Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

Dienstanweisung zur Nutzung des Videokonferenzsystems Zoom vom 30.07.2021

Mit dieser Dienstanweisung verliert die „Dienstanweisung zur Nutzung des Videokonferenzsystems Zoom vom 30.10.2020“ ihre Gültigkeit.

Die Durchführung digitaler Veranstaltungen und Besprechungen ist im Rahmen der Corona-Pandemie notwendig und unerlässlich geworden. Das Ziel muss es sein, Online-Prüfungen, große Veranstaltungen wie Vorlesungen, aber auch andere Besprechungsformate im Tagesgeschäft der Universität bis hin zu Auswahlgesprächen störungsfrei und ohne Abbrüche sowie datensicher durchführen zu können. Das Videokonferenzsystem Zoom bietet unter Beachtung der Vorgaben dieser Dienstanweisung und der Realisierung technischer Rahmenbedingungen diese Möglichkeiten.

Das Regionale Rechenzentrum (RRZ) hat hierfür eigene Serverkapazitäten geschaffen, mit denen die eigentliche Konferenz von den Servern der Firma Zoom weggenommen wird und die Konferenz ausschließlich auf den Servern der Universität Hamburg durchgeführt wird. In Ergänzung dazu setzt eine datenschutzgerechte Nutzung des Systems Zoom auch die Einhaltung bestimmter Verhaltensregeln im Umgang mit Zoom voraus.

Diese Dienstanweisung enthält deshalb Vorgaben für die Nutzung von Zoom, die von allen Beschäftigten der Universität Hamburg zwingend einzuhalten sind. Hinweise zur Umsetzung der folgenden Vorgaben und zur technischen Nutzung von Zoom erhalten Sie über folgenden Link:

https://www.rrz.uni-hamburg.de/zoom

1. Ausschließliche Nutzung des Zoom-Services der Universität Hamburg

Die Nutzung von Zoom ist nur unter Verwendung des Zoom-Services der Universität zulässig, der über die Einstiegsseite http://uni-hamburg.zoom.us angeboten wird. Dabei ist auf dem genutzten Endgerät zwingend die Zoom-Client-Software zu installieren – eine Teilnahme über einen Webbrowser ist nicht möglich. Nur so kann sichergestellt werden, dass die Kommunikation datenschutzkonform über Server erfolgt, die in der Universität im RRZ betrieben werden und dass die Inhalte vertraulich bleiben. Außerdem ist in dieser Lösung sichergestellt, dass die

Authentifizierung der Nutzenden, die ein Meeting einrichten, über die sichere Authentifizierungsinfrastruktur der Universität im RRZ auf der Basis der universitären Benutzerkennung erfolgt. Die Teilnahme an von anderen Einrichtungen initiierten Videokonferenzen, zu denen Sie etwa durch Kolleginnen oder Kollegen außerhalb der Universität Hamburg eingeladen werden, ist zwar nicht grundsätzlich ausgeschlossen. Je nach dem Schutzbedarf der Inhalte und nach verwendeter Videokonferenzlösung ist aber Vorsicht geboten, da dabei nicht notwendigerweise dieselben hohen Maßstäbe an den Datenschutz bzw. die Vertraulichkeit der Kommunikation gelten wie an der Universität Hamburg.

2. Einrichtung eines Meetings

a. Thema

Bei der Einrichtung eines Meetings ist das Thema bzw. der Titel allgemein zu halten (bspw. „Zoom-Meeting“), da dieses an Zoom übermittelt wird. Bei der Einladung von Teilnehmerinnen und Teilnehmern (bspw. über Outlook) kann das eigentliche Thema bzw. der Titel des Meetings angegeben werden.

b. Einladungstext

Im Rahmen der Einladung sind die Teilnehmerinnen und Teilnehmer einer Konferenz auf die Möglichkeit der pseudonymisierten Teilnahme, auf das Verbot der Weitergabe der Zugangsdaten und auf ihre Betroffenenrechte nach den Artikeln 12 bis 21 Datenschutz-Grundverordnung hinzuweisen. Ein entsprechender Hinweistext (https://uhh.de/einladung-zoom-meeting) wird bei der Einladung über den Zoom-Client automatisch in die Termineinladung übernommen und darf nicht gekürzt oder entfernt werden.

c. Beschränkung des Teilnehmerkreises (Zugangsbeschränkungen)

Zur weiteren Wahrung der Vertraulichkeit von Wort und Bild in Veranstaltungen und Konferenzen und um Störungen bzw. Angriffe von außen zu vermeiden (sog. „Zoom-Bombing“) ist die Zahl der Teilnehmerinnen und Teilnehmer in der Form zu begrenzen, dass nur Personen den Veranstaltungen beiwohnen können, die auch tatsächlich eingeladen wurden. Das bedeutet, dass das jeweilige Meeting vom Host der Veranstaltung grundsätzlich mit einem Passwortschutz eingerichtet werden muss und das Passwort ausschließlich mit der Einladung zu versenden ist, um zu gewährleisten, dass nur berechtigte Personen teilnehmen. Eine Veröffentlichung des Passworts auf der Webseite ist nicht zulässig.

Die Teilnehmerinnen und Teilnehmer sollten auch darauf hingewiesen werden, dass die Weitergabe der Login-Daten für eine Veranstaltung ausdrücklich verboten ist.

Die Teilnahme unerlaubter Dritter führt zum Abfluss von personenbezogenen Daten der Teilnehmerinnen und Teilnehmer, was von Seiten der Universität zwingend zu verhindern ist.

3. Aufzeichnung einer Lehrveranstaltung

Aufzeichnungen von Lehrveranstaltungen können nur angefertigt werden, wenn dieses datenschutzkonform ausgestaltet wird. Aufgezeichnete Lehrveranstaltungen via Zoom sind deshalb ausschließlich in Form eines Webinars durchzuführen, mit dem sichergestellt wird, dass nur die Vortragenden gefilmt werden.

Eine Aufzeichnung von Veranstaltungen, Vorlesungen oder Diskussionen außerhalb einer Webinar-Lösung ist nicht zulässig. Außerhalb von Lehrveranstaltungen ist die Aufzeichnung nicht erlaubt.

Folgende weitere Vorgaben sind bei einer Aufzeichnung in Form eines Webinars zu beachten:

a. Fragen nur über Chat- und Q&A-Funktion

Studierende sowie Teilnehmerinnen und Teilnehmer sind vorab in der Mail, welche die Einladungsdaten für die Veranstaltung beinhaltet, darauf hinzuweisen, dass eine Wortmeldung nicht möglich ist und das Fragen nur über die Chat- und Q&A-Funktion von Zoom gestellt bzw. beantwortet werden können. Der Chat wird nicht aufgezeichnet.

b. Belehrung von Teilnehmerinnen und Teilnehmern an hybrider Präsenzveranstaltung

Soweit neben den Vortragenden noch weitere Personen – etwa Studierende – an der Veranstaltung im Vortragsraum – d. h. in Präsenz – teilnehmen, sind sie vor und zu Beginn der Veranstaltung darauf hinzuweisen, dass Fragen durch die Teilnehmerinnen und Teilnehmer vor Ort ausschließlich über die Chat- und Q&A-Funktion gestellt werden dürfen und dafür das Einloggen als Webinar-Teilnehmer bzw. -Teilnehmerin über ein mitgebrachtes mobiles Endgerät erforderlich ist.

c. Keine weiteren Sprecherinnen und Sprecher zulassen

Die Vortragenden und Hosts der Veranstaltung sind nicht berechtigt, weiteren Personen die Rolle „Diskussionsteilnehmer“ zu geben, wenn diese Person nicht Vortragende bzw. Vortragender ist.

d. Einstellung des Webinars

Die Beantragung der Webinarnutzung erfolgt unter folgendem Link: https://uhh.de/zoom-webinar. Der Host meldet sich anschließend unter https://uni-hamburg.zoom.us an und wählt die Funktion Webinar im Bereich „Persönliches“ aus. Es sind anschließend die grundlegenden Parameter einzutragen, welche auch bereits als Veranstaltungsdaten im SharePoint angemeldet wurden.

Die Funktion „Registrierung“ darf nicht aktiviert werden. Es ist ein Webinar-Code zu verwenden und unter „Webinar Optionen“ die Option „Fragen und Antworten“ auszuwählen. Soweit sich ein Teilnehmer oder eine Teilnehmerin über ein mobiles Endgerät einloggen will, wird derzeit von Zoom ein Name und eine E-Mail-Adresse abgefragt. Dies kann derzeit nicht ausgestellt werden. **Den Teilnehmerinnen und Teilnehmern ist im Rahmen der Einladung sowie in den Hinweisen auf der Website des Rechenzentrums zur Nutzung von Zoom mit einem mobilen Endgerät mitzuteilen, dass hier ein beliebiger Name und als E-Mail-Adresse „a@b.de“ angegeben werden kann.** Sobald dieses Problem von Seiten von Zoom abgestellt wurde, wird die Abfrage nicht mehr erfolgen.

Es wird dann eine E-Mail an die Teilnehmerinnen und Teilnehmer versendet, in der die Einladung folgt. Es ist, wie oben beschrieben, darauf hinzuweisen, dass Online-Teilnehmerinnen und -Teilnehmer Fragen nur per Chat- bzw. Q&A-Funktion stellen können. Soweit neben den Vortragenden noch weitere Personen – etwa Studierende – an der Veranstaltung im Vortragsraum – d. h. in Präsenz – teilnehmen, ist, wie oben beschrieben, darauf hinzuweisen, dass Präsenz-Teilnehmer und -Teilnehmerinnen Fragen nur per Chat- bzw. Q&A-Funktion stellen dürfen und dafür das Einloggen als Webinar-Teilnehmer bzw. -Teilnehmerin über ein mitgebrachtes mobiles Endgerät erforderlich ist.

4. Löschung von Protokollen, Chatverläufen und Co.

Nach einer Veranstaltung werden die Chatverläufe und Protokolle einer Veranstaltung automatisch gelöscht. In einer Präsenzveranstaltung gibt es solche Protokolle nicht, weshalb dies keine Einschränkung darstellt. Zur Sicherung des Datenschutzes ist die Löschung zwingend.

5. Abschalten der Videofunktion für Teilnehmerinnen und Teilnehmer

Bei den verwendeten Systemen kann grundsätzlich jeder Teilnehmer und jede Teilnehmerin für sich entscheiden, ob er/sie ein Bild und/oder Ton sendet oder nicht. Dies gilt nicht, wenn der Zweck des Meetings zwingend das Einschalten von Bild und/oder Ton erfordert (bspw. bei Online-Prüfungen, Personalauswahlgesprächen).

Wenn für das jeweilige Nutzungsszenario keine Notwendigkeit besteht, dass Teilnehmerinnen und Teilnehmer mit Bild anwesend sind, sollen die Teilnehmerinnen und Teilnehmer zu Beginn darauf hingewiesen werden, dass die Kamera des eigenen Endgerätes abgeschaltet werden bzw. bleiben kann. Dies ist aus datenschutzrechtlicher Sicht, aber auch zur Minderung der verwendeten Bandbreite, für die Veranstaltung sinnvoll.

6. Namen der Teilnehmerinnen und Teilnehmer

Zoom bietet die Möglichkeit, bei der Teilnahme an einer Konferenz einfach einen Namen anzugeben, der nicht der Klarname sein muss. Da diese Daten an Zoom übersandt werden, dürfen Teilnehmerinnen und Teilnehmer nicht zur Nennung des Klarnamens angehalten werden. Vielmehr soll, sofern die Angabe des Klarnamens nicht notwendig ist, mit einem Pseudonym, z. B. der Matrikelnummer der Studierenden oder Leitzeichen der Beschäftigten, gearbeitet werden.

7. Authentifizierung von Teilnehmerinnen und Teilnehmern bei Online-Prüfungen

Ist bei Online-Prüfungen eine Authentifizierung von Teilnehmerinnen und Teilnehmern erforderlich, haben sich diese durch Vorzeigen eines amtlichen Lichtbildausweises (z. B. Personalausweis) zu authentifizieren. Bei mehreren zu authentifizierenden Personen hat die Authentifizierung in einem gesonderten Besprechungsraum (Breakout-Raum) einzeln zu erfolgen.

8. Teilen des Bildschirms

Der Host einer Veranstaltung ist in der Lage, einzelne Fenster seines Bildschirms mit allen Teilnehmerinnen und Teilnehmern zu teilen und damit Inhalte seines PCs preiszugeben. Hierbei

hat der/die Teilende darauf zu achten, dass dabei keine personenbezogenen Daten Dritter zu sehen sind. Empfohlen wird, nur das Fenster der zur gemeinsamen Betrachtung vorgesehenen Applikation (z. B. PowerPoint) zu teilen. Die Preisgabe von personenbezogenen Daten Dritter (z. B. durch das geöffnete E-Mail-Postfach) muss vom jeweiligen Meeting-Teilnehmer bzw. der Meeting-Teilnehmerin ausgeschlossen werden.

9. Stummschalten der übrigen Teilnehmerinnen und Teilnehmer

Der Host einer Veranstaltung ist in der Lage, die Mikrofone der Teilnehmerinnen und Teilnehmer stumm zu schalten. Dies ist sinnvoll, um eine Geräuschkulisse zu verhindern und zudem schützt es Teilnehmerinnen und Teilnehmer vor der zufälligen Preisgabe personenbezogener Daten Dritter. Deshalb sollte der Host hiervon regelmäßig Gebrauch machen.

Univ.-Prof. Dr. Dr. h.c. Dieter Lenzen
Hamburg, den 30.07.2021