Datenschutzanalyse Zoom

I. Zu bewertendes Verfahren/Tool und Zweckbestimmung

Die Software Zoom Meetings ist ein Dienst, mit dem Nutzende über eine Desktop- oder Smartphone-App, über eine Weboberfläche, per Telefon oder über ein Konferenzraum-System an Online-Videokonferenzen teilnehmen können. Über einen Chat können Nutzende Textnachrichten und Dateien austauschen und ein virtuelles Whiteboard nutzen. Eine eingeschränkte Nutzung des Diensts zur Veranstaltung von Videokonferenzen ist für registrierte Nutzende kostenlos, dabei ist die Dauer von Videokonferenzen mit Gruppen zeitlich beschränkt. Sitz der Zoom Video Communications Inc. ist San José in den USA.

1. Betroffenengruppen, deren personenbezogene Daten verarbeitet werden

- alle Dienstnutzende

2. Art der Daten

Je nach Art und Umfang der Nutzung von Zoom werden verschiedene Arten von Daten erhoben bzw. verarbeitet. Hierzu gehören insbesondere:

- Angaben zu Ihrer Person (z.B. Vor- und Nachname, E-Mail-Adresse, Profilbild)
- Meeting-Metadaten (z.B. Datum, Uhrzeit und Dauer der Kommunikation, Name des Meetings, Teilnehmer-IP-Adresse)
- Geräte-/Hardwaredaten
- Text-, Audio- und Videodaten
- Verbindungsdaten (z.B. Rufnummern, Ländernamen, Start- und Endzeiten, IP-Adressen)

3. An der Verarbeitung beteiligten Komponenten (Systeme und Dienste sowie Prozesse)

An der Verarbeitung und Speicherung personenbezogener Daten durch Zoom als Datenverarbeiter sind 6 Unterauftragnehmer beteiligt, deren Sitz in den USA liegt.

Gefördert vom
Ministerium für Kultur und Wissenschaft des Landes Nordrhein-Westfalen

Zoom behauptet, mit den Unternehmen Auftragsdatenverarbeitungsverträge mit Hinweis auf die Standardschutzklauseln der EU abgeschlossen zu haben. Die Liste der Dienstleister finden Sie unter https://explore.zoom.us/docs/de-de/subprocessors.html Bei der „Bezahlvariante“ kann man als Voreinstellung für die Datenspeicherung „EU“ auswählen, sodass die meisten Daten innerhalb der EU verarbeitet werden. Die kostenlose Variante verarbeitet die Daten an verschiedenen Standorten weltweit. Meeting-Meta-Daten werden immer - auch bei der „Bezahlvariante“ - in den USA verarbeitet.

Zoom setzt 26 Cookies unbekannter Funktion ein, nach eigener Aussage in der Datenschutzerklärung "betriebsnotwendig" für die Seite, darunter auch solche, die eine Google-Captcha-Funktion integrieren. Mit *Google reCAPTCHA* werden Nutzende und ihr Verhalten auf der Webseite, wo *reCAPTCHA* eingebunden ist, ausgesprochen tiefgehend analysiert. Da der *reCAPTCHA* Code u.a. von der Domäne *google.com* geladen wird, erhält das Tool automatisch Zugang zu Cookies, die für angemeldete Google Nutzende gesetzt werden. Das Cookie *NID* enthält eine eindeutige Nutzerkennung, die auch für *Google Signals* verwendet wird, um sogar geräteübergreifend Nutzende wiedererkennen zu können.

Zoom setzt darüber hinaus 3 Tracker ein:

- Google Analytics
- GoogleTagManager
- Tracker von Demandbase

II. Schutzbedarfsbestimmung

1. Gewährleistungsziele: Datenminimierung, Vertraulichkeit, Nichtverkettung, Intervenierbarkeit, Transparenz.

2. Schadenshöhe:

Normal: Je nach Nutzung werden personenbezogene Daten verarbeitet, deren missbräuchliche Verarbeitung den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigen kann.

Gefördert vom
Ministerium für Kultur und Wissenschaft des Landes Nordrhein-Westfalen

Hoch: Abhängig vom Inhalt der Videokonferenz können auch personenbezogene Daten verarbeitet werden, deren missbräuchliche Verarbeitung die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen erheblich beeinträchtigen kann. Darunter fallen personenbezogene Daten besonderer Kategorien, personenbezogene Daten, die dem Berufsgeheimnis unterliegen, deren Verarbeitung zu einer Diskriminierung, einem Identitätsdiebstahl oder -betrug, einem finanziellen Verlust, einer Rufschädigung, der unbefugten Aufhebung der Pseudonymisierung oder anderen erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen führen kann. Das sind z.B. Gesundheitsdaten oder personenbezogene Daten Schutzbedürftiger (z.B. Kinder).
Dient das Videokonferenztool der Geschäftsleitung auch zur Kommunikation über Geschäftsgeheimnisse, ist das Geschäftsgeheimnisgesetz zu berücksichtigen. Aufgrund des sog. Patriot Acts haben amerikanische Behörden das Recht auch auf Inhalte von Videokonferenzen zuzugreifen, ohne dass es den Betroffenen bekannt wird.

III. Ermittlung von Gefährdungen/ Bedrohungen für die Verfahrenskomponenten

Bedrohungen werden anhand des Gefährdungskatalog (IT Grundschutzkompendium) ermittelt.

1. Aus der Gestaltung der Verarbeitungstätigkeit

Es gibt einige „Werkseinstellungen“, die bei Einrichtung von Zoom unbedingt deaktiviert werden müssen, damit die Nutzung von Zoom nicht von vornherein absolut rechtswidrig ist (siehe unter Auswertung – Grundeinstellung bei Meetings).

2. Aus dem Bereich IT Sicherheit und dem organisatorischen Umfeld der Verarbeitung

Aus dem Einsatz der Trackingtools und reCAPTCHA und aus der Tatsache, dass alle Subunternehmer in den USA angesiedelt sind, ergibt sich die Gefahr der Offenlegung persönlicher (oder anderweitig geschützter) Daten. Die Art und Weise, wie Informationen offengelegt werden, kann sehr unterschiedlich sein, zum Beispiel: unbefugtes

Gefördert vom
Ministerium für Kultur und Wissenschaft des Landes Nordrhein-Westfalen

Auslesen von Dateien, unbedachte Weitergabe, Abhören von Übertragungsleitungen, Infektion von IT-Systemen mit Schadprogrammen, Mitlesen am Bildschirm oder Abhören von Gesprächen.

IV Bewertung der Eintrittswahrscheinlichkeit

Äußerst selten:

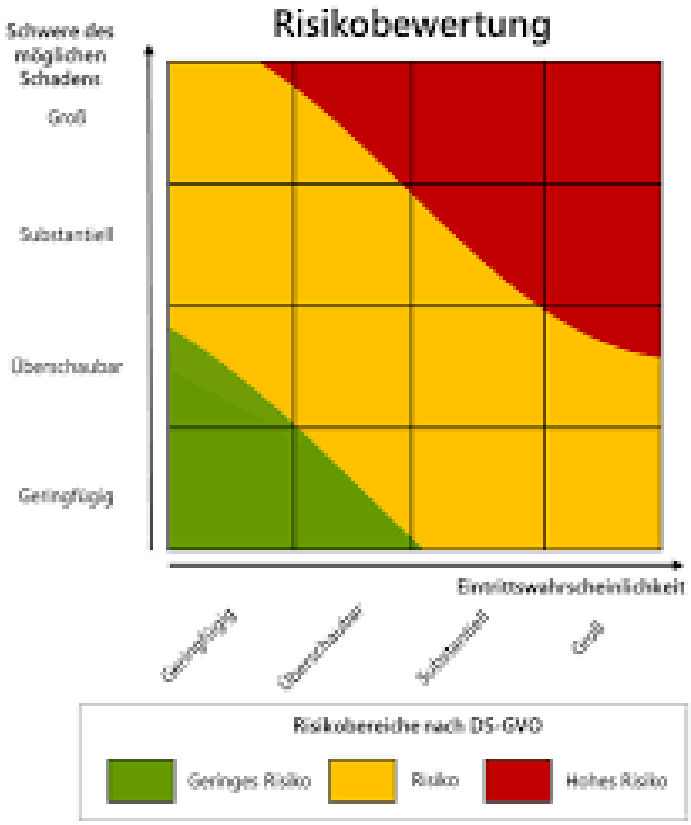
Selten: Identitätsdiebstahl ist nicht ausgeschlossen, aber unwahrscheinlich.

Gelegentlich:

Häufig: Der Einsatz von *reCAPTCHA* dient üblicherweise der Verkettung unterschiedlicher personenbezogener Informationen, umso ein klares Bild des Users zu erhalten.

Ohne Anpassung der Einstellungen besteht ein hoher Grad an Wahrscheinlichkeit dafür, dass die Daten missbräuchlich verwendet werden.

Zumindest die User-Meta-Daten werden auf amerikanischen Servern verarbeitet. Die Metadaten gehen mithin in ein Drittland, dessen Datenschutzniveau nicht mit dem europäischen vergleichbar ist. Die Behauptung, Zoom habe Standardschutzklauseln berücksichtigt, täuscht nicht darüber hinweg, dass aufgrund des sog. Patriot Act sämtliche in den USA verarbeitete personenbezogene Daten durch insgesamt 24 unterschiedliche Behörden abgerufen und verarbeitet werden dürfen, ohne dass der Betroffene davon erfährt bzw. dagegen vorgehen kann.



Gefördert vom
Ministerium für Kultur und Wissenschaft des Landes Nordrhein-Westfalen

Bewertung:

Normale bis hohe Schadenshöhe bei einer häufigen Eintrittswahrscheinlichkeit eines Datenschutzschadens.

V. Auswertung und Endergebnis:

Kein Tool ist umstrittener als das Videokonferenztool Zoom.

Was man der Zoom Video Communications Inc. zu Gute halten muss, ist, dass sie bislang auf Kritik zum Datenschutz immer reagiert hat und im Sinne der DS-GVO nachgebessert hat. So gibt es z.B. seit Mitte letzten Jahres eine Ende-zu-Ende-Verschlüsselung. Stand heute (November 2021) bleibt folgende Problematik ungelöst:

Alle Nutzende müssen auf jeden Fall darüber informiert werden, dass Zoom Trackingtools verwendet und dementsprechend der Einsatz eines entsprechenden Browser-AddOn, wie z.B. Ad AdGuard, unbedingt notwendig ist.

Es bleibt ungeklärt, welche Funktion die 26 Cookies haben, die als betriebsnotwendig bezeichnet werden, bei denen aber auch solche mit Google-Captcha-Funktion zu finden sind, was die Vermutung einer tiefgehenden Nutzeranalyse nahelegt.

Ein großer Teil der Datenverarbeitung erfolgt durch Subauftragnehmer der Zoom Inc. in den USA, mit denen die Zoom Inc. nach eigenen Angaben Verträge abgeschlossen hat, die durch Standarddatenschutzklauseln (Art. 46 DS-GVO) den Datenschutz garantieren. Ebenso verarbeitet Zoom Inc. selbst die User-Meta-Daten in den USA und garantiert ebenfalls durch Abschluss von Standardschutzklauseln, dass auch sie selbst ein angemessenes Datenschutzniveau im Sinne der §§ 44 DS-GVO (§ 40 KDG) gewährleisten. Aufgrund eines amerikanischen Bundesgesetzes, dem sog. Patriot Act, ist es unterschiedlichen US-Behörden erlaubt, sämtliche in den USA verarbeitete personenbezogene Daten einzusehen und zu verarbeiten. Der Hamburger Datenschutzbeauftragte warnt davor, dass die Teilnehmer*innen der Videokonferenz auf diese Weise der Gefahr einer anlasslosen staatlichen Massenüberwachung in

Gefördert vom
Ministerium für Kultur und Wissenschaft des Landes Nordrhein-Westfalen

den USA ausgesetzt werden, gegen die keine ausreichenden Rechtsschutzmöglichkeiten bestehen (Senatskanzlei formell gewarnt: https://datenschutz-hamburg.de/pressemitteilungen/2021/08/2021-08-16-senatskanzlei-zoom).

Insgesamt ist von einem Einsatz auf jeden Fall dann abzuraten, wenn nicht nur dienstliche Endgeräte eingesetzt werden, sondern auch private Endgeräte z.B. von Teilnehmenden.

Wer dennoch Zoom nutzen möchte, sollte mindestens Folgendes bei den Einstellungen berücksichtigen:

Grundeinstellung bei Meetings

- Alle Meetings beginnen mit abgeschaltetem Mikrofon. Das Mikrofon muss von dem Teilnehmer*innen aktiv eingeschaltet werden.
- Einblendung von E-Mail-Adressen in geteilten Inhalten als Wasserzeichen ist unterbunden.
- Für alle Meetings wird als Zugriffsschutz ein 6-stelliger numerischer Pincode gesetzt (dieser ist im Meetinglink bereits enthalten).
- Feedbacks an Zoom am Ende eines Meetings sind deaktiviert.
- Remoteunterstützung ist deaktiviert.
- Kamera-Fernsteuerung ist deaktiviert.

Allgemeine technische Einstellungen

- Beschränkung der eingesetzten Rechenzentrumsregionen von Zoom auf EU-Standorte
- Erzwungene End- zu End Verschlüsselung der Instant Messaging-Chatnachrichten (Chats außerhalb von Meetings!)
  ACHTUNG: Bei der Einstellung End- zu End Verschlüsselung ist es nicht möglich, während des Meetings Breakout-Sessions einzurichten.
- Wenn sich nur zwei Personen in einem Meeting befinden, wird eine Peer-to-Peer-Verbindung aufgebaut.

Gefördert vom
Ministerium für Kultur und Wissenschaft des Landes Nordrhein-Westfalen

Datenaustausch mit anderen Diensten

- Datenaustausch mit Office 365 ist deaktiviert.
- CDN-Nutzung ist deaktiviert.

Speicherung von Meeting-Inhalten

- Die automatische Speicherung der Chat-Kommunikation für den Host ist unterbunden.
- Die automatische Speicherung von Whiteboard-Inhalten ist unterbunden.
- Aufzeichnung von Meetings in der Zoom-Cloud ist deaktiviert.
- Lokale Aufzeichnung von Meetings ist für den Host erlaubt, bedarf allerdings der Zustimmung aller Teilnehmer*innen.
- Automatische Aufzeichnung bei Meeting-Beginn ist generell deaktiviert.
- Benachrichtigungen für den Host bei Start der Meetings-Aufzeichnung.

Eine Aufzeichnung darf nur mit ausdrücklicher schriftlicher vorheriger Einwilligung aller Teilnehmenden erfolgen und auch folgende weitere Hinweise sollten berücksichtigt werden:

1. Aufzeichnung nur mit ausdrücklicher Einwilligung aller Teilnehmenden

Eine Aufzeichnung darf nur mit der ausdrücklichen Einwilligung aller betroffenen Teilnehmer*innen erfolgen und nur soweit dies für die konkrete Aufgabenerfüllung erforderlich ist. Die Einwilligung hat die/der Aufnehmende vorab von allen Teilnehmer*innen einzuholen. Bei Aufzeichnungen sind insbesondere Urheberrechte und die Persönlichkeitsrechte der Betroffenen zu wahren.

2. Speicherung von Aufzeichnungen

Die Speicherung von Aufzeichnungen sollte ausschließlich auf internen Laufwerken/ Datenträgern erfolgen. Aufgezeichnete Veranstaltungen dürfen nur so lange gespeichert werden, wie dies für die Erfüllung der jeweiligen Aufgabe erforderlich ist und solange keine Löschungspflicht besteht.

Gefördert vom
Ministerium für Kultur und Wissenschaft des Landes Nordrhein-Westfalen

3. Achten Sie auf die Umgebung

Darüber hinaus beachten Sie auch, dass keine Unberechtigten der Videokonferenz folgen können sowie, dass smarte Geräte, wie Sprachassistenten wie Alexa, Siri und Co. sich nicht im Anwendungsbereich befinden oder aktiv sind, um unzulässige Datenverarbeitungen/Aufnahmen zu verhindern.

Sie sollten auf jeden Fall die Nutzung von Zoom für den Austausch besonderer Kategorien personenbezogener Daten („sensible Daten“ z.B. Gesundheitsdaten) untersagen.

Es muss ein Auftragsdatenverarbeitungsvertrag mit Zoom geschlossen werden, der allerdings schon bei der Anmeldung generiert wird. Nur bei Nutzung einer bezahlten Version von Zoom kann der Standort Europa für den Teil der Datenverarbeitung, der durch Zoom erfolgt, festgelegt werden.

Gefördert vom

Ministerium für Kultur und Wissenschaft des Landes Nordrhein-Westfalen