Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

Dienstanweisung zur Nutzung des Videokonferenzsystems Zoom vom 19.06.2020

Die Durchführung digitaler Veranstaltungen und Besprechungen ist im Rahmen der Corona-Pandemie notwendig und unerlässlich geworden. Das Ziel muss es sein, 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 hat in den vergangenen Wochen 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. Nur so kann sichergestellt werden, dass die Kommunikation über Server erfolgt, die in der Universität im RRZ betrieben und 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 Kolle-

gen 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. **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 Teilnehmerzahl in der Form zu begrenzen, dass nur Personen den Veranstaltungen beiwohnen können, die auch tatsächlich eingeladen wurden. Das bedeutet, dass ein Passwort mit der Einladung zu versenden ist, um zu gewährleisten, dass nur berechtigte Personen teilnehmen.

   Die Teilnehmenden 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 Teilnehmer, was von Seiten der Universität zwingend zu verhindern ist.

3. **Verbot der Aufzeichnung einer Veranstaltung, Vorlesung oder Videokonferenz**

   Die Aufzeichnung einer Veranstaltung, Vorlesung oder sonstiger Videokonferenz ist untersagt.

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 Teilnehmer**

   Bei den verwendeten Systemen kann jeder Teilnehmer für sich entscheiden, ob er ein

Bild oder Ton sendet oder nicht. Wenn für das jeweilige Nutzungsszenario keine Notwendigkeit besteht, dass Teilnehmer mit Bild anwesend sind, sollen die 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 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 Teilnehmer nicht zur Nennung des Klarnamens angehalten werden. Vielmehr soll, sofern eine Identitätsfeststellung notwendig ist, mit einem Pseudonym, z. B. der Matrikelnummer der Studierenden oder Leitzeichen der Beschäftigten gearbeitet werden.

7. **Teilen des Bildschirms**

   Der Host einer Veranstaltung ist in der Lage, seinen Bildschirm mit allen Teilnehmern zu teilen und damit Inhalte seines PCs preiszugeben. Hierbei hat der Teilende darauf zu achten, dass auf dem geteilten Bildschirm keine personenbezogenen Daten Dritter zu sehen sind. Sinnvoll ist es, auf dem geteilten Bildschirm nur die beabsichtigte Präsentation zu öffnen und alle anderen Fenster zu schließen oder auf einem weiteren Bildschirm zu öffnen. Gegebenenfalls sollte die Freigabe auf einzelne Fenster beschränkt werden. Die Preisgabe von personenbezogenen Daten Dritter (z. B. durch das geöffnete E-Mail-Postfach) ist auszuschließen!

8. **Stummschalten der übrigen Teilnehmer**

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

9. **Einladung**

   Im Rahmen der Einladung sind die Teilnehmer einer Konferenz auf die Möglichkeit der pseudonymisierten Teilnahme hinzuweisen.

Univ.-Prof. Dr. Dr. h.c. Dieter Lenzen

Hamburg, den 19.06.2020