Datenschutzgerechte Videokonferenzen an Schulen

Hinweise der Datenschutzbeauftragten der öffentlichen Schulen im Regierungsbezirk Köln
Stand 12. Mai 2020

Einleitung

Bedingt durch die Schulschließungen im Rahmen der Maßnahmen zur Eindämmung der Corona-Ausbreitung in Deutschland haben viele Schulen den Unterricht behelfsmäßig mit Hilfe von Videokommunikation fortgeführt – auch und gerade entsprechenden Vorschlägen des Schulministeriums folgend. Zu den damit verbundenen Fragen des Datenschutzes haben die Datenschutzbeauftragten der öffentlichen Schulen im Regierungsbezirk Köln unter hohem Zeit- und Handlungsdruck die Schulen dabei beraten.

Mit diesem Papier soll die Thematik mit einigem Abstand nun grundlegender angegangen werden, um für die Zukunft datenschutzgerechte Praxislösungen entwickeln zu können. Nicht von den Datenschutzbeauftragten, sondern von anderer Seite im Bildungswesen sind jedoch soziale und pädagogische Fragen zu klären, die mit dem Einsatz von Videokommunikationswerkzeugen an Schulen verbunden sind.

Anwendungsanlässe für Videokonferenzen in Schule

In Zeiten des schrittweise wieder aufgenommenen Präsenzunterrichts werden die Anwendungsanlässe für Videokonferenzen im Unterricht sicherlich geringer werden. Jedoch wurden bereits in den letzten Jahren immer wieder Projekte durchgeführt, mit denen Schülerinnen und Schüler mittels Videoübertragung zum Beispiel im **Krankheitsfall von zu Hause oder dem Krankenhaus** aus am Unterricht teilnehmen konnten.

Eine andere Anwendung war und ist **internationaler Schüleraustausch** mit gegenseitigen virtuellen Besuchen im Klassenraum.

Videokommunikationslösungen können darüber hinaus die **Zusammenarbeit in Konferenzen und informellen Arbeitsgruppen** an Schulen bereichern – sowohl unter Kolleginnen und Kollegen als auch unter Schülerinnen und Schülern.

Es hat sich in den letzten Wochen auch gezeigt, dass Fortbildungs- und Beratungsformate mit Hilfe von Online-Werkzeugen sinnvoll und effizient durchgeführt werden können. Es ist daher abzusehen, dass Videokommunikation auch künftig für schulische Arbeit bedeutsam sein wird.

Kategorien von Videokommunikationswerkzeugen

Videokommunikationssysteme lassen sich grob in mehrere Kategorien mit teils zunehmender Komplexität der Funktionen, aber auch unterschiedlichen Einsatzschwerpunkten einteilen:

- **Videochatsysteme** bieten Gruppenunterhaltung mit Bildübertragung, meist für den Consumer-Bereich. Die maximal mögliche Teilnehmerzahl ist in der Regel kleiner als übliche Klassenstärken. Zu diesen Systemen zählen z.B. Skype, Facetime oder der Facebook-Messenger. Viele dieser Systeme bieten kostenlose Nutzung für Privatpersonen und eine kostenpflichtige Variante für Geschäftsanwendungen, die sie dann in die nächstfolgende Kategorie aufwerten.
- **Online-Kollaborationswerkzeuge mit integrierter Videokommunikation**. Derartige Systeme bieten Videomeetings für Mitglieder einer Organisation an. Manchmal können auch externe Teilnehmer zusätzlich eingeladen werden, was den Übergang zur nächsten Kategorie darstellt. Derartige Systeme gibt es als Cloud-Angebote internationaler Anbieter (z.B. Slack, Microsoft Teams), aber auch als Open-Source Projekte wie Nextcloud Talk, Kopano Meet oder Rocket.Chat, die auf eigenen Serverns betrieben werden können.
- **Videokonferenzsysteme,** manchmal auch als „Videomeetingsysteme“ bezeichnet, bieten gegenüber Videochatsystemen in der Regel eine größere Anzahl an Teilnehmenden und zusätzlich Werkzeuge zur Zusammenarbeit (Desktopübertragung, Präsentationen, gemeinsames Whiteboard usw.) und Integration in Kalendersysteme zur Planung von Meetings. Teilweise sind die Videokonferenzsysteme Komponenten übergeordneter „Unified Messaging-Systeme“, die die gesamte Unternehmenskommunikation einschließlich Telefonie, Mail usw. auf einer Systemplattform integrieren.
- **Webinarsysteme** erlauben die Durchführung des Unterrichts durch einen Lehrenden, beinhalten also Funktionen zur Steuerung von unterschiedlichen Rollen. Sie bieten vielfach auch für den Einsatz in Schulen nicht relevante Integration von Bezahlsystemen für die Durchführung kostenpflichtiger Veranstaltungen. Die Übergänge der Videokonferenzsysteme sind oft fließend. Webinaresysteme bieten häufig eine höhere maximale Teilnehmerzahl.
- **Fernwartungs- und Supportsysteme:** Eine Reihe von Systemen, die ursprünglich für Support- oder Helpdeskaufgaben konzipiert wurden, bieten mittlerweile auch Videoübertragungs- und somit auch Konferenz-/Meetingoptionen. Ihre Stärken - bzw. Besonderheiten – liegen in der Fähigkeit, entfernte Geräte steuern zu können. Videokommunikation und die Einbeziehung vieler Teilnehmenden ist für diese Anwendungen weniger relevant.

Da die Funktionalitäten für die jeweiligen Einsatzzwecke überschneidend sind, haben sich einige Werkzeuge zu einer Art „Schweizer Taschenmesser“ der Videokommunikation entwickelt. Viele Anbieter differenzieren die bereitgestellten Funktionalitäten teilweise über additive Preismodelle: die Preisskala beginnt z.B. mit der Bereitstellung von kostenlosen Grundfunktionen, die gegen Aufpreis erweitert werden können. Die Preispolitik hat jedoch auf Fragen des Datenschutzes eher geringe Auswirkungen, es sei denn, mit zusätzlich freigeschalteten Funktionen werden auch zusätzliche Datenverarbeitungen vorgenommen oder Sicherheitsoptionen – wie z.B. Wahl des Serverstandorts – angeboten.

Zu bedenken ist insbesondere bei den kostenlosen Grundangeboten, dass hierbei in der Regel keine Auftragsverarbeitung nach Artikel 28 DSGVO vereinbart werden kann.

Risiken für beteiligte Personen

Videomeetings, die durch Schule organisiert werden, finden im Verantwortungsbereich der Schule statt. Jedoch hat die Schule bei Teilnahmen von außerhalb des Schulgebäudes nur bedingt Kontrollmöglichkeiten. Folgende Risiken sind zu nennen:

Öffnen des privaten Lebensbereichs durch Audio- und Videoübertragung

Der Ort, von dem aus sich die Teilnehmenden an einem Videomeeting beteiligen, wird für den Einblick durch Dritte geöffnet. Dies ist häufig – in bestimmten Szenarien sogar überwiegend – der höchst private bzw. familiäre Lebensraum.

Teilnahme unerwünschter Personen

Es kann vorkommen, dass sich unerwünschte Personen Zutritt zu einem Meeting-Raum verschaffen, zum Beispiel, wenn ihnen die Zugangsdaten bekannt sind. Besonders einfach ist dies für Eltern oder Haushaltsmitglieder von Grundschulkindern, da Grundschulkinder die Zugänge vor ihren Bezugspersonen kaum geheim halten können. Im schlimmsten Fall können Erwachsene fremde Kinder während eines Schulmeetings kontaktieren. Dabei kann mittels Einspielung von Videoaufzeichnungen eine falsche Identität vorgetäuscht werden. In solchen Szenarien können Kinder im Extremfall Opfer von Straftaten werden.

Insbesondere muss verhindert werden, dass **Unbefugte die Kontrolle des Meetingraums übernehmen und die Lehrkraft aussperren können** („Kick-out"-Schutz für Gastgeber).

Aufzeichnen von Online-Meetings

Viele Meetingtools bieten die Möglichkeit der Aufzeichnung. Diese werden dann entweder auf dem lokalen Gerät des Aufzeichnenden oder in der Cloud des Anbieters gespeichert.

Aber selbst wenn das verwendete Tool diese technischen Möglichkeiten nicht bietet, kann der Bildschirm einfach mit einer Kamera, z.B. eines Smartphones, abgefilmt werden. Auf die Art und Weise entstehen nicht autorisierte Aufnahmen, die im Extremfall kompromittierend verbreitet werden können.

Einbringen kinder- und jugendgefährdender Inhalte

Praktisch alle Videokonferenzsysteme bieten die Möglichkeit, Inhalte zu teilen. Inhalte können der eigene Desktop, Anwendungsfenster oder Dateien aller Art sein. Auf diese Weise können Gewaltdarstellungen, rassistische Propaganda, Pornografie usw. an die Kinder/Jugendlichen herangebracht werden. Dasselbe gilt auch für das Einspielen anstößiger Geräusche und Live-Kamerabilder (oder über eine Kameraschnittstelle eingespielte Videoinhalte).

Mitschauen und -lauschen aus dem Hintergrund

Im toten Winkel der Kamera können sich weitere Personen aufhalten, die auf diese Weise Einblick in die Kommunikation bekommen.

Mobbing – auch in integrierten Chats des Systems

Sowohl die Werkzeuge der internen Kommunikation – z.B. Chats – als auch die übermittelten Inhalte, z.B. Wohnungseinrichtungen, durch das Bild gehende Personen usw., können Anlass zu diffamierender oder beleidigender Kommunikation, letztlich zu Mobbing, geben.

Datensammlung durch Dienstanbieter

Personenbezogene Daten der Nutzer – in der Regel Metadaten und weniger häufig Inhaltsdaten – können dem Anbieter des Dienstes bekannt werden, der diese wiederum z.B. für Werbezwecke weitergeben kann. Entsprechende Hinweise müssen in den Datenschutzbestimmungen des Dienstes aufgeführt sein.

Informierte Einwilligungen als Nutzungsvoraussetzung

Erfordernis der Einwilligung

Gemäß Anlage 1 zur VO-DV-I ist die Verarbeitung von Fotos und analog dazu auch von Videoaufnahmen von Schülerinnen und Schülern durch Schulen nur auf Basis einer Einwilligung zulässig. Dies gilt analog auch für Lehrkräfte. **Alle Beteiligten sind dabei unbedingt auch über die Risiken (s.o.) zu informieren.**

Diese Voraussetzung **könnte** nur dann entfallen, wenn die Durchführung einer Videokonferenz zur Erfüllung des Bildungs- und Erziehungsauftrags der Schule im Einzelfall **nach strengen Maßstäben erforderlich wäre**. Da dies kaum zu begründen sein dürfte, kann eine Teilnahme an einer Videokonferenz derzeit weder für Lehrende noch für Lernende angeordnet, sondern nur auf der Basis informierter Einwilligungen durchgeführt werden.

Umfang und Form der Einwilligung

Es gelten die Vorschriften gemäß Artikel 7 DSGVO (https://dsgvo-gesetz.de/art-7-dsgvo/) und die Informationspflichten nach Artikel 13 DSGVO (https://dsgvo-gesetz.de/art-13-dsgvo/). Letztere müssen sowohl die Schule als auch der Diensteanbieter – er ist hier Auftragsverarbeiter (s.u.) – in gemeinsamer Verantwortung sicherstellen.

Für die Einwilligung Minderjähriger gilt darüber hinaus Artikel 8 DSGVO (https://dsgvo-gesetz.de/art-8-dsgvo/). Hieraus geht hervor, dass bei Kindern und Jugendlichen unter 16 Jahren die Erziehungsberechtigten die Einwilligung erteilen müssen.

Dies ist jedoch diskutabel, wenn die teilnehmenden Schülerinnen und Schüler die Videoübertragung von ihrem Gerät aus deaktivieren können, bzw. wenn die Videoübertragung aktiv eingeschaltet werden muss.

In Anbetracht der besonderen Risiken ist eine **konkludente Einwilligung durch Teilnahme aus hiesiger Sicht nicht ausreichend**, insbesondere da bei Teilnahme durch jüngere Schülerinnen und Schüler keine konkludente Einwilligung der Erziehungsberechtigten angenommen werden kann.

Schulische Nutzungsbedingungen und -verpflichtungen

Wie oben aufgeführt gibt es Gefahren, die nicht technischer Natur sind, sondern organisatorischer Regelungen in Form von Anweisungen bzw. Nutzungsbedingungen bedürfen. Die folgende Aufzählung ist als minimal einzuhaltender Kriterienkatalog zu verstehen:

- Die Sessions werden **nicht aufgezeichnet**, außer alle Beteiligten haben der Aufzeichnung und dem Verwendungszweck der Aufzeichnung ausdrücklich zugestimmt. Für Aufzeichnungen sind grundsätzlich dieselben Regelungen anzuwenden, wie für Unterrichtsmitschnitte. **Zur Beachtung**: Die Aufzeichnungsfunktionen der Videokonferenzsysteme speichern die Daten je nach Vertrag und Einstellung auf lokalen Geräten oder in der Cloud des Anbieters.
- Alle Teilnehmenden werden zu Beginn des Meetings und danach auch fortlaufend identifiziert.
- Alle Teilnehmenden verpflichten sich, Maßnahmen einzuhalten, mit denen verhindert wird, dass Unbefugte Einblick auf den Bildschirm bekommen und/oder mithören können (in der Regel bedeutet dies, dass die Teilnehmenden alleine in einem Raum sind, was insbesondere bei jüngeren Kindern schwierig umzusetzen sein dürfte).
- Alle Teilnehmenden achten darauf, dass keine anstößigen Bilder (z.B. im Hintergrund der Kamera) oder unangemessene Geräusche übertragen werden.
- Erwachsene (außer die zuständigen Lehrkräfte) kontaktieren keine fremden Kinder über die bereitgestellten Systeme.
- Alle Beteiligten achten auf eine angemessene professionelle Distanz und „Netiquette“.
- Für Beanstandungen werden Ansprechpartner benannt. Insbesondere sollen Kinder angehalten werden, auf merkwürdige Situationen angemessen zu reagieren und die Vertrauenspersonen einzuschalten.
- Schulen führen nur dann Videomeetings durch, wenn die Lehrkräfte eine sachgemäße Nutzung insbesondere zur Abwehr der oben genannten Risiken sicherstellen können.

Verantwortung der Schulleitung nach Artikel 32 DSGVO

Nach Artikel 32 DSGVO steht die Schule in der Verantwortung, ein angemessenes Sicherheitsniveau der Datenverarbeitung zu gewährleisten. Hierbei ist eine Balance zwischen den Umständen der Verarbeitung, ihren Zielen, der möglichen Gefährdungen (Eintrittswahrscheinlichkeit, Schwere der Risiken) und dem zu betreibenden Aufwand herzustellen. Es heißt wörtlich:

„(1) *Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten* (…)“

Besondere Umstände in Zeiten von angeordneten Schulschließungen oder eingeschränkten Schulbetriebs

Durch die staatlich praktisch von einem Tag auf den anderen[1] angeordneten Schulschließungen sind Umstände eingetreten, unter denen eine notbehelfsmäßige Durchführung des Unterrichts als prioritär gegenüber Bedenken bei der Auswahl der Anbieter angesehen werden kann, soweit die Maßnahmen mit marktgängigen Produkten durchgeführt werden und die Teilnehmer einige grundsätzliche Verhaltensregeln beachten[2].

Dies darf jedoch kein Dauerzustand sein und diese Ausnahmesituation darf nicht zu einer Erosion des Grundrechts auf informationelle Selbstbestimmung und der Datensicherheit führen, sodass bei künftiger Nutzung von Videokonferenzen in einem sich wieder normalisierenden Alltag strenge Maßstäbe an die Wahl der Anbieter anzulegen sind.

Dies gilt insbesondere mit Verfügbarkeit von für die Schulen kostenlos verfügbaren Systemen, die speziell für die Anforderungen von Schulen öffentlich, d.h. durch die zuständigen kommunalen Träger bzw. von Landeseinrichtungen bereitgestellt werden.

Endgeräte für die Nutzung durch Lehrkräfte

Die Nutzung privater ADV-Geräte für dienstliche Zecke, die mit der Verarbeitung personenbezogener Daten verbunden sind, bedarf einer Genehmigung durch die Schulleitung. Der Umfang der genehmigungsfähigen Daten für die Verarbeitung auf privaten Geräten ist in Anlage 3 zur VO-DV-1 festgeschrieben.

Die Durchführung von videogestütztem Unterricht ist hieraus nicht unmittelbar zu rechtfertigen. Zwar dürfen bei Vorliegen einer entsprechenden Genehmigung Anwesenheits- und Leistungsdaten von Lernenden verarbeitet werden, jedoch muss die Situation für den Empfang von Bilddaten skeptisch beurteilt werden.

Relativ problemlos kann eine rein passive Teilnahme von Lernenden mit deaktivierter Kamera (und streng genommen auch ausgeschaltetem Ton) gerechtfertigt werden, die aktive Einbringung in das Unterrichtsgeschehen kann dagegen nur auf der Basis einer informierten Einwilligung geschehen – wobei „informiert“ hier bedeutet, dass die Lernenden

[1] Die Bekanntgabe der Schulschließungen in NRW erfolgte am Freitag, den 13. März 2020, nachmittags nach Schulschluss mit Wirkung zu Montag, den 16. März 2020.

[2] Die LDI-NRW hat sich hierzu noch nicht geäußert. Die beschriebene Einschätzung wird explizit vom Landesbeauftragten für Datenschutz und Informationsfreiheit des Landes Rheinland-Pfalz geteilt. (https://www.datenschutz.rlp.de/de/themenfelder-themen/videogestuetzte-kommunikationstechnik/)

Wissen müssen, dass die Lehrkraft ein privates Gerät verwendet, und auch genau darin einwilligen. Ob dies mit dem Grundsatz der Freiwilligkeit vereinbar ist, kann zumindest bezweifelt werden, da bei Nicht-Teilnahme Nachteile nicht auszuschließen sind – zumindest in der Wahrnehmung der Betroffenen.

Die Nutzung privater Endgeräte für Videokonferenzen mit Schülerinnen und Schülern sollte daher – mit Ausnahme des Vorliegens besonderer Umstände z.B. bei Schulschließungen in deren Folge Lehrkräfte keinen Zugang zu dienstlichen Geräten haben – unterbleiben.

Wahl eines Anbieters/Dienstleisters/Hosters für Videokonferenzen

Obwohl grundsätzlich die Möglichkeit besteht, ein Videokonferenzsystem auf eigenen Servern der Schule zu betreiben, ist hiervon im Allgemeinen abzuraten, da Administration und Betrieb große Sachkenntnis erfordert und ständige Aktualisierungen des Servers vonnöten sind. Deutlich effizienter – und auch in der Regel technisch sicherer – ist der Betrieb bei einem spezialisierten Unternehmen als Auftragsverarbeiter[3].

Für Auftragsverarbeitungen gelten die Anforderungen aus Artikel 28 DSGVO (https://dsgvo-gesetz.de/art-28-dsgvo/). Zu empfehlen ist ein Unternehmen mit einem Geschäftssitz in Deutschland und einer Verarbeitung der Daten innerhalb der EU. Hierdurch ist gesichert, dass die Anforderungen des Datenschutzes auch tatsächlich durchgesetzt werden können.

Gerade im Bereich der professionellen Videokonferenzsysteme wird jedoch oft global kommuniziert. Von daher sind Anbieter gerade der „großen“ Systeme entsprechend auf global kommunizierende Kundschaft eingestellt, die Standorte in verschiedenen Kontinenten betreibt. Die Anbieter von Videokommunikationssystemen betreiben in der Regel ihre Angebote auch nicht in eigenen Rechenzentren, sodass Unterauftragnehmer mit weltweit verteilten Verarbeitungsorten eingesetzt werden.

Rechtlich ausgeschlossen sind Unternehmen in Drittstaaten und Datenverarbeitung außerhalb der EU nicht, jedoch gibt es bei Datenverarbeitungen außerhalb der EU keine unmittelbar wirksame Kontrolle durch die hiesigen Aufsichtsbehörden. Die Zulässigkeit ist von geeigneten Garantien wie einem Angemessenheitsbeschluss der EU-Kommission (Artikel 45 DSGVO) oder der Inkludierung geeigneter Garantien nach Artikel 46 DSGVO (z.B. von EU-Standardvertragsklauseln) abhängig.

Bei internationalen Organisationen, die Daten außerhalb der EU verarbeiten oder verarbeiten lassen, ist also trotz grundsätzlich unter den genannten Voraussetzungen möglicher Zulässigkeit generell Vorsicht geboten.

Open-Source oder proprietär / CLosed-Source?

[3] Steht den Schulen jedoch eine professionell betreute Infrastruktur z.B. durch ein qualifiziertes Rechenzentrum zur Verfügung, kann eine „on-premise“ Bereitstellung aus Sicht des Datenschutzes sinnvoll sein. Dringend abzuraten ist jedoch die Annahme von Angeboten hilfsbereiter Eltern entsprechende Systeme aufzusetzen, da diese hierdurch administrativen Zugriff auf schulische Datenverarbeitung bekämen.

Im Bereich der Videokonferenzen gibt es neben den Komplettangeboten entsprechender Anbieter auch Open-Source-Lösungen, die die schulischen Anforderungen erfüllen. **Zu beachten ist aber auch bei diesen Lösungen, dass eine grundsätzlich datenschutzgerecht einsetzbare Software keinen Automatismus für die Bereitstellung eines datenschutzgerechten Diensts darstellt.** Der technische Betreiber muss zusätzlich z.B. das Produkt datenschutzgerecht konfigurieren, regelmäßige Updates einspielen usw. Auch ist bei Verwendung von über einen Dienstleister bereitgestellten Open-Source-Lösungen eine Vereinbarung zur Auftragsverarbeitung nach Artikel 28 DSGVO erforderlich.

Wahl eines Produkts

Aus Sicherheitsgründen sollte ein Videokonferenzsystem folgende Eigenschaften bieten:

- **Verschlüsselung**: Ideal wäre eine Ende-zu-Ende-Verschlüsselung, damit niemand auf dem Weg der Daten (auch nicht der technische Betreiber des Systems) diese zur Kenntnis nehmen kann. Technisch ist dies jedoch nicht möglich bei Diensten, die einen Netzübergang vom Telefon- in ein IP-Netz („Telefoneinwahl“) oder eine Aufzeichnung direkt in der Cloud des Anbieters ermöglichen. Schwierig ist dies zudem bei Meetings mit mehr als zwei Teilnehmenden[4]),
- **Verifizierung der Identität der Teilnehmer**: bei Eintritt in den Unterrichtsraum muss sichergestellt werden können, dass es sich tatsächlich um die Person handelt, für die sie sich ausgibt. Dies kann auf mehrere Arten geschehen, zum Beispiel:
    - Accounterfordernis im System (funktioniert z.B., wenn die Video-kommunikation integrierter Teil einer schulischen Cloud-Lösung, eines Lern-managementsystems oder eines anderen Systems mit Zugangskontrolle ist),
    - Einladungszwang zur Konferenz,
    - Passwortschutz der Konferenz,
    - Virtueller Warteraum: der Moderator muss Teilnehmende explizit „einlassen“.

  Achtung: eine 100%-ige Sicherheit ist jedoch nie zu erreichen!
- Rollenbasiertes Management der Teilnehmenden: „Kick-out“-Schutz für die Gastgeber.
- Datenspeicherung: Sicherheitszertifizierte Speicherung aller ruhenden Daten, **keine Speicherung von Kommunikationsinhalten**.

Ergänzend erscheinen folgende Funktionen – teilweise mit Aspekten des Datenschutzes, teilweise zur Verbesserung der Nutzerfreundlichkeit und der Nutzbarkeit – wünschenswert.

- Einfache Bedienung für Lehrende und Lernende,
- Unkenntlichmachung des Bildhintergrunds („Verschwimmen“) oder Einblendung virtuelle Hintergründe,
- Funktionen zur Freigabe von Dateien, des Desktops, einzelner Anwendungen oder von angeschlossenen Mobilgeräten (meist iPhone/iPad),
- Moderationsfunktionen: Chat, Umfrage, shared Whiteboard, Ermöglichen/Verhindern des Teilens von Inhalten durch Teilnehmerinnen und

[4] Als Beispiel für die eingeschränkte Ende-zu-Ende Verschlüsselung kann das Open-Source-System Jitsi dienen. Die Einschränkung ist explizit dokumentiert: https://github.com/jitsi/jitsi-meet/wiki/Jitsi-Meet-Encryption

Teilnehmer, zentrales mute/unmute, Übergabe der Moderatorenrolle an Teilnehmer, „Breakout-rooms“ (vorübergehende Aufteilung in Teilgruppen) usw.,
- Möglichkeit der Nutzung im Browser ohne zusätzlich erforderliche Software (erleichtert unter anderem die Administration der Rechner, reibungslose Funktion ist jedoch vom Browser abhängig, der das Protokoll WebRTC unterstützen muss),
- Nutzung auf allen gängigen Mobil- und Desktop-Plattformen möglich (hierdurch wird niemand von der Teilnahme ausgeschlossen). Manche Systeme sind auf Mobilplattformen funktional eingeschränkt.

Darüber hinaus müssen auch finanzielle Aspekte berücksichtigt werden. Hierzu gibt es folgende Abrechnungsmodelle auf dem Markt:

- **Kostenlos**: vollständig kostenlos und spontan nutzbare Angebote (Achtung: bei Nutzung dieser Angebote ist keine Auftragsverarbeitung nach Artikel 28 DSGVO möglich – aber sie ist streng genommen erforderlich).
- „**Freemium**“: eingeschränkte Grundfunktionen sind kostenlos verfügbar; Erweiterungen werden nach einem der folgenden Modelle abgerechnet. Oft sind bei derartigen Angeboten die Serverstandorte unklar und es finden anderweitige Verwertung von Nutzerdaten statt.
- **Integriert**: In einem anderen System integriert (kostenlos oder gegen Aufpreis).
- **Miete**: Das System steht jederzeit für die gebuchte Anzahl von Hosts/Räumen für den Mietzeitraum (meist Monat oder Jahr) zur Verfügung. Durch dieses Modell wird die Anzahl der gleichzeitig nutzbaren Konferenzen (nämlich durch die Anzahl der gemieteten Hosts) beschränkt.
- **Kauf**: dauerhafte Bereitstellung eines Raums/Hosts gegen Einmalgebühr (plus obligatorischem Jahresvertrag für Softwarewartung).
- „**Concurrency**“ – Abrechnung nach Zeit: bei diesem Modell wird die Anzahl Minuten abgerechnet. Dabei können auch mehrere Konferenzen parallel stattfinden; die Zeiten addieren sich in diesem Fall einfach zu der abzurechnenden Gesamtzeit. Derartige Angebote sind auch als Prepaid verfügbar.
- **Werbefinanziert**: durch Werbung finanzierte Angebote sind **für die schulische Nutzung ausgeschlossen**, da die Datenverarbeitung auch Zwecken der Werbetreibenden dient.

Steckbrief Videokonferenzsystem: _____ (Name)

Anbieter, Geschäftsadresse	
Website URL	
Unterauftragnehmer (technischer Dienstleister)	
Verwendete Software auf dem Server	( ) eigenes System des Anbieters ( ) Proprietär: _____ ( ) Open-Source: _____
Abrechnungsformen / Preise	( ) kostenlose Version ( ) in folgendem Dienst integriert: _____ ( ) zeitlich befristete Miete ( ) dauerhafter Kauf eines Raums durch Einmalzahlung
Nachweis Datenschutzniveau	( ) nach DSGVO ( ) EU-US-privacy shield ( ) andere: _____
Vertragsgestaltung	( ) Auftragsverarbeitung nach Art. 28 DSGVO
Zugriff über:	( ) Webbrowser Eigene Software für: ( ) Windows, ( ) Mac ( ), iOS, ( ) Android, ( ) Linux
Userzugang und Identifikation (Einstellmöglichkeiten)	( ) auf User mit Account im System beschränkbar ( ) Zutritt mit Einladung (z.B. via Email) ( ) Zutritt ohne Account über URL mit Warteraum ( ) Zutritt ohne Account über URL mit Passwort ( ) Schließen des Raums durch Moderator
Privatsphäre	( ) Bildhintergrund verschwimmen ( ) virtuelle Hintergründe
Funktionen zum Teilen	( ) Präsentationen zeigen (z.B. pptx) ( ) Desktop zeigen ( ) Wahl des Desktops bei mehreren Monitoren ( ) einzelne Anwendungsfenster teilen ( ) an Präsentations-PC angeschlossenes iPad / iPhone teilen ( ) Dateien / Dokumentenaustausch
Zusammenarbeit und Kommunikation	( ) Hand heben (virtuelles „Aufzeigen“) ( ) Chat ( ) Umfrage / Feedback ( ) Breakout Rooms ( ) Dokumente gemeinsam bearbeiten
Moderationsfunktionen	( ) Schutz des Gastgebers des Raums vor „Kick-out“ ( ) Meeting-Rechte und Ansichten für TN einstellbar ( ) TN stumm schalten (mute/unmute) ( ) Moderatorenrolle an TN zuweisen ( ) Bildschirm holen und weiterteilen ( ) Fernsteuerung von TN-Geräten
Aufzeichnen von Sitzungen	( ) keine Aufzeichnung möglich ( ) Aufzeichnen kann wirksam unterbunden werden (außer Abfilmen) ( ) Aufzeichnen mit lokaler Speicherung ( ) Aufzeichnen mit Speicherung in Anbieter-Cloud
Anmerkungen	