

# Richtlinie für die Bereitstellung und Nutzung des Video-Konferenzsystems Zoom an der Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU)

Von der Universitätsleitung verabschiedet am 7. April 2021

## Inhaltsverzeichnis

- §1. Bereitstellung von Zoom für die FAU**
- §2. Zulässige und unzulässige Nutzungen**
- §3. Daten-Schutzbedarf und Zoom-Betriebsart**
- §4. Nutzungspflicht**
- §5. Zentrale Systemeinstellungen**
- §6. Verantwortlichkeit für die übermittelten Inhalte**
- §7. Verhaltensregeln**
- §8. Aufzeichnungen und Speicherung von Aufzeichnungen**
- §9. Weitere Regelungen**
- §10. Geltungsdauer**

Die Universitätsleitung wird allen Lehrenden, Forschenden, Studierenden sowie den wissenschaftsunterstützenden Beschäftigten zur Überbrückung von Engpässen im Zusammenhang mit der SARS-CoV-2-Pandemie neben den bereits bisher genutzten beiden Video-Konferenzsystemen [DFNConf](#) und [Jitsi Meet](#) sowohl für das Sommersemester 2021 als auch das Wintersemester 2021/22 weiterhin Lizenzen für die Nutzung des Video-Konferenzsystems Zoom der Firma Zoom Video Communications, Inc. zur Verfügung stellen. Sie hat sich zu diesem Schritt entschlossen, weil die beiden genannten und auch weitere derzeit in der Erprobung stehende Video-Konferenzsysteme nicht die technische Leistungsfähigkeit und Skalierbarkeit von Zoom besitzen, die in der aktuellen Situation für einen funktionsfähigen digitalen Universitätsbetrieb erforderlich sind. In der Anfangsphase der globalen Nutzung von Zoom im vergangenen Jahr aufgedeckte Sicherheitslücken hat die Fa. Zoom Video Communications, Inc. inzwischen beseitigt und u.a. mit dem Instrument der Ende-zu-Ende-Verschlüsselung (E2EE) auch selbst einen neuen wirksamen Schutz für die via Zoom transportierten Inhalte geschaffen.<sup>1</sup> Bestehenden datenschutzrechtlichen Bedenken, die sich vor allem aus der auf der europäischen Ebene nach wie vor ungeklärten Situation von IT-Lösungen von Anbietern aus Drittstaaten ergeben, kann die Universität selbst naturgemäß nur insofern

---

<sup>1</sup> "In einem typischen Meeting generiert die Zoom-Cloud die Encryption Keys und verteilt sie mit Hilfe der Zoom-Apps an die Teilnehmer, sobald sie beitreten. Bei E2EE generiert der Gastgeber die Schlüssel und verteilt diese mithilfe von Public-Key-Kryptographie an die anderen Meeting-Teilnehmer. Die Server von Zoom werden zu „blinden“ Relays (Oblivious Relays) und haben keinerlei Zugriff auf die Schlüssel, die zum Entschlüsseln der Meeting-Inhalte erforderlich sind", vgl. <https://blog.zoom.us/de/zoom-rolling-out-end-to-end-encryption-offering/> .

entgegenwirken, als sie durch eigene organisatorische und technische Instrumente für einen möglichst sicheren und datensparsamen Systembetrieb und in diesem Sinne ebenso strikte Vorgaben für einzelne Nutzungsszenarien Sorge trägt. Diesem Ziel dient diese Richtlinie.

## §1. Bereitstellung von Zoom für die FAU

- (1) Die Bereitstellung von Zoom zur Erledigung der universitären Aufgaben in Forschung, Lehre, Studium, Weiterbildung und Verwaltung findet ausschließlich über die hierfür getroffenen vertraglichen Vereinbarungen zwischen der FAU und der Firma Zoom Video Communications, Inc. und den vom RRZE unter <https://fau.zoom.us> geschaffenen technischen Zugangswegen statt.
- (2) Die Nutzung freier Lizenzen der Fa. Zoom Video Communications, Inc. oder von Lizenzen aufgrund anderer vertraglicher Vereinbarungen mit der Fa. Zoom Video Communications, Inc. selbst oder deren Vertragspartnern für die Hochschulaufgaben in Forschung, Lehre, Studium, Weiterbildung und Verwaltung ist untersagt.
- (3) Systembetreiber von Zoom für die FAU nach § 5 IT-R<sup>2</sup> ist das RRZE. Datenschutzrechtlich Verantwortlicher ist die FAU vertreten durch den Präsidenten.<sup>3</sup>

## §2. Zulässige und unzulässige Nutzungen

- (1) Zulässig ist die Nutzung von Zoom insbesondere für folgende Szenarien: Online-Lehrveranstaltungen, Online-Prüfungen, Arbeit in Lerngruppen, Vorträge, Konferenzen und Tagungen, Berufungen (Vorträge, Kommissionssitzungen), Besprechungen (Gremiensitzungen, Dienstbesprechungen), Bewerbungs- und Beratungsgespräche.
- (2) Unzulässig ist die Nutzung für medizinisch-therapeutische Zwecke sowie private Nutzung, wenn diese über geringfügigen Umfang hinaus oder in kommerziellem Zusammenhang erfolgt.

## §3. Daten-Schutzbedarf und Zoom-Betriebsart<sup>4</sup>

- (1) Die jeweilige Betriebsart von Zoom (Standard-Modus in der Zoom-Cloud ohne aktivierte Ende-zu-Ende-Verschlüsselung oder Verschlüsselungsmodus mit aktivierter und überprüfter Verschlüsselung<sup>5</sup> in der Zoom-Cloud) richtet sich nach dem Schutzbedarf der von den Teilnehmerinnen und Teilnehmern ausgetauschten Daten (normal/hoch/sehr hoch).

---

<sup>2</sup> Richtlinie für die Bereitstellung und Nutzung von Systemen und Verfahren der Informationstechnologie an der Friedrich-Alexander-Universität Erlangen-Nürnberg (IT-R) vom 25.11.2020,

<https://www.rrze.fau.de/infocenter/rahmenbedingungen/richtlinien/benutzungsrichtlinien/> .

<sup>3</sup> <https://www.anleitungen.rrze.fau.de/multimedia/videokonferenzen/zoom/datenschutz-und-barrierefreiheit/> .

<sup>4</sup> Die nachstehende Klassifikation und die Anlage sind im Wesentlichen der Richtlinie für die Nutzung von Videokonferenzen der Stabsstelle Datenschutz und Informationssicherheit der Universität Bielefeld vom 14.12.2020 entnommen. Die Richtlinie der Universität Bielefeld ist vollständig wiedergegeben unter [https://www.uni-bielefeld.de/verwaltung/informationssicherheit/beschaeftigte/videokonferenzen/2020-12-14\\_Datenklassifizierung\\_Videokonferenzen.pdf](https://www.uni-bielefeld.de/verwaltung/informationssicherheit/beschaeftigte/videokonferenzen/2020-12-14_Datenklassifizierung_Videokonferenzen.pdf) .

<sup>5</sup> Durch die aktivierte Ende-zu-Ende-Verschlüsselung sind folgende Funktionen nicht verfügbar: Breakout Rooms, Umfragen, Teilnahme im Browser, Telefon-Einwahl. Wenn eine Ende-zu-Ende-Verschlüsselung der Inhaltsübermittlung in der Zoom-Cloud aufgrund dieser Beschränkungen nicht in Frage kommt, kann auf Jitsi Meet und den unverschlüsselten Betrieb von Zoom mittels Zoom On-Premise (konfigurierbar über das IdM-Portal der FAU) bzw. auf DFNconf ausgewichen werden, da in

- (2) Zu den Daten mit hohem und sehr hohem Schutzbedarf zählen dabei alle in Art. 9 der Datenschutz-Grundverordnung (DSGVO) aufgeführten Datenkategorien (Daten, aus denen die ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, genetische und biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person), Personalaktendaten sowie Daten, die einer dienstlichen oder vertraglichen Geheimhaltung und/oder bei Bekanntwerden Vertragsstrafen unterliegen.
- (3) Ist davon auszugehen, dass in einem Nutzungsszenarium über Zoom Daten nach Nr. §3 (2). ausgetauscht werden, ist deshalb der Betrieb stets nur mit aktivierter und überprüfter Ende-zu-Ende-Verschlüsselung durchzuführen.<sup>6</sup> Für einzelne ausgewählte Nutzungsszenarien richtet sich die Betriebsart nach den in der Anlage zu dieser Richtlinie genannten Vorgaben.

#### §4. Nutzungspflicht

- (1) Soweit die technischen Voraussetzungen gegeben sind, ist die Nutzung von Zoom vorbehaltlich Nr. §4 (2). verpflichtend
  - für Studierende bei Lehrveranstaltungen und bei elektronischen Fernprüfungen, die auf der Grundlage der Bayerischen Fernprüfungsverordnung<sup>7</sup> und der Satzung der FAU über die Durchführung elektronischer Fernprüfungen<sup>8</sup> sowie den in diesem Zusammenhang geltenden Datenschutzbestimmungen<sup>9</sup> abgehalten werden, sowie bei der Einsicht in Prüfungsunterlagen,
  - für Beschäftigte im Rahmen der Aufgaben und Tätigkeiten ihres Beschäftigungsverhältnisses.
- (2) Veranstalter und Veranstalterinnen können im Rahmen ihrer verantwortlichen Aufgabenwahrnehmung daneben auch andere Video-Konferenzsysteme verwenden, sofern diese das für das jeweilige Nutzungsszenarium nach der Anlage zu Nr. §3 (3) erforderliche datenschutzrechtliche Sicherheitsniveau gewährleisten.<sup>10</sup>
- (3) Zum Schutz personenbezogener Daten gegenüber der Fa. Zoom Video Communications, Inc. kann sowohl von den Studierenden als auch von den Beschäftigten von der im IdM-Portal der FAU implementierten Zoom-Pseudonymisierung<sup>11</sup> Gebrauch gemacht werden.

---

diesen Fällen der Betrieb entweder durch das RRZE selbst (Jitsi Meet, Zoom On-Premise) oder in Deutschland (DNConf) erfolgt und insoweit in allen diesen Fällen zumindest dem in Deutschland geltenden Datenschutzrecht unterliegt.

<sup>6</sup> Das Vorgehen zur Einschaltung des Verschlüsselungsmodus ist beschrieben unter <https://www.anleitungen.rrze.fau.de/multimedia/videokonferenzen/zoom/faq/>.

<sup>7</sup> Verordnung zur Erprobung elektronischer Fernprüfungen an den Hochschulen in Bayern (Bayerische Fernprüfungsverordnung – BayFEV) v. 16. September 2020 (GVBl. S. 570).

<sup>8</sup> Satzung der Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU) über die Durchführung elektronischer Fernprüfungen auf Grundlage der Bayerischen Fernprüfungserprobungsverordnung (BayFEV)-EFernPO-vom 2. Dezember 2020, [https://www.doc.zuv.fau.de/L1/Regelungen\\_zum\\_Studium/EFernPO/](https://www.doc.zuv.fau.de/L1/Regelungen_zum_Studium/EFernPO/).

<sup>9</sup> Informationsblatt zur Datenverarbeitung im Rahmen der Teilnahme an elektronischen Fernprüfungen auf Grundlage der EFernPO i.V.m. BayFEV,

[https://www.doc.zuv.fau.de/L1/Regelungen\\_zum\\_Studium/EFernPO/Information\\_zur\\_Datenverarbeitung/Informationsblatt\\_zur\\_Datenverarbeitung\\_im\\_Rahmen\\_der\\_Teilnahme\\_an\\_elektronischen\\_Fernpruefungen\\_20210112.pdf](https://www.doc.zuv.fau.de/L1/Regelungen_zum_Studium/EFernPO/Information_zur_Datenverarbeitung/Informationsblatt_zur_Datenverarbeitung_im_Rahmen_der_Teilnahme_an_elektronischen_Fernpruefungen_20210112.pdf).

<sup>10</sup> Ist danach eine Ende-zu-Ende-Verschlüsselung erforderlich, so kann dies nach dem gegenwärtigen Stand der Technik jedoch nur durch das System Jitsi Meet, nicht aber durch DNConf erfolgen.

<sup>11</sup> Durch die Pseudonymisierung werden nur noch der Lizenztyp und eine persistente pseudonyme ID an im Auftrag der Fa. Zoom Video Communications, Inc. betriebene Server übertragen, nicht wie ohne Pseudonymisierung Vorname, Nachname und E-Mail-Adresse.

## §5. Zentrale Systemeinstellungen

Das RRZE ist als Systembetreiber verpflichtet und berechtigt, die technischen Zugangswege und globalen Systemeinstellungen von Zoom so anzupassen, dass dem Schutz der Daten der Nutzerinnen und Nutzer sowie der Sicherheit des IT-Betriebs in der nach den jeweiligen Gegebenheiten (Releases etc.) umfassend möglichen Weise Rechnung getragen wird. Hierzu zählen insbesondere Deaktivierung/Einschränkung von Optionen, die für den Betrieb nicht notwendig sind, Deaktivierung der Zoom-Cloud-Speicherfunktion (soweit möglich), Authentifizierung durch FAU-eigenes WebSSO, Bereitstellung einer Pseudonymisierungsfunktion, Begrenzung von Zugriffsrechten.

## §6. Verantwortlichkeit für die übermittelten Inhalte

- (1) Verantwortlich für die über Zoom übermittelten Inhalte sind die jeweiligen Veranstalter und Veranstalterinnen (universitäre Einrichtungen und deren Beschäftigte, Studierende).
- (2) Es ist verboten, Daten und Inhalte (auch Links) zur Verfügung zu stellen, die rechtlichen Grund-sätzen widersprechen.
- (3) Die Nutzung von durch das Urheberrechtsgesetz geschützten Inhalten darf ohne Zustimmung der Rechteinhaberin bzw. des Rechteinhabers nur in den gesetzlich vorgesehenen Fällen erfolgen.
- (4) Personenbezogene und personenbeziehbare Informationen über die Nutzerinnen und Nutzer dürfen außerhalb des jeweiligen Nutzungsszenarios nur mit deren ausdrücklicher Genehmigung verwendet werden.
- (5) Auf die Nutzungsverpflichtungen für die Inanspruchnahme der IT-Systeme und Verfahren der FAU nach § 4 IT-R wird verwiesen.

## §7. Verhaltensregeln

- (1) Die Veranstalter und Veranstalterinnen können Hinweise und Nutzungsregeln festlegen, die die Grundsätze des Verhaltens während der Veranstaltung regeln, die Teilnehmerinnen und Teilnehmer zur Einhaltung der Nutzungsregeln anhalten und diese bei wiederholter Nichtbefolgung derselben von der Veranstaltung ausschließen.
- (2) Teilnehmerinnen und Teilnehmer sind nicht zum Einsatz bestimmter Funktionen von Zoom (insbesondere des Mikrofons, der Webcam oder der Chatfunktion) verpflichtet. Ausnahmen hiervon sind nur bei Vorliegen einer rechtlichen Grundlage möglich.

## §8. Aufzeichnungen und Speicherung von Aufzeichnungen

- (1) Die Aufzeichnung von Inhalten (Video, Audio, Chat) von Veranstaltungen, auch in Teilen, darf nur insoweit erfolgen, als dies für die jeweilige konkrete Erledigung der universitären Aufgaben in Forschung, Lehre, Studium, Weiterbildung und Verwaltung erforderlich ist. Hierunter fallen zum Beispiel Vorlesungsaufzeichnungen zum Nachhören oder für verhinderte Teilnehmerinnen und Teilnehmer.
- (2) Die Teilnehmerinnen und Teilnehmer sind vor Beginn einer Veranstaltung durch einen schriftlichen Hinweis über eine geplante Aufzeichnung aufzuklären. Sie ist ihnen während der Aufzeichnung durch den Veranstalter bzw. die Veranstalterin kenntlich zu machen. Eine

ausdrückliche Zustimmung zur Aufzeichnung ist in den Fällen nach Nr. §8 (1). nicht erforderlich. Im Rahmen der Aufklärung ist den Teilnehmerinnen und Teilnehmern zu eröffnen, dass sie, wenn sie mit einer Aufzeichnung nicht einverstanden sind, nicht an der Veranstaltung teilnehmen sollen, sondern diese nachträglich im jeweiligen Online-Portal anschauen („streamen“) können. In diesem Zusammenhang wird klargestellt, dass die Teilnehmerinnen und Teilnehmer nicht verpflichtet sind, weder ausdrücklich noch stillschweigend, ihre Zustimmung zur Aufzeichnung zu erteilen. Nachteile dürfen diesen durch ihre Nichterteilung der Zustimmung zur Aufzeichnung nicht entstehen. Abweichend von Satz 3 dieser Nr. §8 (2) ist die ausdrückliche Zustimmung der Teilnehmerinnen und Teilnehmer einzuholen, wenn die jeweilige Veranstaltung deren aktive mündliche Teilnahme an der derselben (z.B. Seminarvortrag, mündliche Prüfung) zwingend vorsieht.

#### §9. Weitere Regelungen

- (1) Auf den Betrieb von Zoom an der FAU finden neben den Bestimmungen der IT-R die Bestimmungen der IT-Rahmendienstvereinbarung (IT-RDV)<sup>12</sup> uneingeschränkte Anwendung.
- (2) Insbesondere findet auf der Basis der Nutzung von Zoom keine vergleichende Leistungs- und Verhaltenskontrolle statt und es werden keine personenbezogenen Statistiken erstellt.

#### §10. Geltungsdauer

Diese Richtlinie gilt zunächst bis zum 31.03.2022. Sie wird fortgeschrieben, wenn die FAU darüber hinaus nach den dann geltenden Bedingungen weiterhin Zoom-Lizenzen in Anspruch nimmt.

Erlangen, den 12. April 2021

Prof. Dr.-Ing. Joachim Hornegger  
Präsident

---

<sup>12</sup> Rahmen-Dienstvereinbarung über die Einführung, Anwendung und erhebliche Änderung von Systemen und Verfahren der Informationstechnologie an der Friedrich-Alexander-Universität Erlangen-Nürnberg (IT-RDV) vom 02.10.2020, <https://www.rrze.fau.de/infocenter/rahmenbedingungen/richtlinien/it-rdv/>.

**Anlage zu Nr. §3 (3): Daten-Schutzbedarf und Zoom-Betriebsart**

<b>Nutzungsszenarium</b>	<b>Schutzbedarf</b>	<b>Betriebsart</b>
Lehrveranstaltungen	Normal	Standard-Modus
Lerngruppen	Normal	Standard-Modus
Vorträge, Konferenzen und Tagungen	Normal	Standard-Modus
Berufungen a) Vorträge  b) Sitzungen der Kommissionen	a) Normal (ein Berufungsvortrag ist im Allgemeinen öffentlich und hat keine besonderen Vertraulichkeitsanforderungen) b) Hoch (die Sitzungen der Berufungskommissionen können durchaus hohe Anforderungen an die Vertraulichkeit stellen)	a) Standard-Modus  b) Ende-zu-Ende-Verschlüsselung
Fernprüfungen (nach BayFEV i.V.m. EFernPO) <sup>13</sup> , Einsicht in Prüfungsunterlagen	Sehr hoch	Ende-zu-Ende-Verschlüsselung
Besprechungen (Gremiensitzungen, Dienstbesprechungen) a) Austausch von Informationen bspw. über Abläufe, Änderungen von Zuständigkeiten etc. b) Informationen bspw. zur inhaltlichen, personellen oder finanziellen Ausrichtung	a) Normal b) Hoch	a) Standard-Modus b) Ende-zu-Ende-Verschlüsselung
Bewerbungsgespräche (beispielsweise mit potentiell zukünftigen Beschäftigten der FAU)	Hoch	Ende-zu-Ende-Verschlüsselung
Beratungsgespräche (Sprechstunden) a) Beratung von Studierenden und Absolventen/-innen b) Psychosoziale Beratung von Studierenden beispielsweise in besonderen Belastungssituationen	a) Hoch b) Sehr hoch	a) Ende-zu-Ende-Verschlüsselung b) Ende-zu-Ende-Verschlüsselung
Interviews mit Probanden a) Fragen bzw. potentielle Antworten der Probandinnen und Probanden berühren keine sensiblen oder vertraulichen Bereiche b) Fragen bzw. potentielle Antworten der Probandinnen und Probanden berühren sensible oder vertrauliche Bereiche	a) Hoch b) Sehr hoch	a) Ende-zu-Ende-Verschlüsselung b) Ende-zu-Ende-Verschlüsselung
Austausch zu Forschungsfragen, die z. B. einer vertraglichen Geheimhaltung und/oder Vertragsstrafen unterliegen	Sehr hoch	Ende-zu-Ende-Verschlüsselung
Austausch von Gesundheitsdaten, Daten über die ethnische Herkunft, über religiöse, politische oder weltanschauliche Überzeugungen oder auch von Informationen zur sexuellen Orientierung (Artikel 9 DSGVO), Personalaktendaten oder	Sehr hoch	Ende-zu-Ende-Verschlüsselung

<sup>13</sup> Siehe hierzu auch die Handreichung der FAU zu Prüfungskonzepten im Wintersemester 2020/2021, [https://www.fau.de/files/\\_protected/2020/12/201116\\_pruefungskonzept-handreichung.pdf](https://www.fau.de/files/_protected/2020/12/201116_pruefungskonzept-handreichung.pdf).

anderen Daten, für die eine dienstliche oder vertragliche Verschwiegenheit besteht		
--	--	--