# Projekt Rechtsinformationsstelle Digitale Hochschule NRW

Leitung: Prof. Dr. Thomas Hoeren

Bearbeiter: wissenschaftliche MitarbeiterInnen Malin Fischer, Julian Albrecht

Veröffentlicht am 02. Juli 2020

## A. Fragestellung

Trifft die Hochschulen aus datenschutzrechtlicher Perspektive eine Pflicht, einen anderen Videokonferenzdienst als Zoom zu nutzen.

## B. Hintergrund

Die Corona-Krise erfordert ein in weiten Teilen „digitales Sommersemester“, welches die Hochschulen in NRW ad hoc organisieren müssen, teilweise ohne sich zuvor stark mit der Digitalisierung der Lehre beschäftigt zu haben.

Um den Lehrbetrieb aufrechterhalten und insbesondere Vorlesungen weiterhin stattfinden lassen zu können, haben viele Hochschulen in einem ersten Schritt Videokonferenzsysteme eingerichtet. Sehr häufig wird dabei der Videokonferenzdienst Zoom verwendet, insbesondere aufgrund der einfachen Bedienung und der hohen Maximalanzahl an Teilnehmern eines Meetings. Dessen datenschutzrechtliche Bewertung wurde von der RiDH bereits vorgenommen mit dem Ergebnis, dass Zoom – unter bestimmten Voraussetzungen – datenschutzrechtskonform eingesetzt werden kann.[1]

In einem zweiten Schritt soll nun die Frage behandelt werden, ob und inwieweit Videokonferenzsysteme anderer Anbieter datenschutzrechtlich empfehlenswerter sind als Zoom und daher – auch und insbesondere von Hochschulen – vorrangig genutzt werden müssen.

## Inhalt

A. Fragestellung ..... 1
B. Hintergrund ..... 1
C. Zusammenfassung ..... 2
D. Microsoft Teams ..... 4
I. Allgemeines ..... 4
II. Datenschutz und -sicherheit ..... 4
III. Fazit ..... 5
E. Cisco WebEx Meetings ..... 6
I. Allgemeines ..... 6
II. Datenschutz und -sicherheit ..... 6
III. Fazit ..... 7
F. Jitsi Meet ..... 7
I. Allgemeines ..... 7

[1] *Albrecht u.a.*, Datenschutzrechtlicher Leitfaden Zoom, abrufbar unter https://www.itm.nrw/wp-content/uploads/RiDHnrw_18.05.20_Datenschutzrechtlicher-Leitfaden-Zoom-Angebot-durch-Hochschulen-NRW.pdf (zuletzt abgerufen am 02.07.20).

II. Datenschutz und -sicherheit ..... 8
III. Fazit ..... 8
G. GoToMeeting ..... 8
I. Allgemeines ..... 8
II. Datenschutz und -sicherheit ..... 9
III. Fazit ..... 9
H. DFNConf ..... 9
I. Allgemeines ..... 9
II. Datenschutz und -sicherheit ..... 9
III. Fazit ..... 10
I. BigBlueButton ..... 10
I. Allgemeines ..... 10
II. Datenschutz und -sicherheit ..... 10
III. Fazit ..... 11
J. Linksammlung ..... 11

## C. Zusammenfassung

Eine Pflicht, aus datenschutzrechtlichen Gründen einen anderen Dienst als Zoom zu nutzen, besteht unserer Einschätzung nach nicht.

Mehrere Gründe sprechen für eine solche Einschätzung:

Von der Nutzung von Zoom wurde u.a. durch den Bundesdatenschutzbeauftragten abgeraten, da der Dienst keine Ende-zu-Ende-Verschlüsselung für seine Meetings einsetzt.[2] Allerdings bietet derzeit nur ein anderer der von uns untersuchten Dienste, nämlich Cisco WebEx Meetings, eine solche Ende-zu-Ende-Verschlüsselung für Videokonferenzen mit mehr als zwei Teilnehmern an. Die Verschlüsselung ist bei WebEx nur auf Anfrage verfügbar und geht mit einer Beschränkung einiger Funktionen für die Meetings einher. Indes arbeitet Zoom derzeit an einer Ende-zu-Ende-Verschlüsselung für alle Nutzer des Dienstes.[3]

Zoom stand außerdem wegen diverser Sicherheitslücken in der Kritik, die z.B. das sogenannte „Zoom-Bombing“, also das unbefugte Beitreten fremder Personen zu Videokonferenzen ermöglichten. Der Dienst hat diesen Lücken inzwischen Abhilfe geleistet und insbesondere datenschutzfreundliche Voreinstellungen wie eine standardmäßig aktivierte Passwortschutz- und Warteraumfunktion eingerichtet.[4] Insgesamt hat Zoom in den letzten Wochen und Monaten hinsichtlich des

[2] Vgl. https://www.br.de/nachrichten/netzwelt/bundesdatenschutzbeauftragter-raet-von-videochat-dienst-zoom-ab,RzvSCFk (zuletzt abgerufen am 02.07.20).
[3] Hierzu wird in Kürze noch eine von der RiDH in Zusammenarbeit mit dem DFN erstellte Zusammenfassung erscheinen.
[4] Zu den datenschutzrechtlichen Verbesserungen durch das Update Zoom 5.0. siehe *Fischer/Mc Grath*, Zoom 5.0. – welche Verbesserungen bringt das Update?, abrufbar unter https://www.itm.nrw/wp-content/uploads/RiDHnrw_14.05.20_Neuerungen-bei-Zoom-5.0.pdf (zuletzt abgerufen am 02.07.20).

Datenschutzes erheblich nachgebessert, sodass z.B. der baden-württembergische Landesdatenschutzbeauftragte seine Kritik an dem Dienst weitgehend zurückgezogen hat.[5]

Indes sind auch bei dem Videokonferenzdienst Cisco WebEx Meetings in der Vergangenheit immer wieder erhebliche Sicherheitslücken zutage gekommen, die Angriffe von außen zuließen.

Ein weiterer Kritikpunkt gegenüber Zoom ist allerdings, dass eine Datenübertragung in Länder außerhalb der EU und damit außerhalb des Geltungsbereichs der DSGVO nicht gänzlich ausgeschlossen werden kann. Dasselbe gilt allerdings auch für den Dienst Microsoft Teams, der sich vorbehält, Daten auch an anderen Orten zu verarbeiten. Für den Dienst Cisco WebEx Meetings steht fest, dass bestimmte Daten auch außerhalb der EU verarbeitet werden. Der Dienst GoToMeeting verarbeitet Daten ausschließlich auf Servern in den USA oder in der Cloud.

Die beiden Open-Source-Software-Lösungen von Jitsi Meet und Big Blue Button ermöglichen zwar die Datenverarbeitung auf eigenen Servern oder auf denen von selbst beauftragten Dienstleistern, sodass die Daten stets unter der eigenen Kontrolle bleiben und nicht an Dienstleister außerhalb der EU übermittelt werden. Allerdings haben viele Hochschulen keine ausreichenden Serverkapazitäten, um insbesondere große Veranstaltungen über die Open-Source-Lösungen laufen zu lassen, sodass diese Lösungen keine passende Alternative darstellen.

Gleiches gilt für den Videokonferenzdienst DFNConf, bei welchem die Daten ausschließlich an den Kernnetzknoten im Wissenschaftsnetz oder durch deutsche Anbieter, mit denen ein Auftragsdatenverarbeitungsvertrag geschlossen wurde, verarbeitet werden. Bei diesem Dienst sind derzeit Videokonferenzen nur mit bis zu 23 Personen möglich, sodass sogar der Anbieter selbst dazu rät, für das E-Learning andere Dienste zu nutzen.

Der Aspekt der Maximalanzahl an Teilnehmern und der Funktionalität der Dienste im Allgemeinen spielt auch vor folgendem Hintergrund eine wichtige Rolle: Der Erlaubnistatbestand zur Datenverarbeitung gemäß Art. 6 Abs. 1 UAbs. 1 lit. e DSGVO, auf den eine Datenverarbeitung im Rahmen von Videokonferenzen durch (öffentliche) Hochschulen regelmäßig gestützt werden kann, beinhaltet die Tatbestandsvoraussetzung der Erforderlichkeit der Datenverarbeitung. Die Erforderlichkeit der Datenverarbeitung wiederum umfasst *auch* das Merkmal der Effizienz. Die Datenverarbeitung ist also – unter anderem – dann erforderlich, wenn sie zu einer effizienten Aufgabenerfüllung führt.[6] Die effiziente Erfüllung der öffentlichen Aufgabe der Hochschulen in diesem Zusammenhang – nämlich die Ermöglichung der Teilhabe der Studierenden an der Lehre gemäß den §§ 3 Abs. 1 S. 1, 58 ff. HG NRW – umfasst eben auch den Einsatz von Videokonferenzsystemen, die eine möglichst große Anzahl an Teilnehmern zulassen, nutzerfreundlich sind und eine breite Facette an Funktionen aufweist. Vor diesem Hintergrund kann der Nutzung vom Zoom-Dienst, der bis zu 1000 mögliche Teilnehmer zulässt und durchaus bedienungsfreundlich ist, nicht entgegengehalten werden, dass ohne dessen Einsatz die Aufgabe weniger effizient, aber immerhin überhaupt noch erfüllt werden kann[7], z.B. indem Konferenzdienste eingesetzt werden, die auf eigenen Servern installiert werden und damit einen höheren Datenschutz aufweisen, dann aber nur eine kleine Anzahl an Teilnehmern zulassen und weniger Funktionen bieten.

Aus unserer Sicht besteht zusammenfassend also keine datenschutzrechtliche Pflicht dazu, einen anderen Videokonferenzdienst als Zoom zu verwenden.

---

[5] Vgl. https://www.baden-wuerttemberg.datenschutz.de/warnung-des-lfdi-wurde-gehoert-zoom-bessert-nach/ (zuletzt abgerufen am 02.07.20).

[6] *Heberlein,* in: Ehmann/Selmayr/Heberlein, DS-GVO, 2. Auflage, Art. 6 Rn. 23.

[7] So auch *Reimer*, in: Sydow, DS-GVO, 2. Auflage, Art. 6 Rn. 47.

# D. Microsoft Teams

## I. Allgemeines

Microsoft Teams ist eine Kommunikationsplattform zur digitalen Zusammenarbeit, die neben Funktionen wie Chats, Newsfeeds und der Integration von Office 365 auch das Abhalten von Videokonferenzen mit derzeit bis zu 250 Teilnehmern ermöglicht. Ein geplantes Update soll nun eine Teilnehmeranzahl von bis zu 300 Personen zulassen.

In einer Videokonferenz via Teams gibt es, wie bei vielen anderen Diensten auch, u.a. die Möglichkeit, den eigenen Bildschirm und andere Inhalte zu teilen. Auch eine Chatfunktion besteht. Für die kostenpflichtige Version gibt es außerdem die Möglichkeit, eine Videokonferenz aufzuzeichnen, ein gemeinsames Whiteboard zu nutzen sowie Microsoft-Office Produkte zu verknüpfen.

Der Anbieter Microsoft hat seinen Sitz in Redmond, Washington, USA.

## II. Datenschutz und -sicherheit

Microsoft Teams stand in letzter Zeit hinsichtlich des Datenschutzes deutlich in der Kritik. Insbesondere wurde bemängelt, dass die User-IDs von Nutzern an andere Dienste wie die Adobe Experience Cloud, die Adobe Tochter Marketo, an Google Ads und an Scorecardressearch weitergegeben wurden.[8] In der Rubrik „Datenschutz und Microsoft Teams“ heißt es von Microsoft, dass keine Daten an Dritte weitergegeben werden, es sei denn, der Kunde fordert dies, die Weitergabe ist in den Nutzungsbedingungen für Online-Dienste[9] vorgesehen (z.B. die Weitergabe von Daten an autorisierte Subunternehmer zur Bereitstellung von bestimmten Teilen der Dienste) oder sie ist gesetzlich vorgeschrieben.[10] Inzwischen hat der Dienst die Weitergabe von Daten wohl beendet.[11]

Die Daten von Teams-Nutzern in Deutschland werden in den Rechenzentren in Frankfurt und Berlin, die seit November 2019 bestehen, gespeichert. Allerdings behält sich Microsoft in seinen Datenschutzbestimmungen vor, Daten in den USA oder jedem anderen Land zu verarbeiten, indem Microsoft oder ein Unterauftragsverarbeiter tätig ist.[12]

Die Verbindungen bei Microsoft Teams werden ebenso wie die bei Zoom über TLS transportverschlüsselt. Eine Ende-zu-Ende-Verschlüsselung gibt es also auch bei diesem Dienst nicht.

Für die Datenverarbeitung beim Einsatz von Microsoft Teams sieht der Betreiber genau wie Zoom das Konstrukt der Auftragsdatenverarbeitung (Art. 28 DSGVO) vor. Der Kunde, in diesem Fall also die Hochschule, ist dabei der für die Datenverarbeitung Verantwortliche, Microsoft ist Auftragsdatenverarbeiter.

Hierfür stellt Microsoft nicht einen selbstständigen Auftragsdatenverarbeitungsvertrag zur Verfügung, sondern regelt die Auftragsdatenverarbeitung durch ein Data Processing Addendum

---

[8] *Eberl,* Datenschutz bei Microsoft Teams?, v. 17.05.2020, abrufbar unter https://rufposten.de/blog/2020/05/17/datenschutz-bei-microsoft-teams/ (zuletzt abgerufen am 02.07.20).
[9] Abrufbar unter https://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=31 (zuletzt abgerufen am 02.07.20).
[10] Abrufbar unter https://docs.microsoft.com/de-de/microsoftteams/teams-privacy (zuletzt abgerufen am 02.07.20).
[11] *Eberl*, Fn. 5.
[12] Nutzungsbedingungen für Microsoft-Online-Dienste, Abschnitt „Datenschutzbestimmungen – Datenübermittlungen und Speicherstelle – Datenübermittlungen“, abrufbar unter https://docs.microsoft.com/de-de/microsoftteams/teams-privacy (zuletzt abgerufen am 02.07.20).

(DPA), welches in die Nutzungsbedingungen für Microsoft-Online-Dienste eingebettet ist. Das ist gemäß dem Wortlaut des Art. 28 Abs. 2 DSGVO, wonach die Verarbeitung durch einen Auftragsverarbeiter „auf Grundlage eines Vertrages oder eines sonstigen Rechtsinstruments […]“ erfolgt, rechtlich auch möglich. Akzeptiert der Kunde die Nutzungsbedingungen, akzeptiert er damit auch automatisch die Auftragsdatenverarbeitung. Ob es dem Schriftformerfordernis des Art. 28 Abs. 9 DSGVO genügt, dass der Kunde die Auftragsdatenverarbeitung durch Setzen eines Häkchens gemeinsam mit den Nutzungsbedingungen akzeptiert, wird dabei unterschiedlich beurteilt.[13]

Im Anhang zu den Nutzungsbedingungen finden sich unter anderem von der EU bereitgestellte Standardvertragsklauseln (SCCs), auf denen ein Auftragsdatenverarbeitungsvertrag gemäß Art. 28 Abs. 6 DSGVO unbeschadet individueller Vereinbarungen beruhen kann und die dazu dienen, Datentransfers in Drittstaaten zu rechtfertigen.

An dem DPA wurde unter anderem durch die Berliner Datenschutzbeauftragte deutliche Kritik geübt. So sei der Auftragsverarbeitungsvertrag an verschiedenen Stellen unklar formuliert und widerspreche den Mindestanforderungen der DSGVO. Zudem seien die Standardvertragsklausen unzulässig abgeändert worden, sodass ein Datenexport nicht auf Grundlage der Klauseln gerechtfertigt werden könnte.[14] Microsoft hat inzwischen auf die Kritik reagiert und sowohl die Bestimmungen zum Datenschutz in den Nutzungsbedingungen als auch die Standardvertragsklauseln überarbeitet[15] – allerdings ohne seine Nutzer darüber zu informieren.

Microsoft Teams ist im EU-US-Privacy Shield registriert, welches eine Rechtsgrundlage für die Datenübertragung in die USA in Form eines Angemessenheitsbeschlusses der EU-Kommission nach Art. 45 Abs. 1 DSGVO darstellt. Zudem entspricht der Dienst den Zertifikaten ISO 27001, ISO 27002 und ISO 27018. Die Zertifikaten ISO 27001 und ISO 27002 enthalten Vorgaben und Vorschläge für das Einrichten, Umsetzen, Betreiben und Optimieren eines Informationssicherheits-Managementsystems. Der Standard 27018 beinhaltet einen Verhaltenskodex zum Datenschutz für Cloud-Service-Anbieter.

Zum Datenschutz während der Meetings bietet Microsoft Teams wie auch der Konkurrent Zoom insbesondere die Möglichkeit, Warteräume (Lobbys) einzurichten, damit der Meeting-Host die Teilnehmer einzeln zum Meeting hinzufügen kann. Während des Meetings kann der Moderator außerdem Teilnehmer entfernen, bestimmen, wer Moderator und wer Teilnehmer ist und welche Inhalte von wem geteilt werden dürfen.
Wird eine Sitzung aufgezeichnet, werden alle Teilnehmer im Voraus hierüber benachrichtigt. Die aufgezeichnete Konferenz ist außerdem nur für Teilnehmer des Meetings und für Personen, die zu dem Meeting eingeladen wurden, zugänglich.

## III. Fazit

Die datenschutzrechtliche Bewertung von Microsoft Teams fällt durchwachsen aus.
Insbesondere die bis vor kurzem noch erfolgte Datenweitergabe und das mangelhafte DPA sind kritisch zu beurteilen.
Allerdings reagiert der Dienst auf die an ihm geübte Kritik schnell, z.B. indem er in den letzten Wochen die Weitergabe von Daten eingestellt und das DPA abgeändert hat – inzwischen entspricht

---

[13] Dafür *Thiede*, Office 365 und der Vertrag zur Auftragsverarbeitung, abrufbar unter https://datenschutz-schule.info/2018/10/06/office-365-und-der-vertrag-zur-auftragsverarbeitung/ (zuletzt abgerufen am 02.07.20); dagegen *Notholt*, Auftragsverarbeitung: So schließen Sie einen Vertrag zur AVV richtig ab, abrufbar unter https://comp-lex.de/abschluss-vereinbarung-zur-auftragsvereinbarung-avv/ (zuletzt abgerufen am 02.07.20).
[14] Vgl. https://fragdenstaat.de/dokumente/4760-microsoft-word-682523/ (zuletzt abgerufen am 02.07.20).
[15] Die Änderungen können eingesehen werden unter https://paulinajopes.ch/BlnBDI_Microsoft/TrackChanges_SilentUpdate_Microsoft-DPA_2020-06-09.pdf (zuletzt abgerufen am 02.07.20).

das DPA unseres Erachtens den von Art. 28 DSGVO geforderten Standards und kann daher datenschutzrechtskonform abgeschlossen werden.

Problematischer beurteilen wir, dass Maßnahmen wie die Abänderung des DPA durchgeführt wurden, ohne die Nutzer darüber zu informieren. Dieses Vorgehen erweckt den Eindruck eines intransparenten Umgangs mit dem Datenschutz.

Hier ist z.B. der Konkurrent Zoom, der inzwischen in transparenter Weise über Maßnahmen hinsichtlich Datenschutz und Datensicherheit informiert, fortschrittlicher.

# E. Cisco WebEx Meetings

## I. Allgemeines

Cisco WebEx Meetings ist eine reine Kommunikationssoftware, welche unter anderem die Möglichkeit bietet, Videokonferenzen mit bis zu 200 Teilnehmern abzuhalten. Auch sie beinhaltet Funktionen wie das Teilen des Bildschirms und die Aufzeichnung von Meetings. Zudem bietet WebEx eine flexible Einwahl in die Konferenzen über PC-, Web- oder Mobile Clients.

Der Betreiber Cisco Systems hat seinen Sitz in San José, Kalifornien, USA.

## II. Datenschutz und -sicherheit

Die Daten der deutschen Nutzer von WebEx Meetings werden größtenteils in den europäischen Rechenzentren in London, Amsterdam und Frankfurt verarbeitet. Einige Daten, die z.B. beim Erstellen und Verwalten eines Benutzerkontos anfallen, werden allerdings global, also auch in den USA, gespeichert und verarbeitet. Zudem können von lokal gespeicherten Daten anderenorts Kopien angefertigt werden.

Die Frage der datenschutzrechtlichen Verantwortlichkeit löst Cisco ebenfalls richtigerweise über eine Auftragsdatenverarbeitung. Der Auftragsdatenverarbeitungsvertrag[16], den Cisco hierzu bereitstellt, weist jedoch einige Mängel auf. So geht aus dem Vertrag nicht der Gegenstand der Verarbeitung hervor und auch der Zweck und die Dauer der Verarbeitungen werden nicht genannt.[17]

Im Anhang zu dem AVV finden sich auch die EU-Standardvertragsklauseln.

WebEx verwendet für Videokonferenzen grundsätzlich eine TLS-Verschlüsselung. Auf Anfrage bietet der Dienst auch eine Ende-zu-Ende-Verschlüsselung für Meetings an. Damit einher gehen jedoch Einschränkungen der Funktionen während eines Meetings. So können beispielsweise Aufzeichnungen verschlüsselter Meetings nicht in der Cloud und auch Sitzungsdaten, Abschriften, Besprechungsnotizen usw. nicht gespeichert werden. Es können keine persönlichen Besprechungsräume eingerichtet oder geteilte Daten am Ende eines Meetings in den Konferenzbereich hochgeladen werden. Zudem ist ein Meetingbeitritt mit einem Linux Client nicht möglich. Es wird also deutlich, dass eine Ende-zu-Ende-Verschlüsselung der Meetings über WebEx einen erheblichen Verlust an Funktionen zur Folge hat.

WebEx Meetings kann verschiedene Datenschutzzertifikate vorzeigen: Der Dienst ist sowohl im EU-US-Privacy Shield als auch im Swiss-US-Privacy Shield registriert. Zudem hat sich der Dienst Binding Corporate Rules (BCR) unterworfen. Die BCR sind verbindliche interne Datenschutzrichtlinien, die in einem von der Artikel-29-Datenschutzgruppe entwickelten Rahmen erstellt wurden. Weiterhin hat er sich den APEC Cross Border Privacy Rules und der APEC Privacy Recognition for Processors zur

[16] Abrufbar unter https://trustportal.cisco.com/c/dam/r/ctp/docs/dataprotection/cisco-master-data-protection-agreement.pdf (zuletzt abgerufen am 02.07.20).
[17] Siehe auch https://www.activemind.de/magazin/vergleich-videokonferenz/ (zuletzt abgerufen am 02.07.20).

grenzüberschreitenden Datenschutzregulierung im Pazifik-Raum unterworfen und kann die Zertifikate ISO 27001, ISO 27017 und ISO 27018 vorweisen.

Ein großes Manko des Dienstes ist jedoch die Datensicherheit. Cisco WebEx hat immer wieder mit teils erheblichen Sicherheitslücken zu kämpfen. So wurde beispielsweise Anfang 2017 aufgedeckt, dass über das Chrome-Plugin beliebige Codes auf Windows-Rechnern ausgeführt werden konnten, um so z.B. Schadsoftware auf den PCs zu installieren.[18] Nur wenige Monate später wurde dann ein nächstes Sicherheitsloch aufgedeckt, durch welches erneut über die Chrome- und Firefox-Plugins der Software Schadsoftware auf Windows-Systemen installiert werden konnte.[19] Erst kürzlich wurde nun bekannt, dass die WebEx-Meeting-Software über drei Sicherheitslücken angreifbar ist und dadurch z.B. Schadcode auf den betroffenen Systemen installiert werden kann. Davon betroffen ist die Desktop-App von Rechnern mit dem Betriebssystem macOS.[20] Auch bei einer kürzlich vorgenommenen Risikobewertung von Videokonferenzdiensten mit Fokus auf die Sicherheit der mobilen Android- und iOS-Apps durch ein deutsches Unternehmen, das im Bereich von Mobile Security tätig ist, schnitt der Dienst am schlechtesten ab, da er eine mangelhafte Verschlüsselung und eine unsichere Implementierung von Android Webview aufweist.[21]

Zum Datenschutz während eines Meetings ist ebenfalls der Einsatz eines Passwortes sowie das Sperren eines Meetings möglich. Zudem können (unbefugte) Teilnehmer jederzeit aus einem Meeting entfernt werden. Wird ein Meeting aufgezeichnet, so kann die Aufzeichnung mit einem Passwort versehen werden, um sie nur bestimmten Personen zugänglich zu machen.

### III. Fazit

Zwar bemüht sich Cisco darum, hohe Datenschutz- und -sicherheitsstandard zu implementieren und umzusetzen. Insbesondere die – wenn auch nur auf Anfrage – verfügbare Ende-zu-Ende-Verschlüsselung ist im Vergleich zu anderen Diensten fortschrittlich. Auch die verschiedenen datenschutzrechtlichen Richtlinien und Zertifikate, die der Dienst vorweisen kann, weisen auf einen verantwortungsvollen Umgang mit dem Thema Datenschutz hin. Sehr problematisch sind allerdings die teils erheblichen Sicherheitslücken, die WebEx Meetings immer wieder aufweist. Zwar wird auf diese Lücken von Cisco selbst transparent hingewiesen[22] und schnell reagiert. Nichtsdestotrotz stellen sie ein hohes Risiko für die Daten von Nutzern dar. Auch der unzureichende AVV ist kritisch zu bewerten.

Eine vollumfängliche Empfehlung, Cisco WebEx Meeetings zu nutzen, kann daher nicht ausgesprochen werden.

## F. Jitsi Meet

### I. Allgemeines

Jitsi Meet ist ein kostenloses Open-Source-Videokonferenzsystem, mit welchem Videokonferenzen direkt über einen Browser ohne Installation oder Anmeldung abgehalten werden können. Der Dienst kann auf eigenen Servern installiert werden. Werden keine eigenen Server eingesetzt, können

---

[18] https://www.heise.de/security/meldung/WebEx-Boeses-Sicherheitsloch-in-Ciscos-Web-Conferencing-3606292.html (zuletzt abgerufen am 02.07.20).
[19] https://www.heise.de/security/meldung/Web-Conferencing-Software-Cisco-stopft-erneut-kritische-Luecke-in-WebEx-3774060.html (zuletzt abgerufen am 02.07.20).
[20] https://www.heise.de/security/meldung/Sicherheitsupdates-Cisco-Webex-Meetings-kann-sich-an-Fake-Updates-verschlucken-4787456.html (zuletzt abgerufen am 02.07.20).
[21] https://www.all-about-security.de/security-artikel/management-und-strategie/single/so-unsicher-sind-teamwork-apps-und-video-konferenzen-von-zoom-slack-google-co (zuletzt abgerufen am 02.07.20).
[22] z.B. https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-token-zPvEjKN (zuletzt abgerufen am 02.07.20).

öffentliche Server ausgewählt werden, die ihre Kapazitäten zum Gebrauch zur Verfügung stellen. Diese öffentlichen Server ermöglichen in der Regel Videokonferenzen für maximal 50 bis 200 Teilnehmer.

Für die jeweilige Videokonferenz kann ein Passwortschutz eingerichtet werden. In der Videokonferenz kann der Bildschirm oder andere bestimmte Fenster freigegeben werden. Zudem ist eine Chat-Funktion vorhanden. Außerdem können Verbindungsdetails angezeigt werden, sodass gegebenenfalls nachvollzogen werden kann, wessen Internetverbindung nicht funktioniert.

Der Entwickler von Jitsi Meet, 8x8 Inc., hat seinen Sitz in Campbell, California, USA.

### II. Datenschutz und -sicherheit

Ein Vorteil gegenüber anderen Diensten in datenschutzrechtlicher Hinsicht ist, dass das Tool auf eigenen Servern installiert werden kann. Die Daten, die verarbeitet werden, verlassen somit nicht den eigenen Herrschaftsbereich. Auch die Verarbeitungsvorgänge bleiben intern und somit stets unter der eigenen Kontrolle. Stehen eigene Serverkapazitäten gar nicht oder nicht in ausreichendem Maße zur Verfügung, muss zwar ein anderer Server ausgewählt werden. Auch hier hat man jedoch selbst in der Hand, einen vertrauenswürdigen Serverbetreiber auszuwählen und somit auch einen weitreichenden Schutz der personenbezogenen Daten, die verarbeitet werden, sicherzustellen.

Jitsi Meet wirbt außerdem mit einer Ende-zu-Ende-Verschlüsselung.[23] Standardmäßig funktioniert die Verschlüsselung allerdings nur mit zwei Teilnehmern. Sobald ein dritter Teilnehmer hinzukommt, ändert sich die Ende-zu-Ende-Verschlüsselung aus technischen Gründen in eine Transportverschlüsselung um. In einem Blogpost aus April berichtet das Jitsi Team darüber, dass eine Ende-zu-Ende-Verschlüsselung für Jitsi Meet geplant ist und erklärt, wie diese technisch umgesetzt werden soll.[24] Noch ist die Umsetzung der Verschlüsselung jedoch nicht erfolgt.

Auch für Meetings über Jitsi Meet besteht zum Datenschutz z.B. die Möglichkeit, einen Passwortschutz einzurichten oder Teilnehmer aus dem Meeting zu entfernen.

### III. Fazit

Aufgrund der Tatsache, dass die Daten auf eigenen Servern gespeichert und verarbeitet werden können, ist Jitsi Meet hinsichtlich des Datenschutzes wohl empfehlenswerter als andere Dienste. Allerdings ist zu berücksichtigen, dass die öffentlichen Server, über welche die Verbindungen laufen, regelmäßig nur eine begrenzte Zahl an Teilnehmern während eines Meetings erlauben und zum Teil schnell überlastet sind. Viele Hochschulen haben häufig nicht die entsprechenden eigenen Serverkapazitäten, um große Vorlesungen mit mehreren hundert Teilnehmern über Videokonferenzen stattfinden zu lassen. Hinzu kommt, dass auch dieser Dienst noch keine Ende-zu-Ende-Verschlüsselung für größere Meetings anbietet.

## G. GoToMeeting

### I. Allgemeines

GoToMeeting ist ein Videokonferenzsystem, bei dem bis zu 250 Teilnehmer an einem Meeting teilnehmen können. Es beinhaltet ebenfalls Funktionen wie das Freigeben des Bildschirms oder anderen Anwendungen, den Austausch von Daten, die Fernsteuerung von Maus und Tastatur und ein virtuelles Whiteboard (allerdings nur für Mac).

Der Betreiber von GoToMeeting, LogMeIn, hat seinen Hauptsitz in Boston, Massachusetts, USA.

---

[23] siehe https://jitsi.org/security/ (zuletzt abgerufen am 02.07.20).
[24] https://jitsi.org/blog/e2ee/ (zuletzt abgerufen am 02.07.20).

### II. Datenschutz und -sicherheit

Auch GoToMeeting setzt eine TLS-Verschlüsselung und keine Ende-zu-Ende-Verschlüsselung ein.

Die Datenverarbeitung findet über die Cloud bzw. über Server des Anbieters in den USA statt. Der Dienst hat sich in dem EU-US-Privacy Shield registrieren lassen.

GoToMeeting stellt für seine Kunden ebenfalls einen Auftragsdatenverarbeitungsvertrag bereit. Der Vertrag, der Regelungen zu Betroffenenrechten, dem Einsatz von Unterauftragsverarbeitern und der Rückgabe und Löschung von Kundendaten entspricht den Standards, die Art. 28 DSGVO stellt.[25]

Im Anhang zu dem AVV finden sich auch die EU-Standardvertragsklauseln.

Folgende Einstellungen zum Datenschutz können während eines Meetings über GoToMeeting getroffen werden: Meetings können mittels eines Passworts geschützt werden. Zudem kann eine Sitzung, sobald sie begonnen hat, gesperrt werden, damit keine unberechtigten Teilnehmer der Sitzung beitreten können. Der Moderator hat weiterhin die Möglichkeit, Teilnehmer aus dem Meeting zu entfernen. Wird eine Sitzung aufgezeichnet, kann der Host außerdem darüber entscheiden, welche Personen Zugriff auf die Aufzeichnung haben soll und welche Inhalte (z.B. Notizen o.ä.) in der Aufzeichnung enthalten sind.

### III. Fazit

GoToMeeting ist datenschutzrechtlich alles in allem unbedenklich. Zwar kann auch dieser Dienst keine Ende-zu-Ende-Verschlüsselung aufweisen. Kritisch zu bewerten ist außerdem, dass die personenbezogenen Daten vollständig in den USA verarbeitet werden.

Der Abschluss des Auftragsdatenverarbeitungsvertrags mitsamt den Standardvertragsklauseln, welcher den Vorgaben der DSGVO entspricht, dürfte hier aber für eine angemessene Absicherung hinsichtlich des Datenschutzes auch bei Übertragung der Daten in die USA dienen.

## H. DFNConf

### I. Allgemeines

DFNConf ist ein vom Verein zur Förderung eines Deutschen Forschungsnetzes (DFN) eingerichteter Videokonferenzdienst, der Videokonferenzen über die Videokonferenzlösung Pexip ermöglicht. Videokonferenzen über Pexip sind mit maximal 23 Videoteilnehmern und zusätzlich 50 Audioteilnehmern möglich.

Der DFNConf-Dienst bietet zwei verschiedene Konferenztypen „Meetingraum“ und „Vorlesung“, die sich im Layout für die Konferenz unterscheiden. Im Meetingraum ist das Layout für den Host und die Teilnehmer dasselbe. Bei der Vorlesung ist es möglich, dass die Teilnehmer nur den Dozenten oder die Präsentation sehen und der Host alle oder zumindest einen Teil der Teilnehmer sehen kann. Während eines Meetings kann der Bildschirm geteilt werden. Auch eine Chatfunktion besteht.

Bei DFNConf sind ebenfalls Aufzeichnungen von Meetings möglich. Zudem gibt es die Möglichkeit, ein laufendes Meeting als Livestream über einen Streaming-Link im DFNConf-Portal öffentlich zugänglich zu machen.

### II. Datenschutz und -sicherheit

Die Verbindungen werden während einer Konferenz über TLS transportverschlüsselt.

[25] So auch Conrad, https://www.datenschutz-notizen.de/datenschutz-bei-videokonferenzen-gotomeeting-logmein-unter-die-lupe-genommen-5425789/ (zuletzt abgerufen am 02.07.20).

Personenbezogene Daten werden nur an den Kernnetzknoten im Wissenschaftsnetz und bei Anbietern in Deutschland, mit denen ein AVV abgeschlossen wurde, gespeichert.

Zum Datenschutz während eines Meetings gibt es z.B. die Möglichkeit, den Zugang zu einem Meeting mittels eines PINs zu beschränken. Ein Meeting kann außerdem abgeschlossen werden, damit es für Unbefugte nicht zugänglich ist.

### III. Fazit

DFNConf ist zwar aus datenschutzrechtlicher Perspektive durchaus empfehlenswert. Positiv zu bewerten ist zum einen, dass die Datenverarbeitung nur auf eigenen Servern oder denen von Dienstleistern in Deutschland verarbeitet werden. Zum anderen zeigt insbesondere die vollumfängliche Datenschutzerklärung den bewussten und transparaten Umgang mit dem Datenschutz.

Allerdings sind die Daten auch bei diesem Dienst nur transport- und nicht Ende-zu-Ende-verschlüsselt.

Zudem ist der Dienst derzeit nur für Konferenzen mit einem sehr beschränkten Teilnehmerkreis geeignet und schließt den Einsatz für Vorlesungen o.ä. damit aus. Zwar wird an einem Ausbau des Dienstes gearbeitet. Dies nimmt jedoch Zeit in Anspruch, sodass sogar der DFN selbst dazu rät, für den Bereich des E-Learnings derzeit noch auf andere Dienste zurückzugreifen.[26]

## I. BigBlueButton

### I. Allgemeines

BigBlueButton ist ein kostenloses Audio- und Videokonferenzsystem, welches als Open-Source-Lösung speziell für das E-Learning entwickelt wurde. Die Software bietet dabei wichtige Tools für das digitale Lernen, wie z.B. ein gemeinsames Whiteboard, ein Umfragetool, einen privaten und einen öffentlichen Chat sowie die Funktion, den eigenen Bildschirm zu teilen und eine Präsentation hierüber zu zeigen. Der Dienst ist besonders geeignet dazu, sich gegenseitig während einer Konferenz Dokumente zu zeigen.

Der Anbieter von BigBlueButton empfiehlt, nicht mehr als 100 Personen an einem Meeting teilnehmen zu lassen. Die Konferenzen können mit einer Zugangsbeschränkung versehen werden.

Wie bei Jitsi ist keine Installation einer App o.ä. erforderlich. Der Client läuft vielmehr über den Webbrowser.

Der Betreiber BigBlueButton Inc. hat seinen Sitz in Ottawa, Kanada.

### II. Datenschutz und -sicherheit

Auch bei BigBlueButton ist der Vorteil, dass die Daten nur auf dem eigenen Server bzw. auf dem des beauftragten Dienstleisters verarbeitet werden und damit unter der eigenen Kontrolle oder der des beauftragten Dienstleisters stehen.

Doch auch bei BigBlueButton sind nur die Verbindungen zum Server transportverschlüsselt. Auf den Servern selbst hingegen sind alle Daten lesbar. Man sollte folglich darauf achten, einen vertrauenswürdigen Server auszuwählen. Wie bei Jitsi Meet findet eine Ende-zu-Ende-Verschlüsselung nur bei Verbindungen zwischen zwei Personen statt.

Ein weiterer Kritikpunkt bei BigBlueButton ist die Aufnahmefunktion. Sofern diese beim Erstellen eines Raumes nicht deaktiviert ist, wird die Konferenz vollständig in Form einer RAW-Daten aufgezeichnet, und zwar unabhängig davon, der Aufnahmeknopf betätigt wurde oder nicht. Wurde

[26] https://www.conf.dfn.de/dfnconf-und-covid-19/ (zuletzt abgerufen am 02.07.20).

die Aufnahmefunktion während der Videokonferenz genutzt, also der Aufnahmeknopf betätigt, so wird die RAW-Datei in eine veröffentlichungsgeeignete Datei umgeändert. Wurde der Aufnahmeknopf hingegen nicht betätigt, so wird die Aufzeichnung in Form der RAW Datei zwei Wochen lang gespeichert und anschließend automatisch gelöscht.[27] Diese vergleichsweise lange „anlasslose" Speicherung der Daten ist datenschutzrechtlich durchaus bedenklich.

Vor und während einer Konferenz über BigBlueButton können folgende datenschutzfreundliche Einstellungen vorgenommen werden: Für den Zugang zu einem Raum kann ein Passwort erstellt werden. Der Zutritt zu einem Raum kann zudem von der Erlaubnis des Hosts abhängig gemacht werden. Die potentiellen Teilnehmer werden dann auf eine Warteliste gesetzt und können individuell akzeptiert oder abgelehnt werden. Teilnehmer können außerdem aus einem Raum entfernt werden.

### III. Fazit

BigBlueButton wird derzeit zwar von verschiedenen Seiten als sehr empfehlenswert insbesondere für den Einsatz an Schulen und Hochschulen angepriesen.[28] Auch dieser Dienst kann aber aus datenschutzrechtlicher Sicht nicht vollumfänglich empfohlen werden. Denn trotz der Vorteile, dass BigBlueButton auf eigenen Servern betrieben werden kann und viele hilfreiche Funktionen für die Lehre aufweist, bleiben zwei Schwächen: Zum einen die fehlende Ende-zu-Ende-Verschlüsselung und zum anderen die Tatsache, dass Videokonferenzen, bei denen die Aufzeichnungsfunktion nicht deaktiviert ist, auch ohne Betätigung des Aufzeichnungsknopfes aufgezeichnet und für einen vergleichsweise langen Zeitraum von zwei Wochen gespeichert werden.

## J. Linksammlung

Informationen aus den folgenden Links wurden für die Recherche zusammengetragen:

**Allgemeines:**

- https://www.heise.de/tipps-tricks/Videokonferenz-Tools-im-Ueberblick-4688243.html#
- https://www.datenschutzexperte.de/blog/datenschutz-im-unternehmen/video-konferenz-tools-datenschutz-quick-check-einzelner-anbieter/
- https://www.activemind.de/magazin/vergleich-videokonferenz/
- https://www.e-recht24.de/artikel/datenschutz/12122-videokonferenzen-und-datenschutz-vergleichstest-zoom.html
- https://www.datenschutz-notizen.de/ende-zu-ende-verschluesselung-von-videokonferenzen-1825597/
- https://www.channelpartner.de/a/anforderungen-an-professionelle-collaboration-loesungen-fuer-kmu,3337629

**Microsoft Teams:**

- https://www.microsoft.com/de-de/microsoft-365/microsoft-teams/group-chat-software
- https://docs.microsoft.com/de-de/microsoftteams/teams-privacy
- https://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=31

---

[27]

[28] So z.B. vom baden-württembergischen LfDI, vgl. https://www.baden-wuerttemberg.datenschutz.de/warnung-des-lfdi-wurde-gehoert-zoom-bessert-nach/ (zuletzt abgerufen am 02.07.20).

- https://news.microsoft.com/de-de/datenschutz-und-sicherheit-in-microsoft-teams-nutzer/
- https://windowsunited.de/der-datenschutzskandal-um-microsoft-teams/
- https://www.chip.de/news/Microsoft-Teams-Videokonferenzen-bekommen-tolle-Upgrades_182648401.html
- https://rufposten.de/blog/2020/05/17/datenschutz-bei-microsoft-teams/
- https://datenschutz-schule.info/2018/10/06/office-365-und-der-vertrag-zur-auftragsverarbeitung/

**Cisco WebEx:**

- https://www.webex.com/de/video-conferencing.html
- https://trustportal.cisco.com/c/dam/r/ctp/docs/privacydatasheet/collaboration/cisco-webex-meetings-privacy-data-sheet.pdf
- https://help.webex.com/de-de/WBX44739/What-Does-End-to-End-Encryption-Do
- https://help.webex.com/de-de/oybc4fb/Data-Residency-in-Cisco-Webex-Teams
- https://help.webex.com/de-de/8zi8tq/Cisco-Webex-Best-Practices-for-Secure-Meetings-Hosts#concept_48653A7246C9127435EBB8028B65EE21
- https://trustportal.cisco.com/c/dam/r/ctp/docs/dataprotection/cisco-master-data-protection-agreement.pdf
- https://its.unibas.ch/fileadmin/user_upload/its/Dokumente/Anleitungen/ZOOM___WEBEX/Anleitung_E2EE_WebexMeetingErstellen.pdf
- https://www.heise.de/security/meldung/Sicherheitsupdates-Cisco-Webex-Meetings-kann-sich-an-Fake-Updates-verschlucken-4787456.html

**Jitsi Meet:**

- https://jitsi.org/jitsi-meet/
- https://jitsi.org/meet-jit-si-privacy/
- https://vpn-anbieter-vergleich-test.de/jitsi-statt-zoom-dsvgo-konformes-online-meeting/
- https://www.google.de/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwi74ojFyojqAhXPMJoKHcY-Ai8QFjADegQIBBAB&url=https%3A%2F%2Fscheible.it%2Fdatenschutzfreundliche-konfiguration-jitsi-meet%2F&usg=AOvVaw1omXfrkuUYrV1VPV2ANO5p
- https://t3n.de/news/jitsi-meet-videokonferenzen-einfach-1273518/
- https://www.chip.de/news/Jitsi-Meet-Bestes-Videochat-Tool-ohne-Anmeldung_182627073.html

**GoToMeeting:**

- https://www.gotomeeting.com/de-de
- https://www.logmeininc.com/de/trust/privacy
- https://logmeincdn.azureedge.net/legal/20191226/DPA/LMI-Customer-Data-Processing-Addendum-2019-v2-DE-SAMPLE.pdf
- https://support.goto.com/de/gotomeeting/help/covid-19-tips-for-staying-secure-using-gotomeeting

- https://www.datenschutz-notizen.de/datenschutz-bei-videokonferenzen-gotomeeting-logmein-unter-die-lupe-genommen-5425789/
- https://assets.cdngetgo.com/25/40/3c77ef574320bfc63f6686199928/545de-gotomeetin-gotowebinar-gototraining-die-sicherheit-der-logmein-webkonferenzloesungen-whitepaper-lmi.pdf

**DFNConf:**

- https://www.conf.dfn.de/
- https://www.conf.dfn.de/datenschutz/
- https://blogs.hrz.tu-freiberg.de/elearning/neuen-videokonferenzdienst-dfnconf/
- https://www.itsb.ruhr-uni-bochum.de/themen/zoom.html

**BigBlueButton:**

- https://bigbluebutton.org/
- https://de.wikipedia.org/wiki/BigBlueButton
- https://digitalcourage.de/digitale-selbstverteidigung/videokonferenzen-muessen-keine-datenschleudern-sein
- https://www.datenschutz-notizen.de/videokonferenzen-mit-bigbluebutton-5425839/
- https://datenschutz-schule.info/datenschutz-check/bigbluebutton-videokonferenzen/
- https://info.gwdg.de/docs/doku.php?id=de:services:mobile_working:elearning_tools:faq

*Abschließender Hinweis: Für die Vollständigkeit und Richtigkeit der in diesem Dokument enthaltenen Informationen können wir keine Haftung übernehmen.*