Landesbeauftragte
für Datenschutz und Informationsfreiheit
Nordrhein-Westfalen

Leitplanken für die Auswahl von Videokonferenzsystemen während der Kontaktbeschränkungen aufgrund der Corona-Pandemie

Stand: 14.08.2020

Wir empfehlen Unternehmen, Behörden und anderen Organisationen, bei der Entscheidung für ein Videokonferenzsystem wie folgt vorzugehen:

Wenn Sie Videokonferenzen beruflich einsetzen müssen, haben Sie die Wahl zwischen einem Online-Dienst (SaaS, Software-as-a-Service) oder einer in eigener Verantwortung betriebenen Lösung (On-Premises-Lösung). Wird eine Videokonferenzsoftware selbst bereitgestellt, wurden in der Regel unternehmens- oder behördenintern eine Erforderlichkeits- und Risikobetrachtung durchgeführt und ein entsprechendes Konzept erstellt, wie beispielsweise mit Meta-, Protokoll- und Analysedaten umgegangen wird oder welche Funktionen für die Teilnehmenden verfügbar sind. Diese Lösung erlaubt dem Unternehmen oder der Behörde mehr Kontrolle über die Datenverarbeitung als bei einem Online-Dienst.

Prüfen Sie daher zunächst,

1. ob es Ihnen mit verhältnismäßigem Aufwand möglich ist, einen eigenen Dienst mit öffentlich verfügbarer oder kommerziell erhältlicher Software bereitzustellen. Stellen Sie dabei sicher, dass die eingesetzte Software keine Daten über Ihre Beschäftigten oder deren Kommunikationspartner/-innen an den Hersteller für dessen Zwecke übermittelt.

Wenn Sie keine Software im eigenen Netz nutzen können und die Videokonferenz über einen Online-Dienst realisieren, prüfen Sie,

2. ob die Lösung eines Anbieters mit Sitz im Europäischen Wirtschaftsraum (EWR) oder aus einem Land mit gleichwertigem Datenschutzniveau (https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en - Die Entscheidung für die USA zum Privacy Shield ist ungültig (Europäischer Gerichtshof C-311/18).) möglich ist. Einige deutsche Anbieter sind z. B. in dem Artikel „Mögliche Alternativen für Softwarenutzung“ (Stand 30.03.2020) von Herrn R. Schulze (DIHK) unter https://www.digitales-kompetenzzentrum-kiel.de/homeoffice.html aufgeführt. Die Vertragsgestaltungen der dort genannten Anbieter können wir aus Kapazitätsgründen nicht überprüfen.

   Prüfen Sie des Weiteren, ob der Anbieter

   a) vertrauenswürdig ist,

   b) ausreichende Datensicherheit (zum Beispiel durch Zertifizierung) nachweisen kann und

c) Ihnen die Verschlüsselung der Datenübertragung garantiert (es sollte mindestens eine Transport-Verschlüsselung der gesamten Kommunikation gewährleistet werden; je nach Ergebnis der Datenschutz-Folgenabschätzung kann bei der Übermittlung besonders schutzbedürftiger Informationen auch eine Ende-zu-Ende Verschlüsselung erforderlich sein).

Fällt die Prüfung positiv aus, dann

d) schließen Sie einen ordnungsgemäßen Auftragsverarbeitungsvertrag mit dem Anbieter (Art. 28 Abs. 3 DS-GVO)

und stellen Sie sicher, dass der Betreiber

e) keine Angaben über Schülerinnen und Schüler, Studierende, Beschäftigte oder anderen Nutzer und deren Kommunikation oder über die Nutzung der Software für eigene Zwecke verarbeitet, sowie

f) Unterauftragnehmer mit Sitz außerhalb des EWR für die Bereitstellung des Videokonferenzdiensts nur einsetzt, wenn der Datenexport die Anforderungen des Kapitel V der Datenschutz-Grundverordnung erfüllt.

Bitte beachten Sie, dass ein Datenexport auch dann vorliegt, wenn der Dienstleister aus dem Drittland heraus auf in der EU gehaltene Daten zugreift (z.B. zu Wartungs- und/oder Supportzwecken).

Darüber hinaus ist zu beachten, dass Strafverfolgungsbehörden in den USA auf Grundlage eines US-amerikanischen Gesetzes („US-Cloud Act“) ermächtigt werden, unter bestimmten Umständen auch auf Daten zuzugreifen, die US-amerikanische Dienstleister in der EU halten. Für solche Datenübermittlungen müssen ebenfalls die Anforderungen des Kapitel V der DS-GVO umgesetzt werden. Insoweit ist zu erwarten, dass bei Datenanforderungen nach PATRIOT Act und CLOUD Act kein Rechtshilfeabkommen angewandt wird. Für die Datenübermittlung an US-amerikanische (Strafverfolgungs-)Behörden bzw. deren Zugriff auf in der EU gehaltene Daten kommen dann nur die Ausnahmeregeln nach Artikel 49 in Betracht. Die Rechtmäßigkeit solcher Übermittlungen kann daher nicht allgemein festgestellt werden.

Zur Umsetzung der Anforderungen aus Kapitel V der DS-GVO können z.B. mit dem Unterauftragnehmer zusätzlich die sogenannten EU-Standardvertragsklauseln der EU-Kommission abgeschlossen werden (https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32010D0087). Dies kann der Anbieter für Sie tun, wenn Sie ihn dazu bevollmächtigen.

Allerdings müssen die Verwender dieser Klauseln selbst prüfen, ob diese Garantien ausreichend sind oder durch weitere Maßnahmen ergänzt werden müssen – besonders, wenn im Ziel-Land schlechte Datenschutzbedingungen herrschen. Der Europäische Gerichtshof hat für die USA auf mögliche Behördenzugriffe hingewiesen (EuGH C-311/18), die weitere Maßnahmen erfordern. Werden solche Maßnahmen nicht getroffen, reichen die Standardvertragsklauseln nicht aus.

3. Wenn Sie statt eines Anbieters gemäß Ziff. 2 einen Anbieter mit Sitz außerhalb des EWR oder eines Landes mit gleichwertigem Datenschutzniveau beauftragen wollen, sollten Sie ebenfalls sicherstellen, dass die Anforderungen aus Kapitel V der DS-GVO umgesetzt werden, s. o. Ziffer 2.f). lit. f).

Nicht datenschutzgerechte Lösungen, die aufgrund der Einführung der Kontaktbeschränkungen von Ihrer Institution kurzfristig eingesetzt wurden, sollten so bald wie möglich abgelöst werden.

Hinweise für den datenschutzfreundlichen Einsatz verschiedener Funktionen von Videokonferenzen:

Wenn Sie Videokonferenzen spontan einsetzen müssen, um mit Ihren Kolleginnen und Kollegen, Schülerinnen und Schülern, Studierenden, Mitgliedern usw. während der physischen Kontaktsperre zumindest digital im Kontakt zu bleiben, und noch keine konzeptionelle Grundlage für diese Verarbeitungstätigkeit haben, können Sie zusätzlich kurzzeitig die im Folgenden beschriebenen Hinweise verwenden, um wichtige Anforderungen an die Datenschutzkonformität bei Videokonferenzen umzusetzen.

Mittel- und langfristig ist es aber grundsätzlich notwendig, eine der Datenverarbeitung angemessene Erforderlichkeits- und Risikobetrachtung durchzuführen, auf deren Basis eine geeignete Videokonferenz-Lösung auszuwählen sowie technische und organisatorische Maßnahmen zu Datenschutz und Datensicherheit festzulegen und zu dokumentieren.

- **Als organisierende Person** sollten Sie die Verwendung der angebotenen Funktionen daraufhin überprüfen, ob eine datenschutzfreundliche Voreinstellung möglich ist, z. B.:

  - Aufnahme/Speicherung einer Videokonferenz („Protokoll“, „Archivierung“)
    Auf die Nutzung von Aufnahmefunktionen, die den Verlauf der Videokonferenz in Ton und Bild aufzeichnen, sollte verzichtet werden. Es gibt in der Regel datenschutzfreundlichere Lösungen als eine umfangreiche Aufzeichnung von Wort und Bild inklusive Gestik und Mimik, z. B. schriftliche Protokolle, wie sie auch in nicht-elektronischen Meetings zum Einsatz kommen. Bei einer Speicherung/Archivierung müssen u. a. Zugriffsberechtigungen, Löschfristen und die Wahrung der Betroffenenrechte gewährleistet werden. Die Risiken im Zusammenhang mit der Speicherung und die möglichen technischen und organisatorischen Maßnahmen müssen im Vorfeld betrachtet und festgelegt werden.

  - Integration von sozialen Medien
    Verzichten Sie möglichst auf die Einbindung von Social-Media-Inhalten. Falls Sie darauf nicht verzichten wollen, achten Sie zumindest darauf, dass Sie keine sensiblen Daten anderer Personen offenlegen.
    Achtung: Einige Videokonferenz-Dienste nehmen automatisch Kontakt zu Social-Media-Plattformen auf – das ist jedoch in der Regel weder nötig noch gewollt.

  - Aufmerksamkeitsanzeige
    Einige Videokonferenz-Lösungen bieten Aufmerksamkeitsanzeigen an, die es ermöglichen sollen, zu erkennen, ob Teilnehmende der Videokonferenz folgen. Diese Überwachung ist ein Eingriff in die Persönlichkeitsrechte der Teilnehmenden! Aktivieren Sie die Funktion nur, wenn es zwingend notwendig ist, z. B. bei Online-Seminaren mit Teilnahmenachweis. Auf jeden Fall müssen

Sie darüber vorab informieren und ggf. vorherige Einwilligungen bei den Betroffenen einholen.

- Passwortschutz/Anklopfen
  Wenn die Videokonferenz-Lösung die Möglichkeit bietet, einen Konferenzraum zu sperren und eine Teilnahme erst nach einer Eingabe eines Passworts bzw. nach einem „Anklopfen“ (auch: Warteraum) und Freigabe der Teilnahme durch die Moderation zu erlauben, empfehlen wir, diese Funktion zu verwenden. Damit können Sie erreichen, dass nur berechtigte Personen an Ihrer Videokonferenz teilnehmen.

- Um die Transparenz der Datenverarbeitung in Ihrer Videokonferenz zu gewährleisten bzw. die Teilnehmenden über die Verwendung ihrer Daten zu informieren, sollten Sie

  - den Teilnehmenden Ihrer Videokonferenz die Möglichkeit geben, Ihre Datenschutzerklärung oder Datenschutz-Kurzinformation einzusehen oder herunterzuladen, oder

  - den Teilnehmenden Ihrer Videokonferenz die datenschutzfreundliche Verwendung der Funktionen vor Beginn der Videokonferenz zu erläutern oder die Chatfunktion zu benutzen, um die datenschutzrelevanten Informationen dort bereitzustellen.

  - Sollten Sie Funktionen verwenden, mit denen ein erhöhtes Risiko verbunden ist (Aufnahme, Aufmerksamkeitsanzeige, kein Passwortschutz usw.), informieren Sie darüber deutlich im Vorfeld und holen Sie ggf. vorherige Einwilligungen bei den Betroffenen ein.

- Überlegen Sie, ob Sie die Identität der Teilnehmenden der Videokonferenz prüfen müssen, um zu gewährleisten, dass keine Unbefugten teilnehmen. Bei der Verwendung eines komplexen Passworts beim Zugang kann dies bereits sichergestellt sein.

- Bereiten Sie sich auf mögliche Datenschutz-Probleme vor, die im Laufe der Videokonferenz auftreten können, z. B.:

  - Überlegen Sie sich Ihre Reaktion als Moderation, wenn einzelne Teilnehmende unerlaubt personenbezogene Daten verwenden oder veröffentlichen.

  - Bereiten Sie einen Plan B vor, falls technische Probleme auftauchen – beispielsweise eine Terminverschiebung oder das Ausweichen auf eine Telefonkonferenz.

- Falls die Videokonferenz nicht durch ein Passwort o. ä. geschützt ist, sollten Sie schnell reagieren, falls eine unberechtigte Person an der Konferenz teilnimmt.

- **Als teilnehmende Person** sollten Sie

  - vor Beginn der Videokonferenz überprüfen, welche Funktionen die Videokonferenz-Software zur Verfügung stellt und ob Funktionen deaktiviert wurden, z. B. ausgegraut oder entsprechend markiert, oder ob bestimmte Voreinstellungen bei den Funktionen vorgenommen wurde, z. B. ausgeschaltete Kamera oder ausgeschaltetes Mikrofon,

  - die Funktionen testen, mit denen Sie Ihre Privatsphäre schützen können, um sie während der Videokonferenz sicher verwenden zu können, z. B. Deaktivierung von Ton und/oder Bild,

  - sich bei der organisierenden Person informieren, ob für die Datenverarbeitung im Zusammenhang mit der Videokonferenz eine Datenschutzerklärung oder eine Datenschutz-Kurzinformation bereitgestellt wird. Sollten diese Informationen nicht vorhanden sein, dann bitten Sie bei Unklarheiten die organisierende Person, die Regelungen zur Verwendung der verschiedenen Funktionen zu erläutern,

  - vor dem Aufzeichnen von Teilen der Videokonferenz für die eigene Nachbereitung und vor dem Anfertigen von z. B. Screenshots für die Veröffentlichung in sozialen Medien unbedingt sicherstellen, dass dies ausdrücklich erlaubt ist und die anderen Teilnehmenden vorab eingewilligt haben,

  - keine privat vorhandenen Accounts nutzen (z. B. private Facebook-, Google- oder Microsoft-IDs).

Hinweise zu einigen verbreitet eingesetzten Anbietern von Videokonferenzsystemen

Die LDI sieht die Nutzung von derzeit populären kommerziellen Videokonferenzplattformen unter datenschutzrechtlichen Aspekten grundsätzlich kritisch. Derartige Tools müssen zum Schutz der personenbezogenen Daten der Betroffenen die Anforderungen aus Art. 32 DSGVO an die Datensicherheit erfüllen. Insbesondere sind in diesem Kontext die Vertraulichkeit und Integrität der Daten zu gewährleisten.

Zwar sind viele Produkte häufig benutzerfreundlich gestaltet, was sie für Viele verständlicherweise attraktiv macht. Es können sich jedoch in datenschutzrechtlicher Hinsicht einige Probleme ergeben. Daher sollten Sie in besonderer Weise auf die Einhaltung datenschutzrechtlicher Grundsätze achten. Als Hilfestellung stellen wir im Folgenden datenschutzrechtliche Informationen zu einigen verbreitet eingesetzten Anbietern von Videokonferenzsystemen zusammen. Diese Zusammenstellung ist keinesfalls abschließend. Auch wurden die einzelnen Softwareprodukte nicht von uns geprüft. Insofern kann über die Datenschutzkonformität derartiger Produkte keine abschließende Aussage getroffen werden. Die Anbieter sind zudem nicht in Nordrhein-Westfalen ansässig, sodass die Anbieter selbst nicht der daten-schutzrechtlichen Kontrolle der LDI NRW unterliegen. Vielmehr haben wir die Nutzungsbestimmungen (Stand: 15.05.2020) der einzelnen Anbieter sowie öffentlich zugängliche Informationsquellen zugrunde gelegt.

Soweit die Verarbeitung von Betroffenendaten auf digitalen Wegen dazu führt, dass Dienstleistungen weiter erbracht werden können, haben die jeweiligen Verantwortlichen dies in eigener Verantwortung zu prüfen und insbesondere sicherzustellen, welche organisatorischen Maßnahmen im Einzelfall erforderlich und angemessen sind. Zu beachten ist, dass bei bestimmten Vorgängen (z. B. Online-Prüfungen, Vorstellungsgesprächen oder Berufungsverfahren im Hochschulbereich) wesentlich strengere Maßstäbe anzulegen sind, da hier in der Regel weitaus sensiblere Daten verarbeitet werden, als z. B. bei der reinen Vermittlung von Unterrichtsinhalten im Schulbereich.

Jitisi Meet:

- Jitsi Meet ist eine Open-Source-Lösung für Videokonferenzen.
- Öffentlich zugängliche Server werden außer vom Hauptentwickler der Software, der Firma 8x8 Inc. (USA) von verschiedensten Anbietern weltweit bereitgestellt, darunter aus solchen aus Deutschland und der EU
- Ob eine Registrierung des Organisators und/oder der Teilnehmenden erforderlich ist, ist anbieterabhängig.
- Je nach Wahl des Servers können personenbezogene Daten außerhalb der EU verarbeiten werden.
- Eine korrekte Installation vorausgesetzt, sind die Audio- und Videoströme transportverschlüsselt sowie Chatnachrichten Ende-zu-Ende-verschlüsselt.
- Der Betrieb einer eigenen Instanz ist lizenzkostenfrei möglich.

Microsoft Teams Basic:

- Anbieter: Microsoft Corporation (USA); Microsoft Teams ist Teil des Microsoft 365-Cloudportfolios.
- Microsoft hat sich zwar dem EU-Privacy Shield unterworfen, wobei sich die Zertifizierung auch auf Personaldaten (HR) erstreckt. Die entsprechende Entscheidung der EU-Kommission ist jedoch ungültig (EuGH C-311/18), so dass eine Drittlandübermittlung nicht auf das EU-Privacy Shield gestützt werden kann.
- Zur Einhaltung der Regelungen der Datenschutz-Grundverordnung heißt es auf der Website von Microsoft (https://www.microsoft.com/de-de/trust-center/privacy) lediglich: „Im Rahmen unserer laufenden Verpflichtung für den Datenschutz haben wir einige Investitionen getätigt und Verbesserungen im Bereich der Datenverarbeitung erzielt, um die DSGVO-Compliance und das Recht des Einzelnen auf Privatsphäre zu stärken."
- Auf Basis der derzeit verfügbaren Informationen ist uns eine abschließende allgemeine Bewertung der datenschutzrechtlichen Zulässigkeit nicht möglich.
- Sollte ein Verantwortlicher diesen Dienst ungeachtet dessen in Anspruch nehmen wollen, hat er den Nachweis für die datenschutzrechtliche Zulässigkeit im Einzelfall zu erbringen. Hierzu sind insbesondere explizite vertragliche Regelungen mit dem Hersteller erforderlich, in denen abschließend festgelegt wird, zu welchen Zwecken der Hersteller Daten in welchem Umfang verarbeitet. Dies beinhaltet auch die Weitergabe an Dritte.
- Es ist eine Registrierung des Organisators der erforderlich, nicht aber der Teilnehmenden.
- Der Dienst ist transportverschlüsselt.

Skype:

- Anbieter: Microsoft Corporation (USA); Skype ist Teil des Microsoft 365-Cloudportfolios.
- Microsoft hat sich zwar dem EU-Privacy Shield unterworfen, wobei sich die Zertifizierung auch auf Personaldaten (HR) erstreckt. Die entsprechende Entscheidung der EU-Kommission ist jedoch ungültig (EuGH C-311/18), so dass eine Drittlandübermittlung nicht auf das EU-Privacy Shield gestützt werden kann.
- Zur Einhaltung der Regelungen der Datenschutz-Grundverordnung heißt es auf der Website von Microsoft (https://www.microsoft.com/de-de/trust-center/privacy) lediglich: „Im Rahmen unserer laufenden Verpflichtung für den Datenschutz haben wir einige Investitionen getätigt und Verbesserungen im Bereich der Datenverarbeitung erzielt, um die DSGVO-Compliance und das Recht des Einzelnen auf Privatsphäre zu stärken."
- Es ist eine Registrierung des Organisators der Videokonferenz erforderlich, nicht aber der Teilnehmenden.
- Der Dienst ist transportverschlüsselt und bietet die Möglichkeit, zumindest im 1:1 Textchat eine Ende-zu-Ende-Verschlüsselung zu nutzen.

TeamViewer Blizz:

- Anbieter: TeamViewer Germany GmbH (Baden-Württemberg, Deutschland)
- Da die TeamViewer Germany GmbH ihren Sitz in Deutschland hat, ist die DS-GVO anwendbar. Für den Fall, dass Unternehmen außerhalb der EU oder des

EWR eingebunden werden, wird nach eigener Aussage anhand von Standardvertragsklauseln sichergestellt, dass die personenbezogenen Daten der Nutzer adäquat geschützt werden. Siehe jedoch oben Ziffer 2.f).
- Es ist eine Registrierung des Organisators der Videokonferenz erforderlich, nicht aber der Teilnehmenden.
- Der Dienst ist transportverschlüsselt und bietet die Möglichkeit, eine Ende-zu-Ende-Verschlüsselung zu nutzen.

WebEx:
- Anbieter: Cisco Systems, Inc. (USA)
- Die Cisco Systems Inc. hat sich zwar dem EU-Privacy Shield unterworfen, wobei sich die Zertifizierung auch auf Personaldaten (HR) erstreckt. Die entsprechende Entscheidung der EU-Kommission ist jedoch ungültig (EuGH C-311/18), so dass eine Drittlandübermittlung nicht auf das EU-Privacy Shield gestützt werden kann.
- Es ist eine Registrierung des Organisators der Videokonferenz und der Teilnehmenden erforderlich.
- Cisco WebEx Teams unterstützt nach eigenen Angaben (https://help.webex.com/de-de/weov2i/Cisco-Webex-Support-for-GDPR) die DSGVO durch den Schutz und die Achtung personenbezogener Daten.
- Es ist eine Registrierung des Organisators der Videokonferenz erforderlich, nicht aber der Teilnehmenden.
- Der Dienst ist transportverschlüsselt und bietet nach Herstellerangaben die Möglichkeit, eine Ende-zu-Ende-Verschlüsselung zu nutzen.

WebEx über Telekom:
- Anbieter: Telekom Deutschland GmbH
- Die Telekom Deutschland GmbH hat ihren Sitz in Deutschland. Nach eigenen Angaben können bei der Nutzung der WebEx Software die Webkonferenzdaten der Nutzer (IP-Traffic) auch über Server der Fa. Cisco Systems, Inc. außerhalb der EU geleitet werden (https://geschaeftskunden.telekom.de/vernetzung-digitalisierung/vernetzung/web-videokonferenzen/datenschutz-webex). Mit der datenverarbeitenden Stelle außerhalb der EU bestehen nach Angabe der Telekom Deutschland GmbH Verträge gemäß der von der EU-Kommission genehmigten Standardvertragsklauseln. Mit der datenverarbeitenden Stelle außerhalb der EU bestehen nach Angabe der Telekom Deutschland GmbH Verträge gemäß der von der EU-Kommission genehmigten Standardvertragsklauseln. Siehe jedoch oben Ziffer 2.f).
- Es ist eine Registrierung des Organisators der Videokonferenz und der Teilnehmenden erforderlich.
- Der Dienst ist transportverschlüsselt; Ob die Möglichkeit besteht, eine Ende-zu-Ende-Verschlüsselung zu nutzen, ist uns nicht bekannt.

Zoom:
- Anbieter: Zoom Video Communications, Inc. (USA)
- Zoom hat sich zwar dem EU-Privacy Shield unterworfen, die Zertifizierung erstreckt sich jedoch nicht auf Personaldaten (HR). Die entsprechende

Entscheidung der EU-Kommission ist ungültig (EuGH C-311/18), so dass eine Drittlandübermittlung nicht auf das EU-Privacy Shield gestützt werden kann.
- Zoom gewährleistet nach eigenen Angaben die Einhaltung der Regelungen der Datenschutz-Grundverordnung
- Tracking: Zoom war in der Vergangenheit stark wegen verschiedener Sicherheitslücken in der Kritik. Inzwischen hat der Anbieter nach eigener Darstellung einige datenschutzrechtliche Anpassungen vorgenommen. So gibt Zoom in seinen überarbeiteten Datenschutzrichtlinien vom 29.03.2020 (https://zoom.us/de-de/privacy.html) an, bei der Nutzung des Videokonferenzsystems die personenbezogenen Daten der Nutzer nicht zu verkaufen und sie nicht für Werbezwecke, sondern ausschließlich für die Bereitstellung von Diensten von Zoom zu verwenden. Zudem hat Zoom Verbesserungen bei den nutzer- und datenschutzfreundlichen Voreinstellungen vorgenommen („Privacy by Default“). So ist inzwischen die Einrichtung eines Warteraums ebenso voreingestellt wie die passwortgeschützte Einwahl. Hierdurch wird die Gefahr von Datenschutzproblemen aufgrund unerwünschter Konferenzteilnahmen gemindert.
- Es ist eine Registrierung des Organisators der Videokonferenz erforderlich, nicht aber der Teilnehmenden.
- Der Dienst ist transportverschlüsselt.
- Achtung: Es ist möglich, Funktionen zu verwenden, mit denen ein erhöhtes Risiko verbunden ist (z. B. Aufnahme, Aufmerksamkeitsanzeige). Hier gilt es, die o. g. Hinweise zu beachten.

Liste aller verwendeten Quellen:

- Berliner Beauftragte für Datenschutz und Informationsfreiheit: „Checkliste für die Durchführung von Videokonferenzen während der Kontaktbeschränkungen“ (abrufbar unter https://www.datenschutz-berlin.de/infothek-und-service/themen-a-bis-z/corona-Pandemie.html)

- Unabhängiges Landeszentrum für Datenschutz: „Plötzlich Videokonferenzen – und nun?“ (abrufbar unter https://www.datenschutzzentrum.de/artikel/1329-Ploetzlich-Videokonferenz-und-der-Datenschutz-Die-Landesbeauftragte-fuer-Datenschutz-Schleswig-Holstein-informiert.html)

- Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz: „Checkliste für die Auswahl videogestützter Kommunikationstechnik zum Einsatz an Schulen“ (abrufbar unter https://www.datenschutz.rlp.de/de/themenfelder-themen/videogestuetzte-kommunikationstechnik/)

- Der Bundesbeauftragter für den Datenschutz und die Informationsfreiheit: „Nutzung von Messenger- und Videokonferenzdiensten in Zeiten der Corona-Pandemie“ (abrufbar unter https://www.bfdi.bund.de/DE/Datenschutz/Datenschutz-Corona/Kommunikation/Inhalt/Messenger_Videokonferenzdienste.html)

- Hinweis der Datenschutzbeauftragten von Bund und Länder: „Sichere elektronische Kommunikation gewährleisten - Ende-zu-Ende-Verschlüsselung einsetzen und weiterentwickeln“ (abrufbar unter https://www.ldi.nrw.de/mainmenu_Service/submenu_Entschliessungsarchiv/Inhalt/Entschliessungen_Datenschutzkonferenz/Inhalt/86__Konferenz/Sichere_elektronische_Kommunikation_gew__hrleisten/Sichere_elektronische_Kommunikation_gew__hrleisten.php)