug auf die häusliche Umgebung im Home-Office ein erhöhter Schutz der Privatsphäre möglich ist, kann mit dem Browser nicht genutzt werden.

Der Zoom-Client bietet in der Regel ein besseres Konferenzerlebnis und funktioniert häufig problemfreier. Im Gegenzug werden mehr Daten über die eingesetzten Geräte, wie den eigenen Rechner und die Audio-/Videogeräte erhoben. Die Nutzung der Funktion “Virtueller Hintergrund” ermöglicht einen eingeschränkten Schutz der heimischen Privatsphäre.

Maschinelles Aufmerksamkeits-Tracking

Zoom hat diese Funktion am 1.4.2020 allgemein abgeschaltet.

https://blog.zoom.us/wordpress/2020/04/01/a-message-to-our-users/

Was ist *Zoombombing*?

Wer Videokonferenzen ohne weiteren Zutrittsschutz erstellt (z.B. ein Passwort) und die URL dann öffentlich verfügbar macht, setzt sich dem Risiko aus, das ungewollte Konferenzteilnehmer eintreten und unerwünschtes Verhalten zeigen. Diese Probleme sind dem Bereich Spam, Trolling oder ggf. auch Phishing zuzurechnen, bei dem laufende Kommunikation, die frei im Netz erreichbar ist, gestört wird. Es kann durch den Einsatz von Passwörtern für Konferenzen eingeschränkt werden. Auf jeden Fall sollten Sie nicht ungeprüft auf jeden Link klicken, der in den Chat eingefügt wird sondern immer zunächst auf Plausibilität prüfen, wie bei E-Mails auch. Der Begriff *Zoombombing* geht einerseits auf die aktuelle Beliebtheit der Plattform Zoom zurück und andererseits war es möglich, die URLs für eine Zoom-Videokonferenz zu erraten. Wir haben das Problem derzeit so aufgegriffen, dass neu angelegte Konferenzen standardmäßig mit Passwort angelegt werden (https://www.golem.de/news/zoombombing-trolle-uebernehmen-zoom-konferenzen-2003-147606.html).

Personal Meeting ID nicht veröffentlichen

Die *Personal Meeting ID* kann nicht ohne Weiteres verändert werden. Es ist deshalb darauf zu achten, diese ID nicht auf frei einsehbaren Webseiten zu veröffentlichen.

Welche Zertifizierungen erfüllt Zoom bzgl. Datenschutz und Sicherheit?

(Quelle: https://zoom.us/docs/doc/Zoom-Security-White-Paper.pdf)

- SOC2
- TRUSTe

- FedRAMP
- GDPR (mit Privacy Shield)

Welche Daten werden von Zoom verarbeitet?

Es werden Metadaten wie Konferenznamen und Zeiten, IP und Name, Stadt, aber auch zu den eingesetzten Geräten (z.B. Webcams, Headsets, Lautsprecher) und Betriebssystemen erhoben.

Dazu kommen detaillierte Daten zu der Qualität der Netzwerkverbindung von den Teilnehmenden.

Zusätzlich wird die Anzahl von Chats, gesendeten/empfangen Nachrichten, Anrufen, Dateitransfers, verschickten Bildern, Sprachnachrichten, Videos und Emojis für jede Person gespeichert.

Data Mining findet nach Aussage von Zoom nicht statt und es werden keine Daten an Dritte verkauft.

Datenkategorien und Verarbeitung

Kategorien der personenbezogenen Daten

Nummer	**Bezeichnung der Daten**
1	Benutzerprofil: siehe Daten, die durch SSO übermittelt werden
2	Meeting-Metadaten: Thema, Beschreibung (optional), Teilnehmer-IP-Adressen, Geräte-/Hardware-Informationen
3	Meeting-Aufzeichnungen: Mp4 aller Video- und Audioaufnahmen und Präsentationen, M4A aller Audioaufnahmen, Textdatei aller in der Besprechung, Chats, Audio-Protokolldatei
4	IM-Chat-Protokolle (bei HU-Zoom deaktiviert)
5	Telefonie-Nutzungsdaten (optional): Ggf. Rufnummer des Anrufers, Name des Landes, IP-Adresse, 911-Adresse (registriert Dienstadresse der Humboldt-Universität), Start- und Endzeit, Hostname, Host-E-Mail, MAC-Adresse des verwendeten Geräts
6	Rechnungs- und Beschaffungsdaten (nur für Administrator*innen einsehbar)

Kategorien der betroffenen Personen

Nummer nach Datenkategorien	**Bezeichnung der Daten**
1-5	Nutzende
3-4	In der Kommunikation erwähnte weitere Personen
6	Beschaffer, Anforderer

Kategorien der Empfänger, denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen

(https://zoom.us/de-de/subprocessors.html)

Nr.	**Empfänger**	**Anlass der Offenlegung**	**Speicherort**
1-5	Zoom Video Communications, Inc.	Auftragsverarbeitung	Vereinigte Staaten von Amerika und Unterauftragsverarbeiter
		Unterauftragsverarbeiter	
6	People.ai	Vertrieb, CRM	Vereinigte Staaten von Amerika
1-6	Zendesk	Support	Vereinigte Staaten von Amerika
1, 6	Wootric	Kundenumfragen	Vereinigte Staaten von Amerika
6	Totango	Onboarding, Kundenerfahrung	Vereinigte Staaten von Amerika
1, 6	Answerforce	Kundensupport	Vereinigte Staaten von Amerika
1	Rocket Science Group, LLC	E-Mail-Benachrichtungen	Vereinigte Staaten von Amerika
1, 6	Five9	Callcenter	Vereinigte Staaten von Amerika
1 – 6	EPS Ventures	Support	Malaysia
1- 6	WKJ Consultancy	Support	Malaysia
6	Salesforce	Kundenmanagement	Vereinigte Staaten von Amerika
1, 6	CyberSource	Bezahlung und Betrugsprävention	Vereinigte Staaten von Amerika
1, 6	Adyen	Bezahlung und Betrugsprävention	Europa
6	Zuora	Abomanagement	Vereinigte Staaten von Amerika

1-6	Amazon Web Services	Infrastruktur (IT)	Vereinigte Staaten von Amerika, EU, Kanada, Australien
1-6	Bandwidth	Infrastruktur (Telefonie)	Vereinigte Staaten von Amerika

internationale Organisation

Nummer nach Datenkategorien	**Drittland oder internationale Organisation**	**Geeignete Garantien im Falle einer Übermittlung nach Art. 49 Abs. 1 Unterabsatz 2 DSGVO**
1-6	Vereinigte Staaten von Amerika	Standarddatenschutzklauseln https://zoom.us/docs/doc/Zoom_GLOBAL_DPA_December_19.pdf EU-US-PrivacyShield https://www.privacyshield.gov/participant?id=a2zt0000000TNkCAAW&status=Active
1-6	Vereinigte Staaten von Amerika, Malaysia, Kanada, Australien	Unterauftragsverarbeiter Garantie durch Standarddatenschutzklauseln