Landesbeauftragte
für Datenschutz und Informationsfreiheit
Nordrhein-Westfalen

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

Stand: 26.05.2021

Entscheidung für ein Videokonferenzsystem – Empfehlungen der LDI NRW zum Vorgehen

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, wurde 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 bereitzustellen, so dass die Daten in der Hand des Verantwortlichen verbleiben. Derartige Videokonferenzprodukte sind sowohl kommerziell als auch als Open Source Software erhältlich.
   Stellen Sie dabei sicher, dass die eingesetzte Software keine Daten über Ihre Beschäftigten oder deren Kommunikationspartner/-innen an den Hersteller der Software 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 eine Lösung eines Anbieters mit Sitz im Europäischen Wirtschaftsraum (EWR) oder aus einem Land mit gleichwertigem Datenschutzniveau eingesetzt werden kann (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).)

   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.

3. Wenn Sie statt eines Anbieters gemäß Ziff. 2 einen Anbieter mit Sitz außerhalb des EWR oder eines Landes mit gleichwertigem Datenschutzniveau beauftragen wollen, muss sichergestellt werden, dass die Anforderungen aus Kapitel V der DS-GVO umgesetzt werden.

Feststellen lässt sich bisher bereits, dass an Datenübertragungen in Drittstaaten nach dem "Schrems II"-Urteil des Europäischen Gerichtshofs (Rechtssache C-311/18) erhöhte Anforderungen gestellt sind. Der Datenexporteur muss in jedem Einzelfall das Datenschutzniveau im Empfängerland überprüfen und gegebenenfalls zusätzliche ergänzende Maßnahmen treffen, die im Wesentlichen ein im Europäischen Wirtschaftsraum garantiertes Schutzniveau gewährleisten. Diese Anforderungen sind nicht auf die USA beschränkt, sondern gelten für alle Drittstaaten ohne adäquates Datenschutzniveau.

Der Europäische Datenschutzausschuss (EDSA) gibt für die Umsetzung Empfehlungen (siehe unter https://www.ldi.nrw.de/mainmenu_Aktuelles/Inhalt/Empfehlungen-zum-Datentransfer-in-Drittlaender-nach-dem-_Schrems-II_-Urteil/Empfehlungen-zum-Datentransfer-in-Drittlaender-nach-dem-_Schrems-II_-Urteil.html). Die Dokumente sind zurzeit nur auf Englisch verfügbar. Hierzu siehe auch die Information auf unserer Website (s. https://www.ldi.nrw.de/mainmenu_Aktuelles/Inhalt/Empfehlungen-zum-Datentransfer-in-Drittlaender-nach-dem-_Schrems-II_-Urteil/Empfehlungen-zum-Datentransfer-in-Drittlaender-nach-dem-_Schrems-II_-Urteil.html).

Für das häufig zu betrachtende Empfängerland USA ist zu beachten, dass das EU-US Privacy Shield nicht mehr als Instrument für die Übermittlung in die USA verwendet werden kann. Für alternative Instrumente wie die Standardvertragsklauseln ist es zudem nicht immer möglich, die erforderlichen wirksamen ergänzenden Maßnahmen aufzufinden und umzusetzen. Allgemein können die Anforderungen dazu führen, dass es in einigen Fällen keine datenschutzkonforme Übermittlung in ein Drittland geben kann und deswegen - als Praxisempfehlung - auch nach einer Alternative ohne Drittlandtransfer gesucht werden sollte.

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: 10.05.2021) 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.

Cisco Webex:

- Anbieter: Mutterkonzern: Cisco Systems, Inc. (USA) Niederlassungen: Cisco Systems GmbH, Garching; WebEx Communications Deutschland GmbH, Düsseldorf
- Webex betont auf seiner Website, die DS-GVO durch den Schutz und die Achtung personenbezogener Daten zu unterstützen (https://help.webex.com/de-de/weov2i/Cisco-Webex-Support-for-GDPR).
- Andererseits findet sich in der Datenschutzerklärung von Webex folgende Aussage: „Wir können Ihre personenbezogenen Daten zur Ausübung unseres Geschäfts, zur Bereitstellung, Verbesserung, Sicherung und Anpassung unserer Websites und Lösungen, zur Versendung von Marketingmaterialien und anderen Geschäftsmitteilungen sowie zu weiteren im Rahmen der geltenden Gesetze zulässigen Zwecken an Dritte weitergeben." (https://www.cisco.com/c/de_de/about/legal/privacy-full.html). Im Folgenden wird auf der Website u. a. darüber informiert, dass die Weitergabe weltweit bei den Niederlassungen von Cisco, an Geschäftspartner oder Lieferanten von Cisco u. v. m. erfolgen kann.
- Die Cisco Systems Inc. hat sich nach eigener Aussage zwar dem EU-Privacy Shield unterworfen. 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 (siehe hierzu oben Ziffer 2.g)).
- 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.

Cisco Webex über Telekom:

- Anbieter: Telekom Deutschland GmbH
- Die Telekom agiert nach eigener Darstellung als Reseller der Cisco Webex-Lösung und sei deshalb an die technische Realisierung durch die Firma Cisco gebunden. Diese sehe derzeit die Übermittlung von Daten des Gastgebers sowie Telemetriedaten der verwendeten Teilnehmer-Clients zu bestimmten Zwecken wie Abrechnung (Gastgebername, Meeting-URL, Start/Ende des Meetings) oder Service-Analyse in die USA (Telemetriedaten der Clients) vor. Die Verarbeitung

von usergenerierten Daten (geteilte Bildschirminhalte/evtl. erfolgte Recordings) erfolge ausschließlich auf IT-Systemen in der EU.

- Neben der Vereinbarung von Standardvertragsklauseln hat die Telekom nach eigenen Angaben zusätzliche Maßnahmen, wie insbesondere jene der Verschlüsselung getroffen. Hierbei werde das Schlüsselmanagement vollständig auf den Kunden übertragen. Die entsprechende Stellungnahme der Telekom ist unter https://konferenzen.telekom.de/rechtliches/webex-datenschutz/ abrufbar.
- Sollten Sie diesen Dienst in Anspruch nehmen wollen, haben Sie den Nachweis für die datenschutzrechtliche Zulässigkeit im Einzelfall zu erbringen. Insbesondere ist zu prüfen, ob die von der Telekom genannten Garantien ausreichend sind oder durch weitere Maßnahmen ergänzt werden müssen. In diesem Zusammenhang wird auf das bereits oben unter Ziffer 2 g) erwähnte EuGH-Urteil verwiesen (Schrems II, C-311/18).
- Es ist eine Registrierung des Organisators der Videokonferenz und der Teilnehmenden erforderlich.
- Der Dienst ist transportverschlüsselt; es besteht die Möglichkeit, eine Ende-zu-Ende-Verschlüsselung zu nutzen.

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 auch 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 verarbeitet werden.
- Eine korrekte Installation vorausgesetzt, sind die Audio- und Videoströme transportverschlüsselt sowie Chatnachrichten Ende-zu-Ende-verschlüsselt. Unter bestimmten Voraussetzungen ist auch die Ende-zuEnde-Verschlüsselung der Audio- und Videoströme möglich.
- Der Betrieb einer eigenen Instanz ist lizenzkostenfrei möglich.

Microsoft Teams Basic:

- Anbieter: Microsoft Corporation (USA); Microsoft Teams ist Teil des Microsoft 365-Cloudportfolios.
- Zur Einhaltung der Regelungen der Datenschutz-Grundverordnung heißt es auf der Website von Microsoft (https://www.microsoft.com/de-de/trust-center/privacy) u. a.: „Verlassen Sie sich darauf, dass wir die DSGVO und andere Datenschutzstandards angemessen umsetzen. Unseren Unternehmenskunden und Kunden aus dem öffentlichen Sektor bieten wir einen besonderen Schutz: Wir werden sie finanziell entschädigen, falls wir ihre Daten auf Behördenanfrage in einer Weise offenlegen müssen, die gegen die europäische DSGVO verstößt."
- In Bezug auf die Einhaltung von Kapitel V Datenschutz-Grundverordnung heißt es auf der Website von Microsoft, dass das Unternehmen die Prinzipien des EU-U.S.-Privacy Shield-Frameworks beachtet, das EU-U.S. Privacy Shield-Framework allerdings aufgrund des Urteils des Europäischen Gerichtshofes in der Rechtssache C-311/18 als nicht als legale Basis für die Übertragung persönlicher Daten betrachtet (https://privacy.microsoft.com/de-de/privacystatement). Zudem heißt es dort: „Wenn Drittanbieter personenbezogene Daten in unserem Namen in einer Weise verarbeiten, die mit den Prinzipien jedes Privacy Shield-Abkommens unvereinbar sind, bleiben wir haftbar, sofern wir nicht beweisen können, dass wir für das Ereignis, das den Schaden verursacht hat, nicht verantwortlich sind." Siehe hierzu jedoch oben Ziffer 2.g).
- 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.

- Zur Einhaltung der Regelungen der Datenschutz-Grundverordnung heißt es auf der Website von Microsoft (https://www.microsoft.com/de-de/trust-center/privacy) u. a.: „Verlassen Sie sich darauf, dass wir die DSGVO und andere Datenschutzstandards angemessen umsetzen. Unseren Unternehmenskunden und Kunden aus dem öffentlichen Sektor bieten wir einen besonderen Schutz: Wir werden sie finanziell entschädigen, falls wir ihre Daten auf Behördenanfrage in einer Weise offenlegen müssen, die gegen die europäische DSGVO verstößt."
- In Bezug auf die Einhaltung von Kapitel V Datenschutz-Grundverordnung heißt es auf der Website von Microsoft, dass das Unternehmen die Prinzipien des EU-U.S.-Privacy Shield-Frameworks beachtet, das EU-U.S. Privacy Shield-Framework allerdings aufgrund des Urteils des Europäischen Gerichtshofes in der Rechtssache C-311/18 als nicht als legale Basis für die Übertragung persönlicher Daten betrachtet (https://privacy.microsoft.com/de-de/privacystatement). Zudem heißt es dort: „Wenn Drittanbieter personenbezogene Daten in unserem Namen in einer Weise verarbeiten, die mit den Prinzipien jedes Privacy Shield-Abkommens unvereinbar sind, bleiben wir haftbar, sofern wir nicht beweisen können, dass wir für das Ereignis, das den Schaden verursacht hat, nicht verantwortlich sind." Siehe hierzu jedoch oben Ziffer 2.g).
- 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.

Zoom:

- Anbieter: Zoom Video Communications, Inc. (USA)
- In der Datenschutzerklärung auf der Website von Zoom heißt es (https://zoom.us/de-de/privacy.html#_Toc44414845): „Zoom ist weltweit tätig, was bedeutet, dass personenbezogene Daten in jedem Land, in dem wir oder unsere Dienstanbieter Einrichtungen haben oder Veranstaltungen abhalten, gespeichert und verarbeitet werden können (z. B. in einem Rechenzentrum). Indem Sie Zoom nutzen oder personenbezogene Daten für einen der oben genannten Zwecke bereitstellen, willigen Sie in die Übertragung und Speicherung Ihrer personenbezogenen Daten in den USA oder an einem anderen Ort wie von unserem Kunden bestimmt ein. […] Wenn Sie im Europäischen Wirtschaftsraum

(EWR) ansässig sind und Ihre personenbezogenen Daten außerhalb des EWR übertragen werden, werden wir sie in einem Gebiet verarbeiten, das nach Feststellung der Europäischen Kommission ein angemessenes Schutzniveau für personenbezogene Daten bietet oder geeignete Sicherheitsvorkehrungen zum Schutz Ihrer personenbezogenen Daten implementieren. Dies umfasst die Übertragung gemäß den geltenden Übertragungsmechanismen, der Standardvertragsklausel der Europäischen Kommission."

- Sollten Sie Zoom ungeachtet dessen in Anspruch nehmen wollen, haben Sie den Nachweis für die datenschutzrechtliche Zulässigkeit im Einzelfall zu erbringen. Insbesondere ist zu prüfen, ob die von Zoom genannten Garantien ausreichend sind oder durch weitere Maßnahmen ergänzt werden müssen. In diesem Zusammenhang wird auf das bereits oben unter Ziffer 2 g) erwähnte EuGH-Urteil verwiesen (Schrems II, C-311/18).
- Es ist eine Registrierung des Organisators der Videokonferenz erforderlich, nicht aber der Teilnehmenden.
- Der Dienst ist transportverschlüsselt. Ab Client-Version 5.4.0 sind zudem – bei reduziertem Funktionsumfang – Ende-zu-Ende-verschlüsselte Konferenzen möglich.
- 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: „Hinweise für Berliner Verantwortliche zu Anbietern von Videokonferenz-Diensten“ (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 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 Ländern: „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)