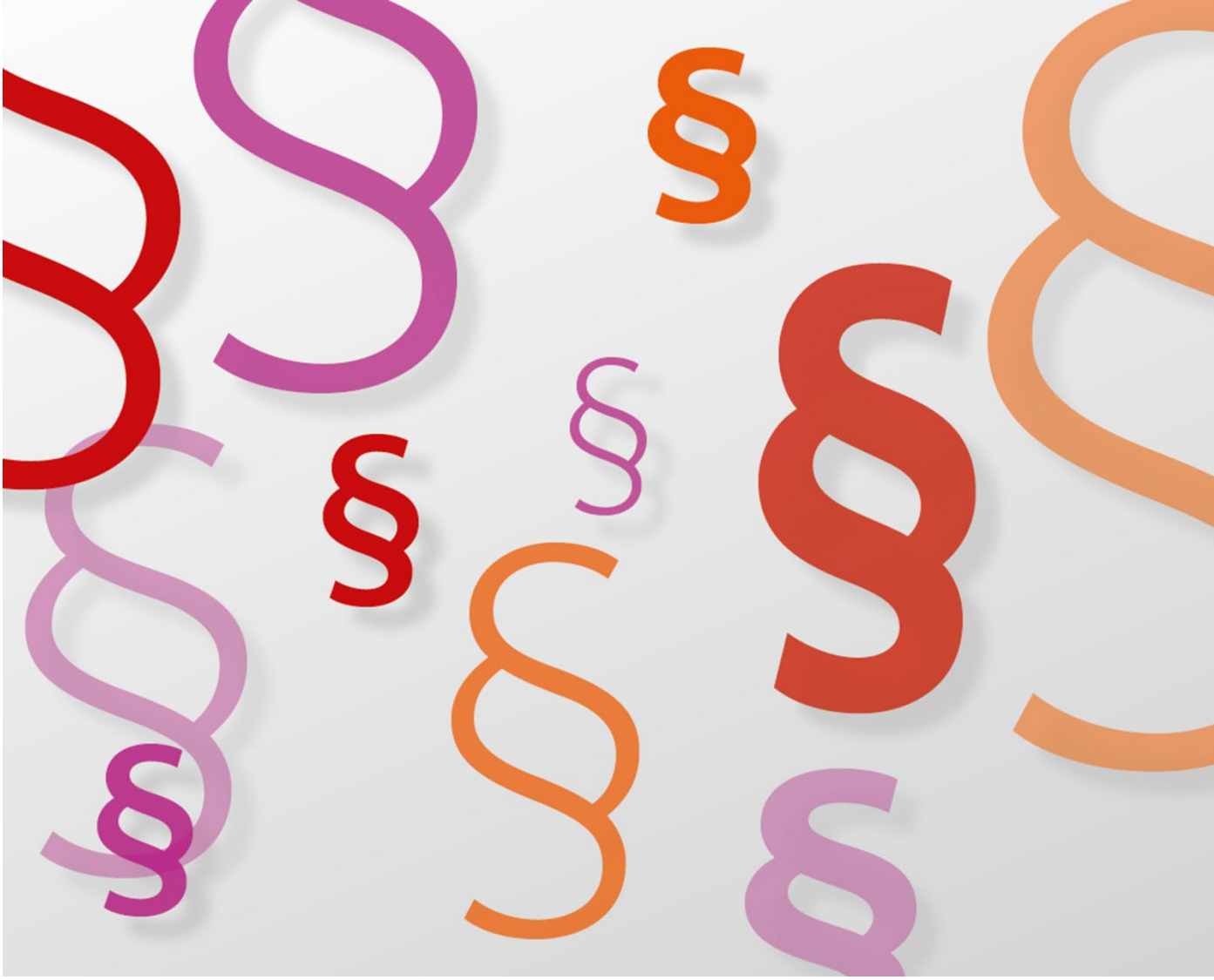

Amtliche Mitteilung Nr. 66/2021

Nutzungsempfehlungen für Videokonferenzlösungen

Vom 17. November 2021

Herausgegeben am 3. Dezember 2021

Technology
Arts Sciences
TH Köln

Nutzungsempfehlungen für Videokonferenzlösungen

Stand: 17. November 2021

Technology
Arts Sciences
TH Köln

Präambel

Die Technische Hochschule Köln hat sich im Rahmen der Bewältigung der aktuellen SARS-CoV-2-Pandemie für einen – zunächst befristeten – Einsatz von Videokonferenzlösungen entschieden, um den Hochschulbetrieb aufrechterhalten zu können.

Aufgrund von Kapazitäts- und Stabilitätsproblemen des bisher angebotenen Tools „DFNconf“ wurde eine cloudbasierte Videokonferenzlösung bereitgestellt, um den Hochschulbetrieb aufrecht zu erhalten. Hierzu wurde das Angebot mit der cloudbasierten Videokonferenzlösung Zoom und der Kollaborationslösung Microsoft Teams ergänzt. Mit den externen Dienstanbietern wurden Auftragsverarbeitungsverträge sowie sog. Standarddatenschutzklauseln vereinbart, um die datenschutzrechtlichen Anforderungen zu erfüllen.

Durch die Campus IT wurden kritische Funktionalitäten (wie z.B. Aufmerksamkeitsüberwachung) deaktiviert sowie datenschutzfreundliche Grund- und Voreinstellungen (wie z.B. verstärkte Verschlüsselung zwischen den Nutzer*innen, Zugangsschutz mit Einladungslinks und Kenncodes, Vorschaltung eines Warteraums etc.) vorgenommen, um einen datenschutzkonformen Betrieb zu gewährleisten und die Datenverarbeitung möglichst datensparsam auszugestalten.

Durch eine Minimierung der Verarbeitung von personenbezogenen Daten bei der Nutzung der Videokonferenztools auf das erforderliche Maß soll das Recht auf informationelle Selbstbestimmung aller Nutzer*innen bestmöglich geschützt werden. Dies ist nur möglich, wenn die Nutzer*innen selbst durch verantwortungsvollen Handeln zum Schutz der personenbezogenen Daten beitragen.

Diese Nutzungsempfehlungen entstanden aufgrund einer Vielzahl von Einzelanfragen und beantworten im Sinne einer FAQ-Liste typische Nutzungsszenarien der TH Köln.

Bitte beachten Sie, dass die Empfehlungen nur allgemeine Szenarien erfassen und nicht spezifisch auf die Inhalte Ihrer Nutzung eingehen (können).

Nutzungsempfehlungen

Die Nutzung von durch die TH Köln bereitgestellten Videokonferenztools ist datenschutzrechtlich und hochschulrechtlich nicht zu beanstanden, wenn insbesondere folgende Grundsätze beachtet werden:

Auswahl eines geeigneten Videokonferenztools

1. Je nach Nutzungsszenario stehen datenschutzrechtlich unterschiedlich geeignete Videokonferenzlösungen zur Verfügung. Bitte prüfen Sie anhand der Tabellen in der Anlage „Typische Nutzungsszenarien“, welcher Dienst für Ihren Nutzungszweck am besten geeignet ist und welche Voreinstellungen und ggf. zusätzliche Schutzmaßnahmen vorgenommen werden müssen, damit die vorgesehene Nutzung möglichst datensparsam und sicher erfolgt.

2. Nicht alle Dienste sind für den Austausch von personenbezogenen Daten (ggf. mit hohem bzw. sehr hohem Schutzbedarf) oder geheimhaltungsbedürftigen Informationen gleichermaßen geeignet oder bieten hierzu die gleichen Funktionalitäten. Beachten Sie jeweils auch die ggf. im Rahmen Ihrer Projekte vereinbarten Vertraulichkeitsregelungen und Vertragsstrafen sowie die Nutzungsbedingungen der jeweiligen Videokonferenzdienstleister und weisen Sie bitte Ihre Teilnehmer*innen darauf hin. Der Schutzbedarf der Daten bzw. der Kommunikationsinhalte einer Videokonferenz bietet die grundlegende Richtschnur für die Auswahl des Videokonferenzdienstes. Zur Bestimmung des Schutzbedarfs kann im Zweifelsfall die Handreichung „Durchführung einer Schutzbedarfsfeststellung“ herangezogen werden. Diese ist abrufbar unter: https://intern.th-koeln.de/finanzen/datenschutzrecht_967.php

3. Bitte beachten Sie bei der Planung einer rein virtuellen Veranstaltung, Besprechung, Sitzung etc. auch die geltenden hochschulrechtlichen Bestimmungen (Hochschulgesetz NRW, die Rechtsverordnungen der zuständigen Ministerien sowie Ordnungen und Geschäftsordnungen der Hochschule in der jeweils aktuell gültigen Fassung) insbesondere hinsichtlich der Verfahrensgrundsätze (Sitzung in Präsenz, Beteiligung der Hochschulöffentlichkeit etc.). Daneben sind die ggf. davon abweichenden und zeitlich befristeten Rechtsverordnungen zur Bewältigung der SARS-CoV-2-Pandemie zu beachten. Während der Corona-Pandemie dürfen (Stand: September 2021) bspw. gemäß § 82a HG NRW i.V.m. § 5 der Corona-Epidemie-Hochschulverordnung NRW die Sitzungen der Hochschulgremien oder Prüfungen grundsätzlich auch in elektronischer Kommunikation unter Einsatz einer Videokonferenzlösung anstelle einer Präsenzsitzung oder Präsenzprüfung stattfinden.

Vorbereitung einer Videokonferenz

4. <u>Anmeldung mit Ihrer campusID:</u>
   Verwenden Sie als Veranstalter*in einer Videokonferenzsitzung bei dienstlichen Anlässen bitte keine dezentral oder privat beschafften Videokonferenzlösungen. Die zentral bereitgestellten Videokonferenzlösungen der TH Köln unterliegen Auftragsverarbeitungsverträgen und es wurden ergänzende technische Schutzmaßnahmen und eine datenschutzfreundliche Konfiguration umgesetzt. Diese Vereinbarungen und Grund- bzw. Voreinstellungen greifen nur, wenn zur erstmaligen Registrierung und bei der Benutzeranmeldung das Single-Sign-On-Verfahren („SSO“) mit der persönlichen campusID verwendet wird. Ihr persönliches Kennwort wird nicht an den Dienst übertragen. Die Benutzerauthentifizierung und -autorisierung erfolgt über das Identity Management der TH Köln (IDM).

5. <u>Zugriffsschutz bei Videokonferenzen:</u>
   Teilnehmer*innen der Videokonferenzen sollten rechtzeitig (z.B. mit der Einladung, bei Terminabsprache) auf den Einsatz des jeweiligen Videokonferenztools hingewiesen werden. Die zugehörigen Zugangsdaten (Einladungslinks, Meeting-IDs, Zugangskenncodes bzw. -passwörter etc.) dürfen nur dem geschützten und berechtigten Teilnehmer*innenkreis mitgeteilt werden, bspw. im Rahmen einer Anmeldebestätigung.

6. Sollten unberechtigte Dritte Kenntnis von den Zugangsdaten erhalten, ist der Veranstalter verpflichtet, sofortige Schutzmaßnahmen zu ergreifen, z.B. Änderung des Zugangskenncodes bzw. -passwortes, Aktivierung des Warteraums. In der Regel sollten nur zugriffsgeschützte Meetingräume erstellt werden, um eine unberechtigte Teilnahme und Kenntnisnahme Dritter auszuschließen.

7. Bitte nutzen Sie bei der Verwendung von Zoom für jede Veranstaltung bzw. Konferenz die Zoom-Voreinstellung „Meeting-ID: Automatisch erzeugen“ und einen jeweils individuellen Kenncode für den Zugang.
   Nutzen Sie möglichst nicht Ihre persönliche, einzigartige Meeting-ID („PMI“), da diese nur aufwändig geändert werden kann. Mit der Verwendung einer individuellen Meeting-ID verhindern Sie die Teilnahme von unberechtigten Dritten wie Störer*innen, die bspw. Ihre PMI für vorherigen Veranstaltungen oder anderweitig erhalten haben. Sollten Sie dennoch Ihre PMI nutzen wollen, richten Sie bitte einen virtuellen Warteraum ein, um den Zugang steuern bzw. beschränken zu können.

8. Prüfung der Teilnehmer*innen an einer Videokonferenzsitzung:
   Der/die Veranstalter*in („Host bzw. Co-Host“ oder auch Gastgeber*in bzw. Moderator*in) muss eine unberechtigte Teilnahme an einer Sitzung verhindern, bspw. indem die vertraulichen Zugangsdaten vorab nur mit berechtigten Teilnehmer*innen geteilt werden oder neue Teilnehmer*innen erst nach einer erfolgreichen Identifizierung in einem vorgeschalteten Warteraum an der Sitzung teilnehmen können.

9. Es wird empfohlen, den öffentlichen Teil immer von dem vertraulichen Teil einer Videokonferenz technisch abzukoppeln. In diesem Fall können bspw. auch zwei getrennte, virtuelle Besprechungsräume mit den entsprechenden Einladungslinks (und Passwörtern) zum Beitritt eingerichtet werden.

Durchführung einer Videokonferenz

10. Bildschirmübertragungen/-freigaben:
    Bitte achten Sie bei der Übertragung des Bildschirms (-ausschnitts) darauf, dass nicht unbeabsichtigt sensible Daten, etwa durch im Hintergrund geöffnete Anwendungsprogramme wie E-Mail-Client oder andere Desktop-Inhalte bzw. -fenster, übertragen werden.

11. Dateiaustausch und Dateiablage:
    Für den Dateiaustausch und die Dateiablage stehen weiterhin die bekannten, zugriffsgeschützten IT-Dienste der TH Köln zur Verfügung: E-Mail, Dateiserver bzw. Netzlaufwerke und Gruppenverzeichnisse der TH Köln, die Sciebo-Cloud, E-Learning-Plattformen wie ILIAS etc. Sollen sensible personenbezogene Daten über die Videodienste ausgetauscht werden, sind diese Daten zum Schutz vor einem potentiellen Fremdzugriff (etwa durch Einsatz einer Ende-zu-Ende-Verschlüsselung, ein Dokumentenkennwort oder eine verschlüsselte ZIP-Datei etc.) zu verschlüsseln.

12. Besonders schutzbedürftige und vertrauliche Daten (bspw. besondere Kategorien personenbezogener Daten i.S.d. Art. 9 EU-DS-GVO wie Gesundheitsdaten, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Angaben zur Gewerkschaftszugehörigkeit etc.) sollten (wenn überhaupt) anonymisiert oder pseudonymisiert besprochen werden, wenn keine Ende-zu-Ende-Verschlüsselung genutzt werden kann.

13. Aufzeichnungen von Videokonferenzsitzungen:
    Das Aufzeichnen und Speichern von Bild- und Tonübertragungen, Anfertigen von Bildschirmfotos etc. anderer Teilnehmer*innen ist grundsätzlich untersagt, es sei denn, die von der Aufzeichnung betroffenen Personen (Veranstalter*in und/oder Teilnehmer*innen) haben vor Beginn der Aufzeichnung nachweisbar und freiwillig ihr Einverständnis für einen vorab definierten Verarbeitungszweck erteilt. Dazu ist es unabdingbar, dass Sie die Teilnehmenden rechtzeitig vor Beginn der geplanten Aufnahme im Rahmen der Einholung der Einwilligungserklärung transparent über die beabsichtigte Datenverarbeitung (Zweck der Aufnahme, beabsichtigte

Weiterverarbeitung und ggf., ob und wo eine Veröffentlichung erfolgt, Hinweis auf das jederzeitige Widerrufsrecht der Einwilligung etc.) informieren und Gelegenheit bieten, sich der Aufnahme zu entziehen (z.B. durch Verwendung eines angemessenen Alias-Namens sowie Deaktivierung von Kamera und Mikrofon etc.). Für Fragerunden kann die Aufnahme pausiert werden oder parallel der Chat verwendet werden, um diese Inhalte von der Aufnahme auszuschließen. Aufnahmedateien, die in einem Videokonferenzdienst temporär gespeichert werden, sind unverzüglich auf einen Datenspeicher der TH Köln zu übertragen und aus dem jeweiligen Videokonferenzdienst zu löschen. Dies gilt entsprechend, wenn eine andere, lokale Aufnahmesoftware verwendet wird. Bitte bedenken Sie, dass ein unerlaubtes Aufzeichnen oder Mitschneiden von Videokonferenzen strafbar sein kann (vgl. auch § 201 StGB - Verletzung der Vertraulichkeit des Wortes, § 201a - Verletzung des höchstpersönlichen Lebensbereichs und von Persönlichkeitsrechten durch Bildaufnahmen).

14. Datensicherung (Backups) der Inhaltsdaten und übertragenen Dateien:
    Bitte beachten Sie, dass Sie eigenverantwortlich geeignete Maßnahmen gegen den Verlust ihrer dienstlichen Daten ergreifen und ihre Datenablage und -sicherung, außerhalb der genutzten Videokonferenzdienste, auf dienstlichen Speichermedien bzw. -diensten vornehmen.

15. Sicheres Beenden einer Videokonferenzsitzung und Löschen von Meetingräumen:
    Eine Videokonferenzsitzung muss durch den/die Veranstalter*in („Host bzw. Co-Host“) für alle Nutzer*innen beendet werden, damit ein ungewollter Informationsabfluss im Nachgang der Sitzung ausgeschlossen ist. Sofern die virtuellen Meetingräume nicht mehr benötigt werden, sollten diese zeitnah gelöscht werden. Falls erforderlich, sichern Sie bitte rechtzeitig die Meetinginhalte, um einen ungewünschten Datenverlust auszuschließen.

Kontaktdaten für Rückfragen und bei Sicherheitsvorfällen

Bei Verdacht der Gefährdung der IT-Sicherheit, bei IT-Sicherheitsvorfällen oder allgemeinen Fragen zur IT-Sicherheit wenden Sie sich bitte unverzüglich an den Informationssicherheitsbeauftragten der TH Köln und nehmen hierzu Kontakt mit dem Service Desk der Campus IT auf:

Selfservice-Portal:	https://selfservice.th-koeln.de
E-Mail:	support@campusit.th-koeln.de
Telefon:	0221-8275-2323

Für datenschutzrechtliche Fragen oder bei einer Datenpanne, etwa, wenn bei einem IT-Sicherheitsvorfall auch personenbezogene Daten betroffen sind (z.B. bei unbefugter Offenlegung gegenüber Dritten, unbefugtem Zugang von Dritten, unwiederbringlichem Datenverlust ohne Backups), wenden Sie sich bitte auch an die Datenschutzbeauftragten der TH Köln unter der Funktionsadresse:

E-Mail: datenschutzbeauftragter@th-koeln.de

Bitte beachten Sie, dass Sie etwaige Sicherheits- und Datenschutzvorfälle unverzüglich nach Kenntnisnahme melden, sodass rasch Maßnahmen ergriffen werden können und im Falle einer Meldepflicht an die Aufsichtsbehörde die gesetzliche Meldefrist von 72 Stunden (ab Kenntnis) eingehalten werden kann.

Anlage: Typische Nutzungsszenarien

Bitte berücksichtigen Sie als Veranstalter*in einer Videokonferenz bei der Auswahl eines geeigneten Videokonferenzdienstes die nachfolgende Tabelle mit typischen Nutzungsszenarien (nicht abschließend). Es muss sichergestellt werden, dass nur die für die jeweilige Aufgabenerfüllung und für die Erreichung des jeweiligen Zwecks notwendigen Daten verarbeitet werden (Prinzip der Datenminimierung und Datenvermeidung).

Folgende Tabelle kann mit Blick auf Datenschutz als Orientierung bei der Auswahl eines geeigneten Videokonferenzdienstes dienen:

Dienst / **Nutzungsszenarien**	**Schutzbedarf**[1]	**Zoom**	**Microsoft Teams**	**DFNconf**	**Cisco Jabber** (für Beschäftigte)
Lehrveranstaltungen	normal	geeignet	geeignet	geeignet	
Lerngruppen	normal	geeignet	geeignet	geeignet	
Wissenschaftliche Vorträge	normal	geeignet	geeignet	geeignet	
Wissenschaftliche Konferenzen und Tagungen	normal	geeignet	geeignet	geeignet	
Informationsveranstaltungen	normal	geeignet	geeignet	geeignet	
Öffentliche Veranstaltungen	normal	geeignet	geeignet	geeignet	
Prüfungen (insbesondere mit sensiblen oder vertraulichen Inhalten)	hoch	bedingt geeignet (1)	nicht geeignet	geeignet	
Prüfungen (mündliche)	hoch	bedingt geeignet (1)	nicht geeignet	geeignet	
Forschung: Austausch sensibler oder vertraulicher Daten und Informationen in Forschungsprojekten, die einer vertraglichen Geheimhaltungsvereinbarung oder Vertragsstrafen unterliegen	sehr hoch	bedingt geeignet (1), (2)	nicht geeignet	bedingt geeignet (2)	
Forschung: Interviews mit Probanden (mit besonders sensiblen oder vertraulichen Inhalten)	hoch bis sehr hoch	bedingt geeignet (1), (2)	nicht geeignet	bedingt geeignet (2)	
Forschung: Interviews mit Probanden (ohne Fragen zu personenbezogenen Daten)	normal	geeignet	geeignet	geeignet	
Dienstbesprechungen / Teammeetings / Projektarbeiten (ohne sensible oder vertrauliche Inhalte, z.B. über Arbeitsorganisation)	normal	geeignet	geeignet	geeignet	geeignet
Dienstbesprechungen (mit sensiblen oder vertraulichen Inhalten, z.B. über Personalaktendaten, Disziplinarberatungen, Fakultätsinterna)	hoch bis sehr hoch	bedingt geeignet (1)	nicht geeignet	geeignet	geeignet

[1] Ausgehend von einer typisierten Betrachtung.

Dienst / **Nutzungsszenarien**	**Schutz-bedarf**	**Zoom**	**Microsoft Teams**	**DFNconf**	**Cisco Jabber** (für Beschäftigte)
Gremiensitzungen (z.B. Personalratssitzungen mit sensiblen oder vertraulichen Inhalten; mit strategischen, vertraulichen Inhalten zur finanziellen Ausrichtung etc.) (3)	hoch bis sehr hoch	bedingt geeignet (1), (2)	nicht geeignet	geeignet	
Gremiensitzungen (ohne sensible oder vertrauliche Inhalte oder geheime Abstimmungen) (3)	normal	geeignet	geeignet	geeignet	
Öffentliche Sitzungen (z.B. Senat) (3)	normal	geeignet	geeignet	geeignet	
Bewerbungs- bzw. Vorstellungsgespräche	hoch	bedingt geeignet (1)	nicht geeignet	geeignet	
Berufungsverfahren (Sitzung der Berufungskommission mit ggf. vertraulichen Inhalten, sofern diese über den Videokonferenzdienst geteilt werden)	hoch	bedingt geeignet (1)	nicht geeignet	geeignet	
Berufungsverfahren (Vortrag, i.d.R. öffentlich)	normal	geeignet	geeignet	geeignet	
sensible Beratungsgespräche (z.B. psychologische)	sehr hoch	nicht geeignet	nicht geeignet	geeignet	geeignet
Austausch von besonderen Kategorien personenbezogener Daten nach Artikel 9 EU-DS-GVO, wie Gesundheitsdaten, politische Meinungen, Daten über die sexuelle Orientierung etc.	sehr hoch	nicht geeignet	nicht geeignet	geeignet	geeignet

Bemerkungen:

(1) Nur mit aktivierter Ende-zu Ende-Verschlüsselung geeignet (Auswahl „durchgehende Verschlüsselung“ in den Zoom Meeting-Einstellung).

(2) Je nach Vereinbarung: Hier ist eine Einzelfallprüfung durch Veranstalter*in erforderlich.

(3) Vorbehaltlich der Schaffung einer Rechtsgrundlage auch nach Auslaufen des Pandemie-Sonderrechts.

TH Köln

Gustav-Heinemann-Ufer 54

50968 Köln

Technology
Arts Sciences
TH Köln