

SMT-Regelung zur Nutzung des Zoom-Diensts an der Goethe-Universität Frankfurt (Stand Juni 2021)

Diese Regelung gilt für alle Angehörigen der Goethe-Universität Frankfurt. Sie regelt die Nutzung des Zoom-Diensts. Ordnungen und Satzungen der Goethe-Universität, insbesondere die IT-Sicherheitsordnung, IT-Sicherheitsrichtlinie und die IuK-Nutzungsordnung¹, werden durch diese Regelung nicht berührt.

Aufgrund der Corona-Krise hat die Goethe-Universität Zoom-Lizenzen angeschafft, um die Lehre auch Online durchführen zu können. Der Videodienst Zoom ist ein weltweit verbreitetes Tool für virtuelle Konferenzen und online Meetings. Der Cloud-Dienst unterstützt dabei unterschiedliche Nutzungsszenarien – von virtueller Teamarbeit über Online-Präsentationen bis zu Online-Lehrveranstaltungen.

Zur Nutzung des Zoom-Diensts sind folgende Regeln des Sicherheits-Management-Teams (SMT) der Goethe-Universität zu beachten:

- 1) Aus Vertraulichkeitsgründen und aus datenschutzrechtlichen Gründen darf der Dienst Zoom **ausschließlich für Lehrzwecke** (Online-Präsentationen, Online-Lehrveranstaltungen usw.) eingesetzt werden.
- 2) Für vertrauliche Gespräche bzw. vertrauliche Video-Konferenzen ist Zoom **nicht geeignet**. Zoom **darf nicht** für Gremiensitzungen, Gruppenmeetings, Bewerbungen, Berufungen o. Ä. verwendet werden. Für diese Zwecke **sind** die Anwendungen „**Vidyo**“ und „**BigBlueButton (BBB)**“ zu nutzen.
- 3) Die Übertragung von sensiblen persönlichen oder sensiblen geschäftlichen Daten über Zoom **ist untersagt**.
- 4) Der Zugriff auf Zoom Webkonferenzen **muss** durch eine der folgenden Schutzvorkehrungen abgesichert werden: PIN, Warteraumfreigabe, geheime Raum-ID.
- 5) Unautorisierte Offenlegung der PINs **ist nicht zulässig**. Die Kommunikation der PINs **muss** per E-Mail oder über andere sichere Wege erfolgen.

¹ Allgemeine Nutzungsordnung für die Informationsverarbeitungs- und Kommunikationsinfrastruktur der Goethe-Universität Frankfurt

- 6) Die ungesicherte Veröffentlichung von Weblinks für Zoom-Konferenzen auf frei zugänglichen Plattformen wie Twitter, Facebook, etc. ist **nicht erlaubt**. Sollte eine Kommunikation auf einer frei zugänglichen Plattform notwendig sein, ist dies im Vorfeld vom SMT zu genehmigen.
- 7) Soweit möglich **sollen** alle möglichen Tracking- bzw. Überwachungsoptionen von Webkonferenzen deaktiviert werden.
- 8) Die Authentisierung über Google und Facebook **ist nicht** erlaubt und **darf nicht** genutzt werden.
- 9) Zur Aufzeichnung einer Vorlesung **muss** die explizite Einwilligung (mindestens in Textform) aller Personen, von denen personenbezogene Daten verarbeitet werden sollen, eingeholt werden. Personenbezogene Daten sind hier neben Bild- auch Tonaufnahmen, Beiträge und Nennung des Namens im Chat usw. Die Einwilligung muss freiwillig im Sinne Art. 6 Abs. 1 lit. a, Art. 4 Nr. 11 und Art. 7 DSGVO erfolgen.

Bitte wählen Sie auf Basis der voraussichtlichen Gesprächsinhalte den geeigneten Videokonferenzdienst. Die im Folgenden beschriebenen Nutzungsszenarien können Ihnen dabei helfen.

Typische Nutzungsszenarien	Zu nutzenden Dienste
Lehrveranstaltungen / Lerngruppen, Wissenschaftliche Vorträge / Wissenschaftliche Konferenzen oder Tagungen.	Zoom BigBlueButton (BBB)
Besprechungen (Gremiensitzungen, Dienstbesprechungen etc.) / Berufungen (Vortrag, Kommissionssitzung etc.) / Interviews mit Probanden / Prüfungen / Bewerbungsgespräche	Vidyo BigBlueButton (BBB)

Soweit es organisatorisch nicht anders möglich ist, können Sie trotz dieser Regelungen an externen Videokonferenzen teilnehmen, zu denen Sie von anderen Universitäten, Forschungseinrichtungen oder externen Unternehmen über Zoom, Cisco Webex, Microsoft Teams, Skype for Business usw. eingeladen wurden. In diesem Fall gelten folgende Voraussetzungen:

- Die Videokonferenz wurde nicht von einem Universitäts-Account der GU (@xxx.uni-frankfurt.de) initiiert.
- Sensible Informationen, die in Artikel 9 der DSGVO aufgeführt sind, dürfen nicht über externe Videokonferenzen kommuniziert bzw. übertragen werden. Dazu gehören personenbezogene Daten über rassische oder ethnische Herkunft, religiöse, politische oder weltanschauliche Überzeugungen, Gesundheitsdaten oder auch Informationen zur sexuellen Orientierung.

Informationsquellen

- Bundesamt für Sicherheit in der Informationstechnik (BSI)
<https://www.bsi.de>
<https://www.bsi-fuer-buerger.de>
- Verein zur Förderung eines Deutschen Forschungsnetzes (DFN-Verein)
<https://www.dfn.de/>
- DFN Computer Emergency Response Team (DFN-CERT)
<https://www.dfn-cert.de>
- IT-Sicherheitsmanagement-Team (SMT) der Goethe-Universität
<https://www.uni-frankfurt.de/smt>
- Goethe-Universität Computer Emergency Response Team (GU-CERT)
<https://www.rz.uni-frankfurt.de/gu-cert>
- Hochschulrechenzentrum (HRZ) der Goethe-Universität
<https://www.hrz.uni-frankfurt.de>
- Vidyo an der Goethe-Universität
https://www.rz.uni-frankfurt.de/50324159/Videokonferenzen_mit_Vidyo
- BigBlueButton an der Goethe-Universität
<https://bbb.uni-frankfurt.de>
- Zoom an Goethe-Universität
<https://zoom.uni-frankfurt.de>