

Datenschutzfreundlicher Einsatz von Video- und Online- Konferenzsystemen

Janet Amm

6. April 2020

Übersicht

1. Datenschutzrechtliche Aspekte beim Einsatz von Video- und Online-Konferenzsystemen an den bayerischen Kunsthochschulen
2. Informationen zu ausgewählten Anbietern

Europäische Anbieter	Amerikanische Anbieter
Jitsi Meet	GoToMeeting
Nextcloud Talk	Microsoft Teams
TeamViewer (Blizz)	Zoom

3. Nutzungshinweise

1. Datenschutzrechtliche Aspekte

Webkonferenz-Systeme

- Anbieter ermöglichen „virtuelle Meetings“ zwischen zwei oder mehreren Teilnehmern
- bekanntere Anbieter: GoToMeeting, Skype for Business, ClickMeeting, WebEx-Meetings oder meetyoo
- üblich ist der Einsatz als SaaS (Software as a Service) – Modell, bei welchem der Anbieter von der Software bis zur Server-Infrastruktur alles Notwendige für die Nutzung des Webkonferenz-Tools bereitstellt
- Bei den Tools zur Videotelefonie handelt es sich meist um „Software as a Service“ (SaaS), d.h. der Dienst wird über das Internet angeboten
- oft wird noch nicht einmal mehr separate Software auf dem PC benötigt, da die Konferenzen direkt im Webbrowser laufen

Rechtsgrundlage für den Einsatz an den Kunsthochschulen

- Für die Statistik
 - Art. 6 Abs. 1 lit. e i.V.m. Art. 4 BayDSG (Art. 10 Abs. 1 BayHSchG, Art. 7 BayHO)
- Für die Lehre
 - Art. 6 Abs. 1 lit. e DSGVO i.V.m Art. 4 BayDSG (Art. 55 Abs. 2 BayHSchG)
- Für die Beschäftigten und Bediensteten
 - Art. 6 Abs. 1 lit. b DSGVO i.V.m. Art. 4 BayDSG (§ 106 Gewerbeordnung)
 - Art. 6 Abs. 1 lit. c DSGVO i.V.m. Art. 4 BayDSG (Art. 33 Abs. 5 GG)
 - Art. 6 Abs. 1 lit. c DSGVO i.V.m. § 3a Abs. 1 ArbStättV

Einbindung des Personalrat

- Art. 75a Abs. 1 Nr. 1 BayPVG:
 - Mitbestimmungsrecht bei der Einführung technischer Systeme, die zur Überwachung des Verhaltens und der Leistung der Mitarbeiter geeignet ist
 - Webkonferenz-Tools erfassen Login-Daten und dadurch kann die Teilnahme und Anwesenheit der Mitarbeiter überprüft werden

Auftragsverarbeitung

- Anbieter verarbeiten hier als Plattformanbieter für ihre Kunden (die die Kunsthochschulen) personenbezogene Daten und haben auf diese (z.B. im Rahmen der Systemwartung) auch eine Zugriffsmöglichkeit
- Kunsthochschulen als Kunden der Anbieter datenschutzrechtlich verantwortlich gem. Art. 4 Nr. 7 DSGVO
- Pflicht zur datenschutzkonformen Auftragsverarbeitung, u.a. durch sorgfältige Auswahl und Vertragsgestaltung mit einem Auftragsverarbeiter und geeignete technische und organisatorische Maßnahmen

Auswahl neuer Auftragsverarbeiter

Bei der Auswahl des IT-Dienst ist die Beantwortung der folgenden Fragen hilfreich:

- Wo liegt der Speicherort?
- Welche Daten werden für welche Zwecke bei dem Anbieter verarbeitet?
- Wie lange wird gespeichert?
- Werden die Daten analysiert?

Auswahl neuer Auftragsverarbeiter

EU-Dienste vorziehen:

- Webkonferenz-Systeme werden meist als SaaS-Dienst über das Internet angeboten → oftmals findet eine Übermittlung personenbezogener Daten zu dem Anbieter statt
- Anbieter aus der Europäischen Union (EU) bzw. dem Europäischen Wirtschaftsraum (EWR) sind zu bevorzugen, da sie unmittelbar den Anforderungen DSGVO unterliegen und die Daten der Nutzenden in der Regel auf Servern innerhalb der EU bzw. des EWR gespeichert
- Bei Datenübermittlung in ein Drittland sind geeignete Garantien erforderlich, um ein angemessenes Datenschutzniveau im Drittland zu gewährleisten (z.B. Angemessenheitsbeschluss der EU, EU-U.S.-Privacy-Shield-Zertifizierungen von US-Unternehmen)

Auswahl neuer Auftragsverarbeiter

Dienste mit datenschutzfreundlichsten Einstellungen wählen:

- **Verschlüsselung** – Übertragungen sollten verschlüsselt erfolgen
- **Geschäftsnutzung** – Die geschäftliche Nutzung sollte erlaubt sein (da datenschutzrechtliche Zusicherungen auf Geschäftskunden beschränkt sein können). Unter Umständen bieten auch nur bezahlte Versionen die erforderlichen Datenschutzfunktionen.
- **Freigaben** – Bildschirmübertragung oder Aufzeichnung sollte eine ausdrückliche Zustimmung voraussetzen
- **Protokolle und Aufzeichnungen** – Gesprächsverläufe und Aufzeichnungen sollten grundsätzlich nach Gesprächsende gelöscht werden
- **Profiling** – Es sollten keine Verhaltensprofile der Teilnehmer gebildet werden oder diese Funktion sollte abgeschaltet werden können

Auswahl neuer Auftragsverarbeiter

- Abschluss eines **Auftragsverarbeitungsvertrag** erforderlich (Art. 28 DSGVO)
- **Prüfung technischer und organisatorischer Maßnahmen sowie Subunternehmer** (Art. 32 DSGVO)
 - Prüfung der Angaben zu technischen und organisatorischen Maßnahmen (z. B. Pseudonymisierung, Backupverfahren, Verschlüsselungen) sowie eingesetzter Subunternehmer

Datenschutzfreundliche Voreinstellungen und Erforderlichkeitsprüfung

- Wenn Sie die Dienste einsetzen, sollten Sie die Einstellungen möglichst datenschutzfreundlich auswählen (“Datenschutz durch datenschutzfreundliche Voreinstellungen“, Art. 25 Abs. 2 DSGVO)
- Bei Tracking-, Beobachtungs-, Protokoll-, Screen-Sharing- und Aufzeichnungs-Funktionen sog. Erforderlichkeitsprüfung durchführen

Hinweise in der Datenschutzerklärung

- Verpflichtung die Kommunikationsteilnehmer unter anderem über die Zwecke, Arten und den Umfang der Verarbeitung ihrer personenbezogenen Daten im Rahmen der Konferenzen oder Webinare zu informieren (Art. 12, 13 DSGVO)
- Aufnahme in Datenschutzerklärung, um Mitarbeiter wie auch Kunden oder Geschäftspartner zu informieren
- Verweis auf die Datenschutzerklärung in Einladungen zu einem Onlinemeeting

Sicherer Gebrauch von Webkonferenz-Systemen

- Sicherheit der Konferenzen ist von der Sorgfalt und Wachsamkeit der Organisatoren und Teilnehmer abhängig → Nachlässigkeit öffnet Tore für Angreifer und Hacker
- Ratschläge:
 - Erinnern Sie die Mitarbeiter an Updates der jeweiligen Software, um Angreifern einen Schritt voraus zu sein.
 - Jede Sitzung muss durch ein Passwort geschützt sein; so kann niemand zufällig in die Konferenz eindringen.
 - Achten Sie auf unbekannte Teilnehmer in Meetings, um mögliche Angreifer sofort zu erkennen.
 - Diskutieren Sie so wenig sensible Inhalte wie möglich, denn Konferenzen könnten über dritte Programme unbemerkt aufgezeichnet werden.

Umsetzung an den Kunsthochschulen

- Tools, die im Bildungswesen genutzt werden sollen, müssen zum Schutz der personenbezogenen Daten der Studierenden die Anforderungen aus Art. 32 DSGVO an die Datensicherheit erfüllen (ins. Vertraulichkeit und Integrität der Daten)
 - Entscheidung für oder gegen ein bestimmtes digitales Kommunikationstool ist abhängig von der
 - Zahl der Teilnehmer
 - Inhalt der Kommunikation
 - Zeit der Nutzungsdauer
- individuelle Entscheidung für jeden Einsatzbereich

2. Informationen zu ausgewählten Anbietern

Übersicht der Anbieter

Name	Land	Sicherstellung Datenschutzniveau im Drittland	AV-Vertrag/DPA	Datenschutzerklärung
Adobe Connect	USA	Privacy Shield	Auf Anfrage	Link
AnyMeeting	USA	Privacy Shield	Auf Anfrage	Link
Arkadin	DE	–	Auf Anfrage	Link
Cisco WebEx	USA	Privacy Shield und Standardschutzklauseln (SCC)	In SCC enthalten	Link
ClickMeeting	PI	–	Im Kundenkonto	Link
Discord	USA	Privacy Shield	nicht angeboten	Link
edudip	De	–	Im Kundenkonto	Link
fastviewer	De	–	Link	Link
Google Hangouts / Meet	USA	Privacy Shield	Link (automatisch mit AGB akzeptiert)	Link
GoToMeeting	USA	Privacy Shield	Link	Link
Intercall Unified Meeting	USA	Privacy Shield	Link	Link
meetgreen	De	–	Auf Anfrage	Link
meetyoo	De	–	Auf Anfrage	Link
Microsoft Teams	USA	Privacy Shield	Link	Link , Link
Skype for Business	USA	Privacy Shield	Link	Link , Link
Slack	USA	Privacy Shield	Link	Link
TeamViewer	De	Nicht erforderlich	in EULA enthalten	Link
Twitch	USA	–	nicht angeboten	Link
Zoom	USA	Privacy Shield und Standardschutzklauseln (SCC)	In SCC enthalten	Link

Datenschutzrechtliche Analyse einer Auswahl von Kommunikationssoftware

	Facebook Messenger	iMessage	Jitsi (XMPP)	Signal	Skype for Business	Telegram	Threema	Whatsapp	Wire
Verschlüsselter Transport	Ja	Ja	Ja	Ja	Ja	unbekannt	Ja	Ja	Ja
E2EE ¹ : Nachrichten	teilweise ²	Ja	Ja (OTR)	Ja	? ³	teilweise ²	Ja	Ja	Ja
E2EE ¹ : Audio / Video	Nein	Ja	Ja (ZRTP)	Ja	Ja	teilweise ²	Ja ⁴	Ja	Ja
Quellcode verfügbar	Nein	Nein	Ja	Ja	Nein	teilweise ⁵	teilweise ⁶	Nein	Ja
Registration	Tel.-Nr. oder E-Mail	Tel.-Nr. oder E-Mail	Benutzername	Tel.-Nr. / Privater Schlüssel	Benutzername / Passwort oder 2-Faktor	Tel.-Nr. / Benutzername	ID / Privater Schlüssel	Tel.-Nr. / Privater Schlüssel	Tel.-Nr. oder E-Mail
Serverstandort	USA	dezentral weltweit	frei wählbar; Standard: FR	dezentral weltweit	Lokal	dezentral weltweit	CH	USA	EU / CH
Anonyme Nutzung	Aliasname ⁷	Aliasname ⁷	Ja	Nein	Nein	Nein	Ja	Nein	Aliasname ⁷
Betriebssysteme	Windows, MacOS, Linux, Android, iOS, Browser	MacOS, iOS	Windows, MacOS, Linux, Android, iOS ⁸	Windows, MacOS, Android, iOS	Windows, MacOS, Android, iOS	Windows, MacOS, Linux, Android, iOS	Android, iOS, Windows Phone	Windows, MacOS, Linux, Android, iOS	Windows, MacOS, Linux, Android, iOS
Website	messenger.com	apple.com/ios/messages	jitsi.org	signal.org	skype.com/business	telegram.org	threema.ch	whatsapp.com	wire.com

datenschutzfreundlich
 teilweise kritisch
 kritisch

Optionen für die bay. Kunsthochschulen

Europäische Anbieter:

- Jitsi Meet
- Nextcloud Talk
- TeamViewer (Blizz)

Amerikanische Anbieter:

- GoToMeeting
- Microsoft Teams
- Zoom

Jitsi Meet



- Opensource-Software für Instant Messaging und (Video-) Telefonie
- datenschutzfreundlicher Webkonferenzdienst am LRZ, der allen Nutzern des Münchner Wissenschaftsnetz (MWN) zur Verfügung steht
- Videokonferenzen mit maximal 10-15 Teilnehmenden
- läuft am besten auf vorhandenen dedizierten Clients (<https://github.com/jitsi/jitsi-meet-electron/releases/tag/v1.1.1>), die Nutzung im Browser sollte nur in Ausnahmefällen geschehen
- Performance mit Browser Chrome am besten
- Verschlüsselung zwischen Client und Server, aber keine Ende-zu-Ende-Verschlüsselung

Nextcloud Talk



- Videokonferenzsystem der freien Kollaborations- und Cloudlösung Nextcloud
- Aufgrund von Performance-Problemen eher für Kleingruppen mit 3-5 Personen geeignet
- vergleichbar mit Jitsi Meet und setzt auch auf der gleichen Codebasis auf
- nur mit Browsern Chrome und Firefox verwendbar
- Ende-zu-Ende Verschlüsselung:
 - Voraussetzungen: max. zwei Teilnehmer und ein unterstützter Browser
 - wird automatisch aktiviert, wenn Voraussetzungen gegeben sind
 - wird automatisch deaktiviert, wenn die Voraussetzungen nicht gegeben sind

TeamViewer



- TeamViewer ist eine Desktop-Sharing-Software, welche Fernwartungen, Online-Präsentationen, Onlinemeetings, Webkonferenzen, Dateitransfer und VPN-Verbindungen ermöglicht
- TeamViewer bietet mit Blizz auch eine aus Deutschland angebotene Videokonferenzplattform
- Webseite von TeamViewer hat leider Tracking und oft sind die Datenschutzinformationen nur auf Englisch
- Muster für AVV vorhanden

GoToMeeting



- Softwarepaket für Online-Besprechungen, Desktop Sharing und Videokonferenzen
- geeignet für Videokonferenzen und Webinare bis zu 250 Teilnehmende
- läuft stabil - Probleme nur bei schlechter Internetverbindung
- kein richtiger Chat (wird durch Referent moderiert und freigeschaltet)

GoToMeeting: Datenschutz

- [Hochschulforum Digitalisierung zu GoToMeeting:](#)
„US-Server. Daher ist GoToMeeting aus Datenschutz-Sicht nicht uneingeschränkt zu empfehlen.“

Microsoft Teams



- Office 365 stellt eine Reihe von Diensten zur Verfügung, beispielsweise Teams für Chat, Meetings, Telefonieren und Teamarbeit
- Office 365 kann im Bildungsbereich datenschutzkonform eingesetzt werden
- Themenseite der Stabsstelle IT-Recht zu Verträgen der Hochschulen mit IT-Dienstleistern (<https://go.uniwue.de/ms-gdpr>)

Microsoft Teams: Datenschutz

- [Hochschul-Forum Digitalisierung zu Microsoft Teams:](#)

"Microsoft garantiert eine Speicherung auf in Deutschland stehenden Servern. Entsprechend bestehen keine Datenschutzbedenken."

Aber: Support und Wartung kommen für Server aus den USA

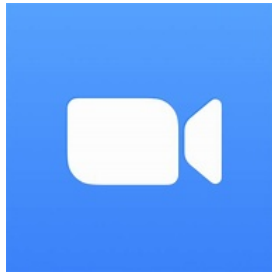
- **Risiken Public Cloud:** Die Daten werden von Microsoft auch für eigene Zwecke verarbeitet, wenn dies erforderlich ist zwecks Abrechnung- und Kontoverwaltung, Vergütung, interner Berichterstattung und Modellierung, Bekämpfung von Betrug, Cyberkriminalität oder Cyberangriffen, Verbesserung der Kernfunktionalität in Bezug auf Barrierefreiheit, Datenschutz oder Energieeffizienz sowie Finanzberichterstattung und Einhaltung gesetzlicher Verpflichtungen
- **Desktop und Mac-Anwendung:** Microsoft nutzt auf Endgeräten gesammelte Informationen für seine eigenen Geschäftsinteressen. Hintergründe dazu erklärt Microsoft etwa zu [Windows 10](#) oder zu Office 365 auf [YouTube](#)

Microsoft Teams: Datenschutzinformationen

Bereitgestellte Datenschutzinformationen und
Datenschutzdokumentationen für öffentliche Stellen in Bayern:

- [MusterVVT für staatliche Hochschulen in Bayern](#)

Zoom



- Zoom ist eine Zusammenarbeitslösung für Audio- und Videokonferenzen sowie das Teilen von Inhalten
- technisch gute Lösung mit guter Performance, aber gebunden an Domain/dienstliche E-Mail-Adresse
- Abschluss eines Auftragsverarbeitungsvertrags erforderlich
- unter dem EU-U.S. Privacy Shield zertifiziert → rechtliche Voraussetzungen für ein angemessenes Datenschutzniveau liegen vor
- Themenseite der Stabsstelle IT-Recht zu Verträgen der Hochschulen mit IT-Dienstleistern (<https://go.uniwue.de/zoom-faq>)

Zoom: Datenschutz

- [Hochschul-Forum Digitalisierung zu Zoom:](#)
„US-Server. Daher ist Zoom aus Datenschutz-Sicht nicht uneingeschränkt zu empfehlen, außerdem gibt es Kritik am Datengrabbung der Anwendung. Einige Hochschulen ([bspw. die Universität Kassel](#) vom 23. März 2020) raten daher davon ab, Zoom zu nutzen.“
- Zoom hat unverzüglich auf öffentliche Kritik reagiert
- seit 29. März 2020 neue [Datenschutzrichtlinie](#)
- am 1. April 2020 umfassendes [Statement](#) zu Maßnahmen für die datenschutzkonforme Nutzung von Zoom:
 - Beendigung der Datenweitergabe an Facebook
 - Update der Datenschutzerklärung
 - Deaktivierung des in Kritik geratenen „Aufmerksamkeitstracking“ (welches darüber hinaus sowieso nur aktiv war, wenn der Host es bewusst aktiviert)

Zoom: Telemetrie und Tracking

- **Webseite:** Die Webseite dient Zoom auch zur Verfolgung umfangreicher Marketingaktivitäten. Das Verfahren zu den Einstellungen von Cookies wirkt nur sehr eingeschränkt. Da dies leider auf fast alle Webseiten im Netz zutrifft sollten nicht auf den Anbieter der Webseite vertrauen und eigene Schutzmaßnahmen ergreifen.
- **Desktop und Mac-Anwendung:** Für diese Anwendung ist aktuell kein ungewollter oder unerwünschter Abfluss an Daten bekannt. Nur für den Fall, dass die die Option Login mit Google oder Facebook nutzen, würde von die Anbietern Daten mit Zoom ausgetauscht.
- **Android-App:** Die Android App setzt u.a. für Analysen auf Firebase. Verbliebene Fragen zu den Rechtsgrundlagen des Einsatzes von Firebase in der App sind derzeit zur Klärung an Zoom weitergegeben worden.
- **iOS-App:** Das Facebook-SDK ist aus der jüngsten App-Version von Zoom für iOS entfernt worden.

Zoom: Nutzungshinweise

- um Zoom verantwortungsvoll zu nutzen, sollte insbesondere auf folgende Funktionen verzichtet werden

- Aufmerksamkeitskontrolle der Teilnehmer

<https://support.zoom.us/hc/en-us/articles/115000538083-Attendee-attention-tracking>

- Tracking auf der Registrierungsseite

<https://support.zoom.us/hc/en-us/articles/115003478863-Using-Facebook-Pixel-with-Zoom>

Besprechung planen

In Meeting (Grundlagen)

In Meeting (Erweitert)

Einladung E-Mail Markenbildung

E-Mail-Benachrichtigung

Administratoroptionen

DSCP-Markierung

Klassifizierung für Netzwerkdatenverkehr bestimmen DSCP Markierung für Signalisierung und Medienpakete aktivieren. (Standardeinstellung ist 56 für Audio, 40 für Video und 40 für Signalisierung.) 



Den Benutzern ermöglichen, in ihren Client-Einstellungen Stereoton zu wählen

Benutzern erlauben, Stereo-Audio während eines Meetings zu wählen



Den Benutzern ermöglichen, in ihren Client-Einstellungen den Originalton zu wählen

Benutzern erlauben, Originalton während eines Meetings zu wählen



Aufmerksamkeitstracking

Ermöglicht dem Host, eine Anzeige in der Teilnehmergruppe zu sehen, wenn ein Teilnehmer der Besprechung/des Webinars während der Bildschirmfreigabe Zoom nicht scharf eingestellt hat.



Wartezimmer

Teilnehmern erlauben, das Herunterladen der Zoom Anwendung zu umgehen und an einem Meeting direkt von ihrem Browser teilzunehmen. Das ist eine Übergangslösung für Teilnehmer, die keine Anwendungen heruntergeladen, installieren oder ausführen können. Beachten Sie, dass das Meetingerlebnis vom Browser begrenzt ist.



Einen Link "Von Ihrem Browser teilnehmen" zeigen

Teilnehmern erlauben, das Herunterladen der Zoom Anwendung zu umgehen und an einem Meeting direkt von ihrem Browser teilzunehmen. Das ist eine Übergangslösung für Teilnehmer, die keine Anwendungen heruntergeladen, installieren oder ausführen können. Beachten Sie, dass das Meetingerlebnis vom Browser begrenzt ist.



Zoom: Datenschutzinformationen

- Bereitgestellte Datenschutzinformationen für öffentliche Stellen in Bayern ([Stabsstelle IT Sicherheit](#)):
 - Auftragsverarbeitung ist (noch) zusätzlich zur Bestellung etwa mit Hilfe dieser [Anleitung](#) abzuschließen
 - [Information gemäß Art. 13 DSGVO für bayerische staatliche Hochschulen](#)
 - [MusterVVT für Zoom](#)
- Andere Quellen:
 - [Datenschutzhinweise für Online-Meetings, Telefonkonferenzen und Webinare via „zoom“](#) (Datenschutz-Guru)

3. Nutzungshinweise

HfM Nürnberg

(AG Digitalisierung und Informationskompetenz)

Handreichung (pdf) für verschiedene Unterrichtsszenarien zur Unterstützungen der digitalen Lehre

- Bitte verwenden Sie bei online-Portalen und Software-Lösungen, die Sie für Ihre Tätigkeit an der HfM Nürnberg verwenden, stets Ihre HfM-Email-Adresse. Privater Unterricht sollte nicht über die HfM-EmailAdresse bzw. einen entsprechend für die HfM-Tätigkeit eingerichteten Account abgewickelt werden.
- Bitte beachten Sie, dass es in der Regel nicht funktioniert, wenn mehrere Videokonferenz-Plattformen bzw. -Programme parallel geöffnet sind, da ein gleichzeitiges Verwenden von Mikrofon und Kamera (auch im Standby-Modus) von einigen Programmen nicht zugelassen wird.
- Überprüfen Sie im Fall von Anmeldeschwierigkeiten auch die Sicherheitseinstellungen (Privacy Einstellungen) Ihres Browsers oder probieren einen alternativen Browser (Firefox, Chrome, Safari etc.).

LMU München

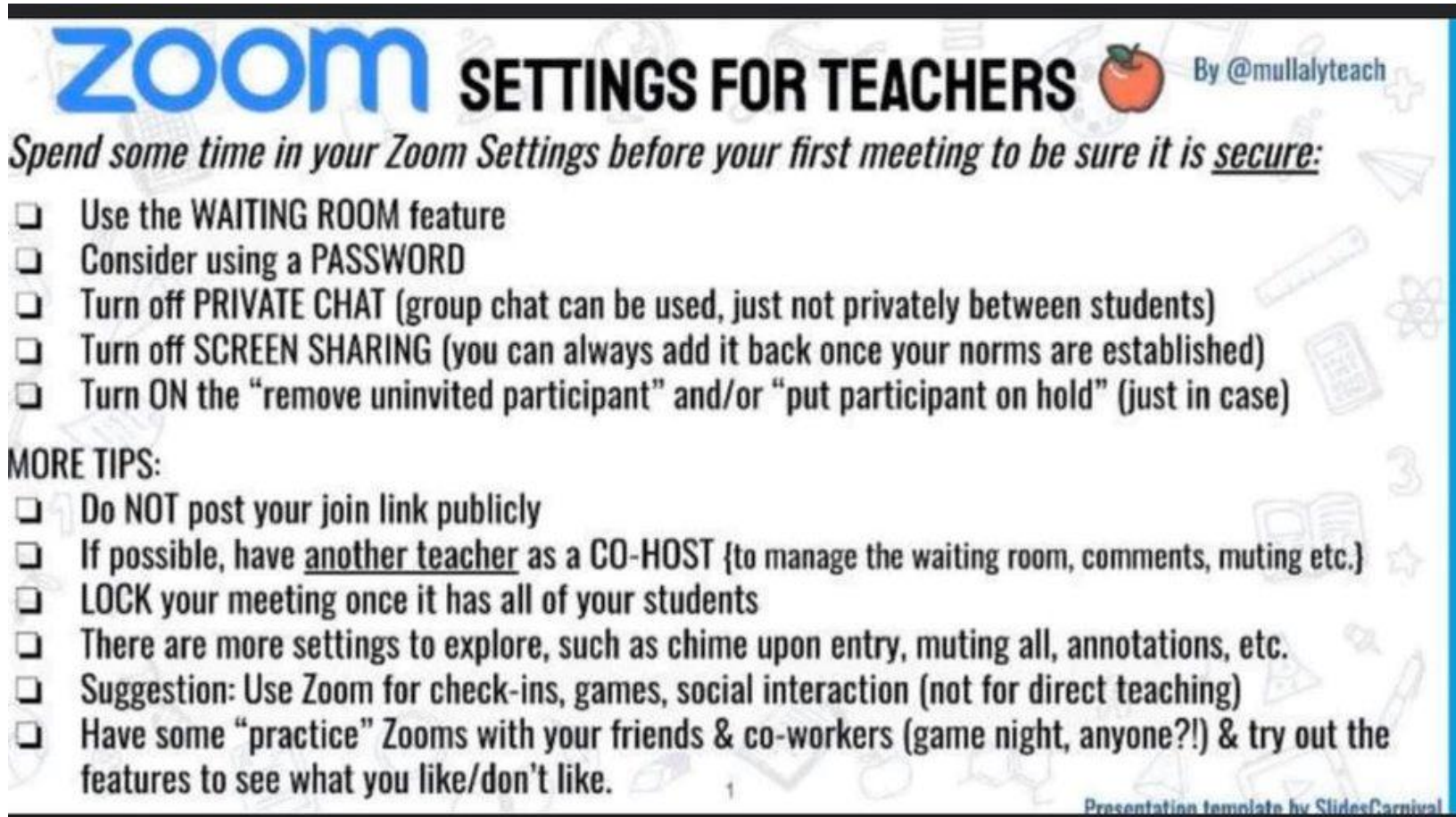
Nutzungsbedingungen, Datenverwendungshinweise und Datenschutzinformationen für die Verwendung von Zoom:

- Es sollten in der Regel keine Inhalte über diesen Dienst ausgetauscht werden, die einen hohen Schutzbedarf haben oder streng vertraulich sind. Ausgeschlossen ist die Nutzung, soweit besondere Kategorien personenbezogener Daten verarbeitet werden, z.B. Gesundheitsdaten.
- Der Dienst sollte in der Regel nicht für die Durchführung von Berufungsverfahren oder Bewerbungsgesprächen genutzt werden. Für diese Themen können Sie DFNconf oder andere als sicherer eingestufte Tools einsetzen.
- Für den Austausch von schützenswerten Dateien zwischen Teilnehmenden sollten in der Regel bestehende sichere Kanäle, z.B. Sync&Share, LMU-Teams oder gemeinsame Laufwerke, genutzt werden.
- Hochschulprüfungen sollten in der Regel nur in begründeten Ausnahmefällen über Zoom durchgeführt werden, insbesondere wenn andere geeignete Möglichkeiten nicht zur Verfügung stehen.

Uni Würzburg

- Bedingungen zur Nutzung von Zoom:
 - Vermeiden Sie bei der Anmeldung zur Konferenz als Teilnehmer die Nutzung des vollständigen Klarnamens. Geben Sie dazu ein Pseudonym ein.
 - Es ist nicht gestattet, innerhalb der Konferenz Dateien zwischen den Teilnehmern zu verschicken. Nutzen Sie zum Verteilen von Dateien die bei uns üblichen internen Mechanismen.
 - Vermeiden Sie die Diskussion personenbezogener Details in der Konferenz.
- Zoom - Datenschutzerklärung und Information zu Datenverarbeitung

Megan Mullaly

A presentation slide titled "Zoom SETTINGS FOR TEACHERS" with an apple icon and the text "By @mullalyteach". The slide includes a list of settings to check in Zoom, a section for more tips, and a footer with a SlidesCarnival watermark.

zoom **SETTINGS FOR TEACHERS**  By @mullalyteach

Spend some time in your Zoom Settings before your first meeting to be sure it is secure:

- ☐ Use the WAITING ROOM feature
- ☐ Consider using a PASSWORD
- ☐ Turn off PRIVATE CHAT (group chat can be used, just not privately between students)
- ☐ Turn off SCREEN SHARING (you can always add it back once your norms are established)
- ☐ Turn ON the “remove uninvited participant” and/or “put participant on hold” (just in case)

MORE TIPS:

- ☐ Do NOT post your join link publicly
- ☐ If possible, have another teacher as a CO-HOST {to manage the waiting room, comments, muting etc.}
- ☐ LOCK your meeting once it has all of your students
- ☐ There are more settings to explore, such as chime upon entry, muting all, annotations, etc.
- ☐ Suggestion: Use Zoom for check-ins, games, social interaction (not for direct teaching)
- ☐ Have some “practice” Zooms with your friends & co-workers (game night, anyone?!) & try out the features to see what you like/don't like.

1 Presentation template by SlidesCarnival

Kontakt/Ansprechpartner

Janet Amm

Datenschutzkoordinatorin

- Hochschulübergreifende Beratung der sechs bayerischen Kunsthochschulen in München, Nürnberg und Würzburg
- Syndikusanwältin (Zulassung beantragt)
- CIP - Certified Information Professional (AIIM, 2020)
- Zertifizierte Datenschutzschutzbeauftragte (IHK, 2019)
- Rechtsanwältin in Frankfurt am Main bei der Rechtsanwaltskanzlei White & Case LLP im Bereich Knowledge Management sowie Records & Information Governance (2003-2020)
- Juristisches Referendariat am Landgericht Darmstadt sowie bei Rechtsanwaltskanzlei Heller Ehrmann White & McAuliffe LLP, San Francisco (2001-2003)
- Juristische Mitarbeiterin der Staatswissenschaftlichen Fakultät an der Universität Erfurt (2000)
- Studium der Rechtswissenschaften an der Friedrich-Schiller Universität Jena, Masaryk-Universität Brno und Karls-Universität Prag (1994–2000)



Akademie der Bildenden Künste München
Akademiestraße 2-4
80799 München
Büro: E.O1.09
089/3852-2943
amm@adbk.mhn.de

**Vielen Dank für Ihre
Aufmerksamkeit!**