

Policy der Universität Bremen für die Nutzung von Videokonferenzsystemen

Stand: Juni 2024

Für die Online-Kommunikation in Echtzeit in Forschung, Lehre und Verwaltung stehen an der Universität Bremen unterschiedliche Videokonferenzsysteme zur Verfügung. Ihre basalen Funktionalitäten sind identisch, sie unterscheiden sich jedoch in einigen Zusatz-Funktionen, der Gebrauchstauglichkeit, Grad der Barrierefreiheit, Schutz personenbezogener Daten und Performance.

Jedes dieser Werkzeuge ist in der Bedienung leicht unterschiedlich. Sie können mit allen Systemen Videokonferenzen (mit und ohne Bildübertragung) für unterschiedliche Szenarien nutzen und die verschiedenen Funktionen für die interaktive Gestaltung und Zusammenarbeit einsetzen. Wir empfehlen deshalb allen Nutzenden sich vorab mit dem gewählten Werkzeug, seinen Optionen und rechtlichen Rahmenbedingungen vertraut zu machen. Informationen zu Nutzungsszenarien mit den verschiedenen Systemen in einem rechtlich erlaubten Rahmen finden Sie in der Tabelle am Ende.

An der Universität Bremen werden zwei Systeme zentral unterstützt, ZoomX powered by Telekom (dies hat das „normale“ Zoom abgelöst) und BigBlueButton (BBB). Informationen dazu finden Sie hier:

<https://www.uni-bremen.de/dezernat5/medienstelle/videokonferenzen>

ZoomX powered by Telekom (ZoomX)

Mit ZoomX gibt es nun ein Zoom-Angebot, das den Video- und Audio Datenverkehr verschlüsselt über Server in der EU ermöglicht. Mit der Telekom als Hosting- und Vertragspartner von Zoom X bleiben die Nutzer:innendaten in Deutschland. Für mehr Sicherheit ist zudem standardmäßig eine Ende-zu-Ende-Verschlüsselung (E2EE) aktiviert; erkennbar durch ein Schloss in einem grünen Wappen in der oberen rechten Ecke des aktiven Fensters. Mit dieser Einstellung sind jedoch nicht alle Funktionen verfügbar, bspw. die Telefoneinwahl, Whiteboard, Untertitel (die vollständige Aufzählung der Einschränkungen finden Sie hier: https://support.zoom.com/hc/de/article?id=zm_kb&sysparm_article=KB0065418). Diese kann von der veranstaltenden Person aufgehoben werden, um diese Funktionen zusätzlich zu ermöglichen, sodass nur noch eine einfache Transportverschlüsselung gegeben ist

Eine E2EE ist aber zum einen immer zwingend dann einzusetzen, wenn ein Bruch der Vertraulichkeit von personenbezogenen Daten im Video- und Audio-Datenverkehr ein hohes Risiko für die Rechte und Freiheiten von natürlichen Personen darstellen würde. Dies ist immer bei den sog. besonderen

Kategorien personenbezogener Daten¹ gem. Art. 9 Datenschutz-Grundverordnung (DSGVO), also Gesundheitsdaten, biometrische etc., der Fall. Zum anderen ist auch für personenbezogene Inhalte mit vertraulichen Personaldaten (Auswahlgespräche/Berufungskommissionen, Personalgespräche o.ä.), mit Finanz- und mit Prüfungsinhalten sowie für betrieblich sensible Daten der Universität wie bspw. Vertrags- und Finanzdaten sowie relevante Regelungen und Entscheidungsgrundlagen stets die E2EE zu nutzen (vgl. Sie hierzu auch die Vorgaben in der Tabelle am Ende).

Den datenschutzrechtlichen Vorgaben zur Auslagerung der Datenverarbeitung an die Telekom wird durch einen DSGVO-konformen Auftragsverarbeitungs-Vertrag mit der Telekom sichergestellt. Dieser Vertrag wurde durch die Datenschutzbeauftragte geprüft. Personenbezogene Daten der Uni-Nutzerinnen und Nutzern (Metadaten sowie die übermittelten Daten aus LDAP) werden im Rahmen der Auftragsverarbeitung über eine verschlüsselte Verbindung übermittelt und sind nur von der Telekom in Deutschland einsehbar. In die USA werden ausschließlich pseudonymisierte Daten der Nutzenden weitergegeben. Die Pseudonymisierung funktioniert mit einem Secure Hash Algorithmus (SHA-256). Dies ist ein Einweghash, der aus dem Account (E-Mailadresse) generiert wird. Die Ausgangsdaten können aus dem Hash nicht wieder hergestellt werden.

Weitere Informationen zum Datenschutz und zur Datenverarbeitung nach Art. 13 DSGVO finden sie hier:

https://www.uni-bremen.de/fileadmin/user_upload/dezernate/dezernat5/referat53/Medienstelle/Videokonferenzen/Zoom-Datenschutz_Art13.pdf

Damit wird ZoomX powered by Telekom als sicheres und DSGVO-kompatibles Videokonferenzsystem eingeschätzt.

BigBlueButton (BBB)

BBB ist eine Opensource-Software für webbasierte Videokonferenzen, die auch Präsentationen, Desktop-Freigabe und Screen-Sharing unterstützt und von der Universität Bremen auf eigenen Servern betrieben wird. Die Datenverarbeitung findet damit ausschließlich innerhalb der universitären Systeme statt.

<https://www.uni-bremen.de/zfn/weitere-it-dienste/chat-konferenzsysteme/bigbluebutton-videokonferenzen>

<https://www.uni-bremen.de/zmml/faq-bigbluebutton>

¹ Besondere Kategorien personenbezogener Daten sind personenbezogene Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

Hier gelistete Videokonferenzsysteme die von oder über die Universität Bremen bereitgestellt werden dienen zur Erfüllung von Aufgaben aus Forschung, Lehre, Verwaltung und Aus- und Weiterbildung. Eine Nutzung dieser Systeme zu privaten-, politischen- oder kommerziellen Zwecken im Rahmen der von der Uni-Bremen zur Verfügung gestellten Lizenzen ist nicht zulässig.

Übersicht: Empfehlungen und Zulässigkeit der Systeme²

Konferenzen / VK-System	ZoomX ³	BBB
<p>mit besonderen Kategorien personenbezogener Daten oder mit folgenden anderen personenbezogenen Daten:</p> <ul style="list-style-type: none"> - vertrauliche Personaldaten (Auswahlgespräche /Berufungskommissionen, Personalgespräche o.ä.), - personenbezogene Finanzdaten oder - Prüfungen sowie Beratung Studierender <p>oder</p> <p>mit sonstigen besonders schützenswerten Daten (auch ohne Personenbezug), d.h. betrieblich sensible Daten der Universität wie bspw. Vertrags- und Finanzdaten und Forschungsdaten mit besonderem Schutzbedarf</p>	X mit E2EE	x
<p>Sonstige Inhalte wie bspw. bei der Durchführung von Lehrveranstaltungen, Infoveranstaltungen, etc. in denen keine besonderen Kategorien personenbezogener oder besonders schützenswerter Daten vorkommen</p>	x	x

² Die Angebote über das DFN sind weiterhin nutzbar, werden aber hier nicht weiter ausgeführt. DFNconf kann nicht im größeren Rahmen oder für Lehrveranstaltungen genutzt werden, da die Teilnehmendenzahl auf 23 begrenzt ist. Zudem können Studierende kein Meeting anlegen, da sie den Dienst nicht als Gastgeber:in nutzen dürfen. Informationen zum DFNconf finden sich hier: <https://www.conf.dfn.de/anleitungen-und-dokumentation/> Informationen zum Datenschutz hier: <https://www.conf.dfn.de/datenschutz/>

³ Lizenzen für ZOOMx powered by Telekom werden direkt bei der Anmeldung über Single-Sign-On (SSO) vergeben; Webinarlizenzen müssen angefragt werden. Beide Lizenzen werden automatisch am Ende eines Semesters entzogen, um eine möglichst ökonomische Verwaltung umzusetzen.

University of Bremen Policy on the Use of Video Conferencing Systems

Status on: June 2024

At the University of Bremen, various video conferencing systems are available for real-time online communication in research, teaching, and administration. Their basic functionalities are identical, but they differ in some additional functions, usability, degree of full accessibility, protection of personal data, and performance.

Each of these tools is slightly different in terms of operation. All systems allow you to use video conferencing (with and without image transmission) for different scenarios and utilize the various functions for interactive design and collaboration. We therefore recommend that all users familiarize themselves with the selected tool, its options, and legal framework conditions in advance. Information on usage scenarios for the various systems within a legally permitted framework can be found in the table at the end.

At the University of Bremen, two systems are supported centrally, ZoomX powered by Telekom (this has replaced the "normal" Zoom) and BigBlueButton (BBB). You can find more information here:

<https://www.uni-bremen.de/dezernat5/medienstelle/videokonferenzen> (in German only)

ZoomX powered by Telekom (ZoomX)

With ZoomX, there is now a Zoom service that enables encrypted video and audio data traffic via EU servers. With Telekom as the hosting and contractual partner of ZoomX, user data remains in Germany. For greater security, end-to-end encryption (E2EE) is also activated by default; this is indicated by a lock in a green emblem in the top right-hand corner of the active window. However, not all functions are available with this setting, e.g. telephone dial-in, whiteboard, subtitles (the full list of restrictions can be found here: https://support.zoom.com/hc/de/article?id=zm_kb&sysparm_article=KB0065418). The said encryption can be revoked by the host of the class / meeting in order to enable these additional functions, allowing only simple transport encryption.

However, E2EE encryption must always be used if a breach of confidentiality of personal data in video and audio data traffic poses a high risk to the rights and freedom of natural persons. This is always the case for the so-called special categories of personal data⁴ in accordance with Art. 9 of the General Data

¹ Special categories of personal data are personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as genetic data, biometric data for the purpose of

Protection Regulation (GDPR), i.e. health data, biometric data, etc. In addition, E2EE encryption must always be used for personal content with confidential personnel data (selection interviews / appointment committees, personnel interviews, etc.), financial and audit content, as well as for operationally sensitive university data such as contract and financial data, relevant regulations, and decision-making principles (see also the requirements in the table at the end).

The data protection requirements for outsourcing data processing to Telekom are ensured by a GDPR-compliant order processing contract with Telekom. This contract has been reviewed by the Data Protection Officer. Personal data of university users (metadata and the transmitted data from LDAP) are transmitted via an encrypted connection as part of the order processing and can only be viewed by Telekom in Germany. Only pseudonymized user data is transmitted to the USA. The pseudonymization works with a secure hash algorithm (SHA-256), which is a one-way hash that is generated from the account (email address). The original data cannot be recovered from the hash.

Further information on data protection and data processing in accordance with Art. 13 GDPR can be found here (in German only):

https://www.uni-bremen.de/fileadmin/user_upload/dezernate/dezernat5/referat53/Medienstelle/Videokonferenzen/Zoom-Datenschutz_Art13.pdf

ZoomX powered by Telekom is therefore considered a secure and GDPR-compliant video conferencing system.

BigBlueButton (BBB)

BBB is an open source software for web-based video conferencing that also supports presentations, desktop sharing, and screen sharing and is operated by the University of Bremen on its own servers. Data processing thus takes place exclusively within the university systems.

<https://www.uni-bremen.de/zfn/weitere-it-dienste/chat-konferenzsysteme/bigbluebutton-videokonferenzen> (in German only)

<https://www.uni-bremen.de/zmml/faq-bigbluebutton> (in German only)

uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation.

Video conferencing systems listed here that are provided by or through the University of Bremen serve to fulfill tasks in research, teaching, administration, and further training. The use of these systems for private, political, or commercial purposes within the scope of the licenses provided by the University of Bremen is not permitted.

Overview: Recommendations and Permissibility of the Systems⁵

Conferences / Video Conference Systems	ZoomX ⁶	BBB
<p>special categories of personal data or the following other personal data:</p> <ul style="list-style-type: none"> - confidential personnel data (selection interviews / appointment committees, personnel interviews, or similar), - personal financial data, or - examinations and advice given to students <p>or</p> <p>other particularly sensitive data (including data without personal reference), i.e. operationally sensitive university data such as contractual and financial data and research data with special protection requirements</p>	<p>X via E2EE</p>	<p>x</p>
<p>Other content, e.g. when holding classes, information events, etc., where no special categories of personal data or data requiring special protection are involved</p>	<p>x</p>	<p>x</p>

2 The services offered via the DFN can still be used, but are not described further here. DFNconf cannot be used on a larger scale or for classes, as the number of participants is limited to 23. In addition, students cannot create a meeting as they are not allowed to use the service as hosts. Information on DFNconf can be found here: <https://www.conf.dfn.de/anleitungen-und-dokumentation/> (in German only) and data protection information is available here: <https://www.conf.dfn.de/datenschutz/> (in German only)

3 Licenses for ZOOMx powered by Telekom are issued directly upon registration via Single-Sign-On (SSO); webinar licenses must be requested. Both licenses are automatically withdrawn at the end of a semester in order to implement the most economical administration possible.