Unsere Freiheiten:
Daten nützen – Daten schützen

Bild: ST.art - stock.adobe.com

Der Landesbeauftragte für
Datenschutz und
Informationsfreiheit
Baden-Württemberg

Handreichung Videokonferenzsysteme – Hinweise zur praktischen Nutzung

Videokonferenzsysteme

Hinweise des LfDI zur praktischen Nutzung von Videokonferenzsystemen (VKS)

Herausgegeben vom
Landesbeauftragten für den Datenschutz und die Informationsfreiheit Dr. Stefan Brink
Lautenschlagerstraße 20, 70173 Stuttgart
Telefon: 0711/615541-0
Telefax: 0711/615541-15
https://www.baden-wuerttemberg.datenschutz.de
E-Mail: poststelle@lfdi.bwl.de
Mastodon: https://bawü.social/@lfdi
PGP Fingerprint: E4FA 428C B315 2248 83BB F6FB 0FC3 48A6 4A32 5962
Stand: Dezember 2021; aktualisierte Tabelle Version 1.3.0. Stand 8.12.21

Weiterführende Angaben zu verschiedenen Anbietern
von Videokonferenzsystemen unter wikipedia.de

Inhalt

Videokonferenz als Online Dienst: Rahmenbedingungen und Empfehlungen

Dieses Papier soll Unternehmen, Behörden und Vereine bei der Auswahl geeigneter Videokonferenz-Dienste unterstützen. Es gibt einen auf das Wesentliche beschränkten Überblick über die rechtlichen und technischen Datenschutz-Anforderungen, beschreibt einige gängige Anbieter und stellt tabellarisch eine Übersicht an Eigenschaften der Softwares und Dienste dar. Unser Ziel: Wer Videokonferenzen veranstalten möchte, soll sich orientieren können, was unterschiedliche Systeme leisten und welche „Baustellen" es gibt.

Der Verantwortliche (zur Definition dieses Begriffs siehe Artikel 4 Nr. 7 DS-GVO) hat grundsätzlich drei Möglichkeiten, ein Videokonferenzsystem (VKS) zu betreiben: Entweder er betreibt das System auf Basis eigener Infrastruktur und Software vollständig selbst[1], oder er greift dabei auf einen Dritten zurück, der die Videokonferenz (VK) als externer IT-Dienstleister mitsamt Hard- und/oder Software anbietet. Aktuell greifen die meisten Verantwortlichen auf die dritte Möglichkeit, einen Online-Dienst (Software as a Service) zurück. Diese Fallgestaltung untersucht der LfDI näher und gibt Empfehlungen zu den einschlägigen rechtlichen und technischen Fragestellungen, wobei er eine Reihe von verbreiteten Online-Dienste-Anbietern näher betrachtet.

Bestehen aus Sicht des Verantwortlichen besondere Anforderungen an das VKS, etwa wegen der besonderen Sensibilität der verarbeiteten Daten (z.B. bei der Verarbeitung von besonderen Kategorien personenbezogener Daten nach Artikel 9 DS-GVO oder bei Sicherheitsbehörden) oder der besonderen Schutzbedürftigkeit der Nutzer (z.B. im Schulbereich), so wird das selbst (ggf. auf Basis von Open Source Software wie BigBlueButton oder Jitsi) oder von einem sorgsam ausgewählten IT-Dienstleister betriebene VKS vorzugswürdig oder sogar alternativlos sein.

Bestehen weniger hohe Anforderungen an den Betrieb des VKS, so kommen auch die gängigen Online-Dienste-Anbieter in Betracht. Alle diese Online-Dienste weisen zwar funktionale Unterschiede auf, aber alle sind grundsätzlich nutzbar und funktionsfähig. „Gefühlte" Qualitätsunterschiede („System X ruckelt und stürzt ab" oder „System Y klappt immer reibungslos") beruhen auf der Art der Einbindung beim Verantwortlichen (und dessen verfügbarer Bandbreite des Internetzugangs) und sind regelmäßig nicht systembedingt. Folglich bleiben „gefühlte" Unterschiede zwischen den VKS ebenso wie rein werbende Aussagen („intuitive Führung", „moderne, selbsterklärende Benutzeroberfläche") hier außer Betracht.

[1] Dieser Fall ist selten; zu den Pflichten eines Verantwortlichen nach der DS-GVO vgl. DSK, Orientierungshilfe Videokonferenzsysteme, Stand 23.10.2020: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2020/11/OH-Videokonferenzsysteme_final.pdf

VKS per Online Dienst

Anstatt das Videokonferenzsystem selbst zu betreiben oder von einem Dienstleister nach eigenen Vorstellungen betreiben zu lassen, gibt es also auch die Möglichkeit, bestehende Online-Dienste zu verwenden. Für die Entscheidung für einen Online-Dienst spricht zunächst die einfache Bereitstellung des angebotenen VKS. Der Verantwortliche schließt in diesem Fall einen Vertrag mit dem Anbieter. Hier beginnt die Aufgabe des Verantwortlichen, sich in die Lage zu bringen, den Online-Dienst vollständig zu kontrollieren, um seinen Pflichten nach der DS-GVO nachzukommen und deren Erfüllung auch belegen zu können (Rechenschaftspflicht Art. 5 Abs. 2 DS-GVO).

In Abhängigkeit von der konkreten Ausgestaltung des Online-Dienstes sind daher zentrale Konfigurationsoptionen (z.B. Datenabflüsse, Zugriffsrechte) zu prüfen und ggf. anzupassen. Danach melden bei Bedarf die dafür autorisierten Personen eine Videokonferenz beim Anbieter an und laden die teilnehmenden Personen ein.

Der Verantwortliche muss dazu zunächst einen Auftragsverarbeitungsvertrag schließen. Der Verantwortliche muss die Einhaltung der Datenschutz- grundsätze durch Auswahl eines geeigneten Anbieters sicherstellen (vgl. hierzu die Anforderungen des Art. 28 Abs. 1 DS-GVO) sowie entsprechende Anweisungen an den Anbieter als seinen Auftragsverarbeiter erteilen und eigene Vorkehrungen treffen. Dazu hat der Verantwortliche die vom Auftragsverarbeiter vorgelegten Nutzungsbedingungen und Sicherheitsnachweise und auch die vom Anbieter bereitgestellten Datenschutzinformationen zu prüfen. Ganz grundsätzlich ist bei der Auswahlentscheidung für einen Anbieter darauf zu achten, dass dieser geeignete technische und organisatorische Maßnahmen (TOMs) ergreift, damit die Verarbeitung im Einklang mit den Anforderungen der DS-GVO erfolgt. Der Anbieter muss hierfür hinreichende Garantien bieten.

Die größten und bekanntesten Anbieter von Videokonferenzprodukten haben ihren Firmensitz allerdings in den USA und verarbeiten dort (zumindest teilweise) die personenbezogenen Daten der Teilnehmenden als auch der Organisatoren einer Videokonferenz. Bei Datenübermittlungen in die USA oder andere Drittstaaten sind die Anforderungen des Kapitels V der DS-GVO einzuhalten.

Auftragsverarbeitung mit Auftragsverarbeitungsvertrag

Bei dem Einsatz eines von einem Anbieter betriebenen Online-Dienstes ist ein Vertrag nach Art. 28 DS-GVO abzuschließen; dabei sind verschiedene Punkte zu beachten:

- Bei der Auswahl des Auftragsverarbeiters ist darauf zu achten, dass dieser hinreichende Garantien für die erforderlichen technischen und organisatorischen Maßnahmen (TOM) bietet.2

- Vertragsmuster des Anbieters müssen vom Verantwortlichen überprüft und ggf. angepasst werden. Es sollte besonders darauf geachtet werden, dass die Weisungsgebundenheit des Auftragsverarbeiters umfassend geregelt wird und dass dem Verantwortlichen hinreichende Kontrollbefugnisse eingeräumt werden.
- Weigert sich ein Anbieter, seine Vertragsmuster nach Art. 28 DS-GVO rechtskonform anzupassen, so scheidet er als Vertragspartner des Verantwortlichen aus.

- Behält sich der Anbieter die Datenverarbeitung zu eigenen Zwecken vor (z.B. Verarbeitung von personenbezogenen Daten zum Nutzerverhalten, Einsatz von Analysetools, Tracking zu Werbezwecken), so verlässt er die Rolle des Auftragsverarbeiters und wird insoweit selbst Verantwortlicher. Dann muss eine Rechtsgrundlage für die Übermittlung nach DS-GVO zwischen den beiden Verantwortlichen bestehen (Art. 6 Abs. 1 DS-GVO), um das VKS rechtskonform betreiben zu können. Denkbar ist in diesem Fall, dass eine gemeinsame Verantwortlichkeit besteht, welche einen weiteren Vertrag nach Art. 26 DS-GVO erfordert. Auch hierzu halten Anbieter regelmäßig eigene Vertragsmuster bereit, welche der Verantwortliche prüfen und anpassen muss. Weigert sich ein Anbieter, seine Vertragsmuster nach Art. 26 DS-GVO rechtskonform anzupassen, so scheidet er als Vertragspartner des Verantwortlichen aus.

- Gegenüber den betroffenen Personen muss stets transparent gemacht werden, wer in welcher Rolle welche personenbezogenen Daten verarbeitet (vgl. Art. 12 ff. DS-GVO). Der Veranstalter muss als Verantwortlicher mit Nennung der Kontaktdaten und ggf. des Datenschutzbeauftragten und dessen Kontaktdaten klar aus der Information über die Datenverarbeitung hervorgehen (vgl. Art. 13 DS-GVO). Das gilt auch für den ggf. gemeinsam verantwortlichen Anbieter des Dienstes (vgl. Art. 26 DS-GVO), wobei auch klar darü-

ber informiert werden muss, welche Daten in gemeinsamer Verantwortlichkeit verarbeitet werden und welche nicht. Ist der Anbieter hingegen Auftragsverarbeiter, muss er nur bei den Empfängern der Daten genannt werden (vgl. Art. 13 Abs. 1 lit. e DS-GVO). Für die Erstellung der Datenschutzinformationen (vgl. Art. 13 DS-GVO) für die betroffenen Personen ist der Verantwortliche auf die vom Anbieter bereitgestellten Informationen zu den stattfindenden Verarbeitungen angewiesen.

Drittstaaten-Transfer

Verarbeitet das VKS die Daten der Nutzer nicht nur in Deutschland und Europa, sondern kommt es dabei zu sog. Drittstaaten-Transfers von personenbezogenen Daten, so ist in Folge einer Entscheidung des Europäischen Gerichtshofs (EuGH-Entscheidung zum Privacy Shield) besondere Vorsicht geboten. Insbesondere ist die Nutzung von Videokonferenzprodukten US-amerikanischer Anbieter sorgfältig zu prüfen. Dies gilt auch, wenn der Vertragspartner eine europäische Tochtergesellschaft ist. Das gleiche gilt für europäische Anbieter, sofern sie ihrerseits personenbezogene Daten in die USA übermitteln.

Dies hat den folgenden Hintergrund: Die DS-GVO bietet ein hohes Datenschutzniveau. Die Verordnung gilt unter den in Art. 3 Abs. 2 DS-GVO geregelten Voraussetzungen auch für Anbieter von Videokonferenzsystemen, die außerhalb der EU niedergelassen sind. Anbieter aus Nicht-EU-Staaten unterliegen in aller Regel auch den Rechtsvorschriften ihres Heimatstaates und damit unter Umständen Zugriffsrechten von Behörden von Drittstaaten, die eine Einhaltung der datenschutzrechtlichen Anforderungen der DS-GVO erschweren oder zu letzteren im Einzelfall im Widerspruch stehen können.

Werden Videokonferenzsysteme ausgewählt, die zu Datenübermittlungen in Drittländer, also in Länder außerhalb der EU bzw. des Europäischen Wirtschaftsraums führen, muss die Übermittlung besondere Bedingungen einhalten (Kapitel V, Art. 44 ff. DS-GVO, siehe dazu auch die Orientierungshilfe „Was jetzt in Sachen internationaler Datentransfer?“ des LfDI[2]). Solche Übermittlungen kann es insbesondere bei Anbietern geben, die selbst im Drittland ihren Sitz haben oder Unterauftragnehmer aus Drittländern einsetzen. Eine Datenübermittlung in Drittländer liegt auch dann vor, wenn der Anbieter oder ein Unterauftragsverarbeiter aus dem Drittland heraus auf in der EU verarbeitete Daten zugreift (z. B. zu Wartungs- und Supportzwecken, für die Abrechnung oder zur Erstellung von Statistiken).
Für manche Drittländer hat die EU-Kommission beschlossen, dass dort ein angemessenes Datenschutzniveau vorliegt. Dann sind für die Zulässigkeit des

[2] online verfügbar unter https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2021/10/OH-int-Datentransfer.pdf

Datenexports keine weiteren Bedingungen zu erfüllen (Art. 45 DS-GVO). Da mit dem Urteil C-311/18 des EuGH (Schrems II) der Beschluss der EU-Kommission zum sog. EU-U.S. Privacy Shield für ungültig erklärt wurde, steht dieser, als Mittel zur Sicherstellung eines angemessenen Schutzniveaus in den USA nicht mehr zur Verfügung. Die Bedingungen aus Kapitel V der DS-GVO können sonst z. B. durch die Standardvertragsklauseln der EU-Kommission eingehalten werden, die der Verantwortliche mit dem Anbieter als Auftragsverarbeiter abschließt. Wenn das unzureichende Schutzniveau aus behördlichen Zugriffsmöglichkeiten herrührt, sind ausreichende zusätzliche Maßnahmen im Bereich von Videokonferenzdiensten allerdings schwer vorstellbar, denn zumindest bestimmte Rahmendaten der Konferenzen müssen dem Anbieter aus technischen Gründen zugänglich sein. Verantwortliche, die Videokonferenzdienste nutzen, müssen nach Art. 5 Abs. 2 DS-GVO auch nachweisen, dass sie diese Prüfung vorgenommen haben und die Daten im Drittland nach diesen Maßstäben ausreichend geschützt sind.

Technische Anforderungen an VKS

Das Videokonferenzsystem ist gemäß Art. 24, 25, 32 DS-GVO durch Auswahl und Umsetzung geeigneter technischer und organisatorischer Maßnahmen so einzurichten, dass es den Anforderungen der DS-GVO an die Verarbeitung personenbezogener Daten genügt.

Nutzerauthentifizierung

Nur berechtigte Personen dürfen auf eine Videokonferenzsitzung und deren Daten zugreifen können. Hierzu müssen sich die teilnehmenden Personen gegenüber dem Videokonferenzdienst authentifizieren. Die benötigte Mindeststärke der Authentifizierung hängt von der Schwere der Risiken für die Rechte und Freiheiten der betroffenen Personen ab, die sich bei einem Bruch der Vertraulichkeit oder Integrität der Inhaltsdaten ergeben können.

Bei normalen Risiken genügt eine Authentifizierung mit Nutzername und geeignetem Passwort. Passwörter dürfen beim Dienstleister nicht im Klartext oder mit einem schwachen Hashing-Verfahren gespeichert werden. Das Authentifizierungsprotokoll sollte im Idealfall so ausgestaltet sein, dass Passwörter nicht im Klartext übertragen werden. Dem Stand der Technik entsprechende Authentifizierungsverfahren verhindern, dass aus dem Passwort abgeleitete Daten, die im Zuge eines Authentifizierungsvorgangs übertragen wurden, für einen zweiten Authentifizierungsvorgang wiederverwendet werden können. Sie verhindern ferner, dass die beim Verantwortlichen oder beim Auftragsverarbeiter, der die Authentifizierung durchführt, gespeicherten Verifikationsdaten für eine Anmeldung verwendet werden können, um die Folgen einer Kompromittierung dieser Daten zu minimieren.

Sind mit dem Bruch der Vertraulichkeit der voraussichtlich in den Inhaltsdaten der Konferenz enthaltenen Angaben über natürliche Personen hohe Risiken für die Rechte und Freiheiten dieser Personen verbunden, muss zumindest eine Zwei-Faktor-Authentifizierung nach dem Stand der Technik erfolgen. Dafür kommen je nach Höhe des Risikos insbesondere Softwaretoken bzw. Hardwaretoken in Frage.

👉 Viele Videokonferenzsysteme bieten auch einen Gastzugang an, der keine vorherige Identifizierung des Nutzers voraussetzt. Wenn keine vorherige Authentifizierung erforderlich ist, ist dies eine datensparsamere Variante, insbesondere bei der Nutzung von nicht selbst betriebenen Diensten, da der Betreiber des Dienstes damit weniger Informationen über die Teilnehmer erhält. Die Verwendung von Gastzugängen ist insbesondere dann empfehlenswert, wenn gewährleistet ist, dass nur Personen teilnehmen, die untereinander bekannt sind, wenn die Risiken, die durch eine nicht autorisierte Teilnahme entstehen, gering sind oder wenn nicht autorisierte Personen erkannt und ausgeschlossen werden können, bevor sie an der Videokonferenz teilnehmen.

Ein Gastzugang kann in den gängigen Systemen beispielsweise über einen Einladungslink ermöglicht werden, der den Gästen im Vorfeld zur Videokonferenzsitzung mitgeteilt wird und bei denen die Gäste vor Beginn der Videokonferenz lediglich ein Pseudonym für sich vergeben müssen. Die Empfänger dieses Links sind auf die Folgen einer nicht autorisierten Weitergabe des Links hinzuweisen. Die Übergabe des Links muss die Vertraulichkeit auf angemessenem Niveau wahren.

Deinstallation

Alle Komponenten, die für die Teilnahme an einer Videokonferenz auf einem Client installiert werden, müssen ebenso einfach und vollständig wieder deinstalliert werden können. Auch im Fall einer nur einmaligen Nutzung eines nativen Clients durch eine teilnehmende Person muss sichergestellt sein, dass keine nicht gewartete Software auf dem System verbleibt und ein mögliches Sicherheitsrisiko darstellt. Sofern webbasierte Videokonferenzsysteme genutzt werden, muss für einen sicheren Betrieb stets eine aktuelle Webbrowser-Version eingesetzt werden. Dasselbe gilt für ggf. erforderliche Browser-Erweiterungen. Insbesondere bei Diensten, die Tracking betreiben oder Daten an Dritte übermitteln, sollten Teilnehmende den privaten Modus des Browsers nutzen, um die Verknüpfung mit anderen Daten zu erschweren.

👉 Wenn Clients verwendet werden, sollten Verantwortliche prüfen, ob diese sich nach der Installation beim Systemstart automatisch starten und im Hintergrund unerkannt Informationen an den Hersteller oder Dienstebetreiber übermitteln.

Data Protection by Default

Videokonferenzsysteme müssen die Grundsätze des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen erfüllen (Art. 25 DS-GVO). So müssen im Sinne der Datensparsamkeit jedenfalls die Kamera, das Mikrofon und das Teilen des Bildschirms von Teilnehmern vor Eintritt in die Konferenz standardmäßig ausgeschaltet sein. Dasselbe gilt für die Aufnahmefunktion eines VKS. Darüber hinaus muss das VKS so gestaltet sein, dass nur der jeweilige Teilnehmer über das Einschalten seines Mikrofons und Bildes entscheiden kann. Zentrales Abschalten von Ton und Bild ist allerdings möglich.

Verschlüsselung (Transport / Ende-zu-Ende Verschlüsselung)

Videokonferenzsysteme müssen eine Verschlüsselung nach dem Stand der Technik implementieren. Hierzu liefert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zu geeigneten kryptographischen Verfahren.[3]

Für die Übertragung von Videokonferenzdaten ist mindestens eine Transportverschlüsselung entsprechend den einschlägigen Technischen Richtlinien des BSI erforderlich. Die Transportverschlüsselung muss die Vertraulichkeit, Integrität und Authentizität aller übertragenen Daten gewährleisten, der Inhaltsdaten wie auch der Metadaten. Dies verhindert, dass Dritte, die passiv die Kommunikation abhören, Zugriff auf die Inhalte erhalten.

Wenn die Verarbeitung von Daten im Rahmen einer Videokonferenz zu einem hohen Risiko für betroffene Personen führen kann, müssen der Verantwortliche und ggf. der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen treffen, um insbesondere die Vertraulichkeit der übermittelten Inhaltsdaten auf zentralen Servern und den anderweitig beteiligten IT-Komponenten sicherzustellen. Dies kann beispielsweise über eine Ende-zu-Ende-Verschlüsselung und eine Verschlüsselung gespeicherter Daten sichergestellt werden. Eine wirksame Ende-zu-Ende-Verschlüsselung setzt voraus, dass die Endgeräte der Teilnehmenden sich gegenseitig nachprüfbar authentifizieren und für jede Konferenz neue flüchtige Verschlüsselungsschlüssel unter Kontrolle der Konferenzteilnehmer so erzeugt, ausgehandelt bzw. verteilt werden, dass dem Betreiber keine Kenntnisnahme des Schlüsselmaterials möglich ist.

[3] vgl. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr02102_node.html

Zum Zeitpunkt der Erstellung dieses Papiers waren Ende-zu-Ende-verschlüsselnde Lösungen, die diese Anforderungen erfüllen und die Videokonferenzen für eine höhere Anzahl von teilnehmenden Personen auch dann ermöglichen, wenn den teilnehmenden Personen an den von ihnen genutzten Endpunkten nur eine geringe oder variierende Bandbreite und Rechenleistung zur Verfügung steht, noch nicht marktgängig. Unter den beschriebenen Umständen kann daher eine Transportverschlüsselung zur Erfüllung der gesetzlichen Verpflichtungen genügen, sofern durch kompensierende Maßnahmen ein dem Risiko angemessenes Schutzniveau gewährleistet wird. Die kompensierenden Maßnahmen müssen sich auf die Sicherheit der Dienste und Systeme des Betreibers – also des Diensteanbieters oder des für das Hosting des Dienstes in Anspruch genommenen Auftragnehmers – erstrecken (zusätzliche Härtung) und auch organisatorische Maßnahmen des Betreibers einschließen, die eine Kenntnisnahme der verarbeiteten Daten durch Beschäftigte des Betreibers erschweren.

Ist im Zuge der Durchführung von Videokonferenzen ein unbefugter Abfluss personenbezogener Daten zu befürchten, dann sollte der Nutzen der Inanspruchnahme von bestimmten Funktionalitäten des Dienstes (insbesondere private Chats, Screensharing und die Bereitstellung von Dokumenten in einem allen Teilnehmenden offenstehenden Arbeitsbereich) mit den hierbei verbundenen Risiken abgewogen und sollten ggf. diese Funktionalitäten unterbunden werden. Wenn der Veranstalter zentral für alle teilnehmenden Endgeräte entsprechende Funktionalitäten zuverlässig technisch deaktivieren kann, so ist dies hilfreich.

Eine geeignete Maßnahme zur Aufdeckung derartiger Abflüsse kann auch in einer Protokollierung der Inanspruchnahme der genannten Funktionalitäten liegen. Die Transparenz einer solchen Protokollierung für die Teilnehmenden ist zu wahren. Der Einsatz der einzelnen Funktionalitäten eines eingesetzten Videokonferenzsystems sollte separat und im Kontext betrachtet werden. So kann bei einem Verantwortlichen bspw. ein Dokumentenmanagementsystem (DMS) im Einsatz sein. Hier wäre zu prüfen, ob dieses System einer Dokumentenaustauschfunktionalität des Videokonferenzsystems vorzuziehen ist.

Bei der Prüfung sind insbesondere auch die Risiken für Rechte und Freiheiten der betroffenen Personen zu berücksichtigen. Betreibt der Verantwortliche (oder ein für das Hosting des Dienstes in Anspruch genommener Auftragnehmer) Serversoftware für den Betrieb oder stellt der Verantwortliche den Teilnehmenden (mobile) Anwendungen zur Verfügung, für die er von einem Dritten Nutzungsrechte erworben hat, ist er ebenfalls verpflichtet, sicherzustellen, dass der Hersteller und andere Dritte keinen Zugriff auf die verarbeiteten Daten erhalten, auch nicht auf einzelne Teile wie Nutzungsdaten.

Metadaten, Telemetrie- und Diagnosedaten

Bei der Durchführung von Videokonferenzen fallen neben den Inhaltsdaten zahlreiche Meta- und Verbindungsdaten an. Diese betreffen beispielsweise Informationen über die Teilnehmer (wer, wann, wie lange, von wo, mit welchem Gerät usw. teilgenommen hat). Aus diesen Daten lassen sich teils sehr tiefgehende Rückschlüsse auf das Kommunikationsverhalten ziehen. Verantwortliche müssen prüfen, ob der Anbieter diese nur im unbedingt erforderlichen Maß verarbeitet und anschließend löscht.

Einige Anbieter von Videokonferenzsoftware erheben darüber hinaus teils sehr detaillierte Daten über das Verhalten der Nutzenden. Diese Daten werden oftmals als Telemetrie- oder Diagnosedaten bezeichnet. Dies bedeutet regelmäßig eine Übermittlung personenbezogener Daten durch den Verantwortlichen an den Anbieter zu dessen eigenen Zwecken. Dafür ist jeweils eine Rechtsgrundlage nach Artikel 6 Absatz 1 DS-GVO nötig und Verantwortliche müssen in der Lage sein, ihrer Rechenschaftspflicht nach Artikel 5 Absatz 2 nachzukommen.

App oder Browser?

Die meisten Videokonferenzsysteme lassen sich sowohl mit Desktop- und Mobil-Apps als auch im Web-Browser nutzen. Grundsätzlich kann die Nutzung des Web-Browsers datenschutzfreundlicher sein, da der Browser für eine Abschottung vom restlichen System sorgt und weniger Zugriff auf sensible Daten besteht. Zum Schutz vor Tracking und der Verarbeitung von Telemetrie- und Diagnosedaten können Nutzende den privaten Browsermodus verwenden. Insbesondere Desktop-Apps können sich tief im System verankern, bereits beim Systemstart im Hintergrund starten und dabei Daten übermitteln. Ebenso können sie Zugriff auf sensible Daten wie die Kalender der Nutzenden erhalten. Welche Daten an den Hersteller oder Dienstebetreiber übermittelt werden, ist bei Desktop- und Mobil-Apps nur schwer zu kontrollieren, während dies bei Web-Anwendungen relativ leicht überprüfbar ist.

Daher sollten Verantwortliche die Browser-Versionen empfehlen bzw. betroffene Personen die Browser-Version nutzen, auch wenn die Anbieter den Nutzenden die Installation der Desktop-Anwendungen deutlich „vorschlagen“.

Hinweise zu verbreiteten Videokonferenzsystemen

#Zu Alfaview

Kurzbeschreibung des VKS-Angebots

alfaview ist eine in Deutschland entwickelte Software für Videokonferenzen, spezialisiert auf virtuelle Online-Meetings, Seminare, Unterrichtseinheiten und Konferenzen. In den Live-Konferenzräumen von alfaview können über 200 Personen mit Video und Audio vernetzt übertragen werden. Der Zuschauermodus ermöglicht die gleichzeitige Teilnahme von 500 Personen. Den Nutzern steht eine Toolbox zur Integration kollaborativer Programme (White- board, Umfrage, Voting) zur Verfügung. Außerdem sind Breakout Rooms, das Screen-Sharing, die Live-Transkription des gesprochenen Wortes im Raum sowie deren Live-Übersetzung in viele Sprachen möglich.
Die Videokonferenzsoftware kann von privaten Nutzenden kostenfrei heruntergeladen werden. Unternehmen können sie kostenpflichtig erwerben und nach Unternehmensbedarf konfigurieren. Die Software wird u.a. von Privatanwendern, Wirtschaftsunternehmen und Bildungseinrichtungen verwendet.

I. Rechtlich

@ Datenschutzerklärung (DSE)

Stand 3/2021

Erfüllt Pflichten nach Art. 12/13/14 DS-GVO?

Ja. Die DSE von Alfaview ist sehr gut.

DSE in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache (Art. 12 Abs. 1 DS-GVO)?

Ja. Verbesserungen möglich bei:

> „Diese Daten werden verarbeitet, um Ihnen im Rahmen unseres berechtigten Interesses die Dienstleistung zur Verfügung stellen zu können (Art. 6 Abs. 1 S. 1 lit. f DSGVO). Die Verarbeitung geschieht zu folgenden Zwecken: … um den Service fortlaufend verbessern zu können."
>
> Was unter Serviceverbesserung genau zu verstehen ist, ist nicht ganz klar.

„Grundsätzlich werden die Daten spätestens nach acht Wochen gelöscht."

Das Wort „Grundsätzlich" lässt die Möglichkeit von Ausnahmen offen.

Verwendung von personenbezogenen Daten zu eigenen Zwecken?

Nein.

👉 Eine Verwendung personenbezogener Daten der Nutzer zu eigenen Zwecken des Anbieters schließt den Einsatz eines VKS im öffentlichen Dienst (insbesondere an Schulen) aus. Die neben einer Einwilligung nach Art. 6 Abs. 1 lit. a DS-GVO, welche nach EGr. 43 gegenüber Behörden grundsätzlich nicht freiwillig abgegeben werden kann, einzig verbleibende Rechtsgrundlage des berechtigten Interesses nach Art. 6 Abs. 1 lit. f DS-GVO ist für Behörden nicht einschlägig (vgl. Art. 6 Abs. 1 Satz 2 DS-GVO).

@Auftragsverarbeitungs-Vertrag (AVV)

Klarstellung durch Alfaview in § 1 Abs. 1 des AVV: Alfaview ist Auftragsverarbeiter (Art. 28 DS-GVO), es sei denn, „der Auftraggeber setzt als natürliche Person die Anwendung alfaview® zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten ein" (dann ist die DS-GVO nach Art. 2 Abs. 2 lit. c DS-GVO nicht anwendbar). Eine Kostenabwälzung für Kontrollen auf den Auftraggeber ist nach Auffassung des Landesbeauftragten in dieser Form zulässig („Die Kosten für die Durchführung der Kontrolle trägt der Auftraggeber, es sei denn, die Kontrolle steht in Zusammenhang mit einem Verstoß gegen Datenschutzvorschriften oder Festlegungen in diesem Vertrag, welche der Auftragnehmer zu vertreten hat.").

@Drittstaaten-Transfer

Keine Datentransfers in Drittländer im Rahmen des VKS, die für die Leistungserbringung notwendigen Dienste werden ausschließlich auf Servern innerhalb der EU gehostet; bei der Einbindung der Dienste Dritter (Sprachübersetzungsdienste etc.) sind Datentransfers möglich, die nach den Kriterien des DS-GVO erfolgen müssen.

II. Technisch

@ Verschlüsselung (Transport / Ende-zu-Ende Verschlüsselung)

Bei der Transportverschlüsselung haben wir keine Mängel festgestellt. Eine Ende-zu-Ende-Verschlüsselung bietet alfaview nicht an.

@ Tracking

Nein.

@ Aufnahmemöglichkeit

Aufzeichnung: nein

#Zu BigBlueButton (BBB)

Kurzbeschreibung des VKS-Angebots

BigBlueButton (BBB) ist ein Open-Source-Webkonferenzsystem, das insbesondere für die Lehre gestaltet ist, aber auch als normales Videokonferenzsystem genutzt werden kann. Aufgrund seiner Historie als Konferenzsystem für Online-Unterricht verfügt es über Integrationen für viele der wichtigsten Lern- und Inhaltsverwaltungssysteme. BBB ist kostenfrei verfügbar.

Es ist kein Online-Dienst, den man direkt nutzen kann, vielmehr ein Software-Paket, das auf einem Server aufgesetzt wird und individuell konfiguriert werden muss. Verantwortliche können die Software auf eigenen oder gemieteten Servern selbst betreiben oder von einem Dienstleister betreiben lassen. Das Land Baden-Württemberg bietet allen Schulen des Landes kostenlos die Möglichkeit der Nutzung auf einer eigenen Instanz. Beim eigenen Betrieb von BBB liegt der Vorteil auf der Hand: Alle anfallenden Daten werden nur auf dem eigenen Server verarbeitet. BBB ist daher aus datenschutzrechtlicher Sicht anderen Diensten vorzuziehen.

Der Server, auf dem der Dienst aufgesetzt wird, sollte zur Vermeidung von Datenschutzproblemen in der EU stehen und abseits von der Teilnahme von außerhalb keine Daten in Drittländer transferieren. Wird ein IT-Dienstleister damit beauftragt, BBB aufzusetzen, muss mit diesem Unternehmen vor Nutzungsbeginn ein Vertrag zur Auftragsverarbeitung nach Art. 28 DS-GVO abgeschlossen werden.

BBB bietet die Möglichkeit verschiedene Administrations-Frontends zu nutzen, die unterschiedliche Funktionalitäten bieten. Die Einladung der Teilnehmenden erfolgt dann entweder per Anmeldung über Nutzerkonten oder über Einladungs-Links. BBB unterstützt die gemeinsame Nutzung mehrerer Audio- und Videoformate, Präsentationen mit erweiterten Whiteboard-Funktionen – wie Zeiger, Zoomen und Zeichnen –, öffentliche und private Chats, Desktop-Sharing, die Präsentation von PDF-Dokumenten und Microsoft-Office-Dokumenten und verfügt über untergeordnete Online-Konferenzräume (sog. Breakout-Räume). Darüber hinaus können Benutzer in einer von zwei Rollen an der Konferenz teilnehmen: als Betrachter oder als Moderator.

Als Betrachter können Nutzer an der Konferenz teilnehmen, ihre Webcams mit anderen teilen und mit anderen chatten. Moderatoren können bei BBB benannt werden. Diese können Präsentationen hochladen und bedienen.

Für mobile Endgeräte stehen keine Apps zur Verfügung, BBB funktioniert ab Android 6.0 mit Google Chrome und mit Safari bei Apple-Geräten ab iOS 12.2. Die Screen-Sharing Funktion ist in beiden Varianten nicht möglich, sie wird von diesen mobilen Browsern nicht unterstützt. BBB ist im Bildungssektor weit verbreitet (Schulen, Hochschulen). Es ist integrierbar in unterschiedliche Lernplattformen.

I. Rechtlich

@Datenschutzerklärung (DSE)

Stand 3/2021

Erfüllt Pflichten nach Art. 12/13/14 DS-GVO?

Das Video- und Webkonferenz-System BBB kann auf eigenen Servern betrieben werden, sodass die Einhaltung des Datenschutzes eigenverantwortlich sichergestellt und nachgewiesen werden kann.

DSE in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache (Art. 12 Abs. 1 DS-GVO)?

Das Video- und Webkonferenz-System BBB kann auf eigenen Servern betrieben werden, sodass die Einhaltung des Datenschutzes eigenverantwortlich sichergestellt und nachgewiesen werden kann.

Verwendung von personenbezogenen Daten zu eigenen Zwecken?

Nein.

👉 Eine Verwendung personenbezogener Daten der Nutzer zu eigenen Zwecken des Anbieters schließt den Einsatz eines VKS im öffentlichen Dienst (insbesondere an Schulen) aus. Die neben einer Einwilligung nach Art. 6 Abs. 1 lit. a DS-GVO, welche nach EGr. 43 gegenüber Behörden grundsätzlich nicht freiwillig abgegeben werden kann, einzig verbleibende Rechtsgrundlage des berechtigten Interesses nach Art. 6 Abs. 1 lit. f DS-GVO ist für Behörden nicht einschlägig (vgl. Art. 6 Abs. 1 Satz 2 DS-GVO).

@Auftragsverarbeitungs-Vertrag (AVV)

Das Video- und Webkonferenz-System kann auf eigenen Servern betrieben werden, sodass die Einhaltung des Datenschutzes eigenverantwortlich sichergestellt und nachgewiesen werden kann. Ein Auftragsverarbeitungsverhältnis nach Art. 28 DS-GVO besteht daher nicht.

Sofern man Dienstleister einsetzt, um über diese BBB zu nutzen, sind die Anforderungen des Art. 28 DS-GVO einzuhalten; dies ist zu dokumentieren.

@Drittstaaten-Transfer

Das Video- und Webkonferenz-System kann auf eigenen Servern betrieben werden, sodass die Einhaltung des Datenschutzes eigenverantwortlich sichergestellt und nachgewiesen werden kann. Ein Transfer von Nutzerdaten in Drittstaaten ist nicht vorausgesetzt.

II. Technisch

@Technisch-organisatorische Maßnahmen (TOM)

Grundsätzlich gehört BigBlueButton zu den sicheren Webkonferenzsystemen, weil auf den Einsatz von proprietärer Software verzichtet wurde (Open Source). BigBlueButton ist sicher vor Manipulationen Dritter oder Backdoors eines kommerziellen Anbieters. Aktuell (September 2021) sind keine Sicherheitsprobleme durch Programmierfehler bekannt.

Im Oktober 2020 veröffentlichte golem.de einen Artikel, in dem auf verschiedene Sicherheitsprobleme von BigBlueButton hingewiesen wurde. Kritikpunkte waren die unsichere Einbindung von LibreOffice, das Setzen von Cookies ohne secure-Flag (beide behoben mit Version 2.2.27) und die Verwendung von Ubuntu 16.04 (Unterstützung bis April 2021) und alten Node.js-Versionen.

@Verschlüsselung (Transport / Ende-zu-Ende Verschlüsselung)

Die Datenübertragung erfolgt verschlüsselt (SRTP).

@Tracking

Nein.

@Rollenkonzept für die Nutzung (Einladung/Teilnahme/Vorraum/Steuerung)

Die Anzahl der möglichen Teilnehmer mit BBB hängt von verschiedenen Faktoren ab, z.B. der gleichzeitig aktivierten Kameras der Teilnehmer sowie der Bandbreite und Leistungsfähigkeit der Server. Der LfDI betreibt selbst einen

kleinen BBB-Server und konnte über 100 Teilnehmer im Rahmen von Veranstaltungen des Bildungszentrums BIDIB bedienen.

@Aufnahmemöglichkeit

Aufzeichnung: Konferenzen werden standardmäßig aufgezeichnet.
Zum Prüfzeitpunkt sah die offizielle Version der Software vor, dass stets eine Aufnahme der gesamten Konferenz erfolgt und dass diese Aufnahme (Speicherdauer 14 Tage) zu einem späteren Zeitpunkt anhand von Schnittmarken bearbeitet wird. Dasselbe gilt für gezeigte Präsentationen. Für einzelne Meetings kann dies deaktiviert werden. Da dies für die Teilnehmer nicht ersichtlich ist, führt das zur Unrechtmäßigkeit der Verarbeitung und widerspricht dem Grundsatz der Datenminimierung. Diese Recording-Funktion kann (und muss) durch den Administrator deaktiviert werden (Anleitung unter https://docs.bigbluebutton.org/admin/privacy.html#recordings).

#Zu Cisco Webex

Kurzbeschreibung des VKS-Angebots

Cisco Webex ist eine Software und ein Online-Dienst für Videokonferenzen, IP-Telefonie, Instant-Messaging, Dateiübertragung und Screen-Sharing von Cisco Inc. mit Sitz in den USA. Die Leistungen werden als Software as a Service (SaaS) erbracht, für Einzelnutzer zum Teil auch kostenlos.

Webex kann mit Desktop- und Smartphone-Apps sowie im Web-Browser genutzt werden. Die Software bietet zahlreiche Funktionen, die nicht alle in der Browser-Version verfügbar sind, wie beispielsweise die Möglichkeit des Ausblendens des Hintergrunds bei Videokonferenzen.

I. Rechtlich

@Datenschutzerklärung (DSE)

Die Datenschutz-Richtlinie von Cisco bleibt unbestimmt. In weiteren Dokumenten - https://trustportal.cisco.com/ - werden weitere Details der Verarbeitungen aufgeführt.

Die englische Version (Cisco Online Privacy Statement) datiert vom 10.05.2021, die deutsche Version vom 12.08.2021. Beide Versionen beziehen sich immer noch auf das für unwirksam erklärte EU-US-Privacy Shield. Cisco behält sich die Nutzung personenbezogener Daten zu eigenen Zwecken sowie die Weitergabe an Dritte auch ohne Einwilligung des Betroffenen vor. Soweit Zustimmungen der Nutzer unterstellt werden („Durch die Nutzung unserer Websites und Lösungen oder die Bereitstellung personenbezogener Daten stimmen Sie im Umfang der geltenden Gesetze zu und akzeptieren, dass diese Daten an ein Ziel außerhalb Ihres Aufenthaltslands übertragen und dort verarbeitet oder gespeichert werden, wo unter Umständen andere Datenschutzstandards gel ten."), ist dies offensichtlich unwirksam.
Metadaten werden laut Beschreibung teilweise sehr lange (sieben bzw. drei Jahre) gespeichert.

@Auftragsverarbeitungs-Vertrag (AVV)

Standardmäßig wird bei der Online-Buchung kein Auftragsverarbeitungsvertrag geschlossen, sodass dies jeweils nachgeholt werden muss.

Der Mustervertrag (Stand Dezember 2020) sieht Abweichungen von Art. 28 DS-GVO vor, etwa bei der Weisungsbindung von Cisco: Im Fall von Verpflichtungen des Auftragsverarbeiters aus anderem Recht als dem der Europäischen Union oder der Mitgliedstaaten erlaubt der Mustervertrag Abweichungen von den Weisungen des Auftraggebers. Dies genügt nicht den Anforderungen von Art. 28 Abs. 3 lit. a DS-GVO.

@ Drittstaaten-Transfer

Es finden zahlreiche Transfers personenbezogener Daten in Drittstaaten statt. Hierfür bedarf es einer wirksamen Rechtsgrundlage.

II. Technisch

@ Verschlüsselung (Transport / Ende-zu-Ende Verschlüsselung)

Cisco WebEx Meetings bietet optional die Möglichkeit der Ende-zu-Ende-Verschlüsselung, die in der beschriebenen Form prinzipiell sicher sein kann. Diese optionale Möglichkeit kann allerdings in vielen Fällen gar nicht genutzt werden und kommt in der Praxis daher meist nicht zum Einsatz.

@ Tracking

Es finden Übermittlungen und Verarbeitungen personenbezogener Daten zu eigenen Zwecken des Anbieters ohne erkennbare Rechtsgrundlage statt.
Eine Kurzanalyse hat Tracking durch Drittanbieter offenbart, die weder im Auftragsverarbeitungsvertrag noch in der Datenschutzerklärung genannt werden.

#Zu GoToMeeting

Kurzbeschreibung des VKS-Angebots

Anbieter von GoToMeeting ist die LogMeIn Inc. mit Hauptsitz in Massachusetts, USA. Der kostenpflichtige Dienst kann vom Nutzer als Organisator genutzt werden, um bis zu 150 weitere Teilnehmende in Konferenzen (für diese kostenlos) einzuladen.

Der Dienst ist ein Softwarepaket für Online-Besprechungen, Desktop-Sharing und Videokonferenzen, mit dem der Benutzer via Internet mit anderen Computernutzern kommunizieren kann; er ist verfügbar für Android, iOS, PC und Mac.

GoToMeeting ist auch im Browser (außer Safari) einsetzbar, der Hersteller versucht Nutzende allerdings zur Installation der Desktop-Version zu veranlassen.

I. Rechtlich

@ Datenschutzerklärung (DSE)

GoToMeeting tritt als Auftragsverarbeiter nach Art. 28 DS-GVO auf, die zur Verfügung gestellten Datenschutzrichtlinien, Nutzungsbedingungen und ergänzenden Vertragsunterlagen sind für den juristischen Laien schwer einzuordnen und gerade auch durch das Konglomerat von konzernangehörigen Unternehmen kaum zu durchschauen.

GoToMeeting sichert in seinen Nutzungsbedingungen (vgl. 4.1 – https://www.logmein.com/de/legal/terms-and-conditions) zu, auf "Inhalte" der Nutzer nur zuzugreifen, wenn sie vereinbarungsgemäß dazu berechtigt oder angewiesen sind oder wenn dies erforderlich ist, um ihre Richtlinien, geltendes Recht oder Regierungsanfragen zu erfüllen. Das erscheint vertretbar. Dagegen wird im Dokument „Security and Privacy Operational Controls" - https://logmeincdn.azureedge.net/legal/GoToServices-SPOC.pdf - in Ziffer 5.7 auf Seite 12 „Tracking and Analytics" eine Verarbeitung für eigene Zwecke beschrieben. Auf dieses Dokument wird über den Link zu „GoToMeeting, GoTo Webinar und GoToTraining" in Anhang 4 (technische und organisatorische Maßnahmen) des DPA - https://logmeincdn.azureedge.net/legal/lmi-customer-dpa-de.pdf - verwiesen.

@ Auftragsverarbeitungs-Vertrag (AVV)

Der aktuelle „Datenverarbeitungsnachtrag“ vom 8.4.2021 enthält Angaben zu Art. 28 DS-GVO und Hinweise auf Sub-Unternehmer. Kritikpunkte der Berliner Aufsichtsbehörde zum Auftragsverarbeitungsvertrag wurden mittlerweile aufgegriffen.[4]

@ Drittstaaten-Transfer

Ja, gemäß Erklärung über Sub-Unternehmer (https://logmeincdn.azureedge.net/legal/GoToCollab-Subprocessor-List.pdf) auch in die USA.
Bei Drittstaaten-Transfers stützt sich GoToMeeting (via LogMeIn Inc.) auch im aktuellen DPA (Datenverarbeitungsnachtrag vom 8.4.2021) in seinen Standardvertragsklauseln auf den nicht mehr einschlägigen Artikel 26 Absatz 2 der Richtlinie 95/46/EG.

II. Technisch

@ Verschlüsselung (Transport/ Ende-zu-Ende Verschlüsselung)

Die Videokonferenzen können nach Angaben des Herstellers Ende-zu-Ende verschlüsselt durchgeführt werden (vgl. Sicherheits-Whitepaper). Diese Angaben konnten nicht überprüft werden. Andere Angaben aus dem Whitepaper wie die Authentifizierung per SRP haben sich beim Test mit der Browser-Version als unrichtig herausgestellt, da Passwörter wie herkömmlich nur transportverschlüsselt im Klartext übermittelt wurden.

@ Tracking

Tracker in der Android-App: Appsflyer, Google CrashLytics, Google Firebase Analytics, MixPanel.[5]

[4] vgl.https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2021-BlnBDI-Hinweise_Berliner_Verantwortliche_zu_Anbietern_Videokonferenz-Dienste.pdf, S.19
[5] vgl.: https://reports.exodus-privacy.eu.org/en/reports/com.gotomeeting/latest/

#Zu Jitsi Meet

Kurzbeschreibung des VKS-Angebots

Jitsi Meet ist eine Videokonferenz-Software, die ebenfalls unter Open Source Lizenz steht und von Verantwortlichen auf eigenen Servern selbst betrieben oder von Dienstleistern als Software-as-a-Service bezogen werden kann. Der Hersteller der Software, die Firma 8x8 Inc. (USA), betreibt zusätzlich auch einen öffentlichen Jitsi-Server (https://meet.jit.si/). Jitsi Meet kann im Webbrowser und als mobile App sowie mit Jitsi Meet Electron auf dem Desktop genutzt werden.

Teilnehmende werden grundsätzlich per Link eingeladen, ohne dass die Teilnehmenden ein Nutzerkonto haben müssen. Sie können optional einen frei wähl baren Namen setzen. Alle Teilnehmenden können einen Videokonferenzraum eröffnen und auch andere einladen. Dadurch bietet Jitsi ein hohes Maß an Pseudonymität. Moderationsrechte werden dem ersten Teilnehmenden übergeben, der die Konferenz betritt, Räume können mit einem Passwort geschützt oder nur bestimmte Teilnehmende zugelassen werden.

Es gibt aber auch die Möglichkeit, den Jitsi Server so zu konfigurieren, dass personalisierte Logins möglich sind. Jitsi Meet bietet zudem weitere Funktionen wie Screen-Sharing oder eine Chat-Fuktion. Auch ist es möglich den Hintergrund auszublenden. Die Aufzeichnung von Konferenzen ist bei entsprechender Server-Einstellung möglich.

In der COVID-19-Pandemie gewann Jitsi Meet viele neue Nutzende in Schulen, Bildungseinrichtungen, der Verwaltung und in Unternehmen, nicht zuletzt aufgrund der einfachen Bedienbarkeit ohne Installation auf dem Desktop-Computer und der Datensparsamkeit bei der Anwendung.

I. Rechtlich

@Datenschutzerklärung (DSE)

Stand 9/2021

Erfüllt Pflichten nach Art. 12/13/14 DS-GVO?

Die Videokonferenz-Software Jitsi Meet kann auf eigenen Servern betrieben werden, sodass die Einhaltung des Datenschutzes eigenverantwortlich sichergestellt und nachgewiesen werden kann.

Die Angaben der als Auftragsverarbeiter einsetzbaren Firma 8x8 Inc. (USA) genügen diesen Anforderungen nicht.

DSE in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache (Art. 12 Abs. 1 DS-GVO)?

Die Videokonferenz-Software Jitsi Meet kann auf eigenen Servern betrieben werden, sodass die Einhaltung des Datenschutzes eigenverantwortlich sichergestellt und nachgewiesen werden kann.
Die Angaben der als Auftragsverarbeiter einsetzbaren Firma 8x8 Inc. (USA) genügen diesen Anforderungen nicht.

Verwendung von personenbezogenen Daten zu eigenen Zwecken?

Die Videokonferenz-Software Jitsi Meet kann auf eigenen Servern betrieben werden, sodass die Einhaltung des Datenschutzes eigenverantwortlich sichergestellt und nachgewiesen werden kann.

Bei Nutzung der Jitsi Meet App vom Google Play Store sind Drittanbieter Tracking-Komponenten enthalten, die personenbezogene Daten für den Hersteller erheben. Dies kann durch die Nutzung der F-Droid-App vermieden werden.

👉 Eine Verwendung personenbezogener Daten der Nutzer zu eigenen Zwecken des Anbieters schließt den Einsatz eines VKS im öffentlichen Dienst (insbesondere an Schulen) aus. Die neben einer Einwilligung nach Art. 6 Abs. 1 lit. a DS-GVO, welche nach EGr. 43 gegenüber Behörden grundsätzlich nicht freiwillig abgegeben werden kann, einzig verbleibende Rechtsgrundlage des berechtigten Interesses nach Art. 6 Abs. 1 lit. f DS-GVO ist für Behörden nicht einschlägig (vgl. Art. 6 Abs. 1 Satz 2 DS-GVO).

@Auftragsverarbeitungs-Vertrag (AVV)

Sofern man Dienstleister einsetzt, um über diese Jitsi Meet zu nutzen, sind die Anforderungen des Art. 28 DS-GVO einzuhalten, dies ist zu dokumentieren. Die Angaben der als Auftragsverarbeiter einsetzbaren Firma 8x8 Inc. (USA) genügen diesen Anforderungen nicht.

@Drittstaaten-Transfer

Bei der Nutzung von Jitsi Servern in den USA kommt es zu Drittstaaten-Transfers. Es stehen auch alternative Server, sogenannte Instanzen, in Europa oder Deutschland bereit (https://jitsi.github.io/handbook/docs/community/com-

munity-instances).
Die offizielle Smartphone-App aus dem Google Play Store setzt Google Analytics ein, so dass bei deren Nutzung nicht erforderliche Daten verarbeitet und in die USA übermittelt werden.

Auch die Server-Konfiguration sollte vor dem Einsatz genau geprüft und die Konfiguration angepasst werden, um zu einem datenschutzkonformen Einsatz zu kommen (vgl. https://www.kuketz-blog.de/jitsi-meet-server-einstellungen-fuer-einen-datenschutzfreundlichen-betrieb/).

@ Nutzungsbedingungen/AGB

Jitsi setzt auf Datensparsamkeit. Da es in der Standardkonfiguration keine Anmeldung gibt und keine Daten von Nutzenden über die Konferenz hinaus gespeichert werden, könnten selbst bei einem Zugriff auf den Server keine Daten missbraucht werden.

II. Technisch

@ Verschlüsselung (Transport/ Ende-zu-Ende Verschlüsselung)

Der Gruppen-Videochat erfolgt in der Regel transportverschlüsselt, wird auf dem Server jedoch kurzzeitig entschlüsselt. Chatnachrichten sind Ende-zu-Ende verschlüsselt.

@ Tracking

Tracking: Nein.
Die Anbieter von jitsi-basierten Diensten stellen keine eigenen mobilen Anwendungen (Apps) zur Nutzung ihrer Dienste bereit. Stattdessen stehen die vom Hersteller 8x8 Inc. für alle allgemein einsetzbaren Apps zur Verfügung. Apps aus dem Google Play Store und dem Apple App Store enthalten häufig Software von Tracking-Anbietern wie Crashlytics und Firebase.

@ Rollenkonzept für die Nutzung (Einladung/Teilnahme/Vorraum/Steuerung)

Am digitalen Unterricht mit Jitsi Meet können bis zu 75 Personen teilnehmen. Außer in Anwendungsfällen mit geringfügigen Risiken sollten die Verantwortlichen darauf achten, dass der von ihnen genutzte Dienst eine Moderati-

onsrolle anbietet, die nur nach Anmeldung mit personenindividuellen Merkmalen (typischerweise mit Nutzername und Passwort) übernommen werden kann. Viele Jitsi-Instanzen vergeben die Moderationsrolle an die erste Person, die einen Konferenzraum betritt. Dies ist für Anwendungsfälle mit mehr als geringfügigen Risiken problematisch.

@Aufnahmemöglichkeit

Aufzeichnung: möglich.

#Zu Microsoft Teams

Kurzbeschreibung des VKS-Angebots
Microsoft Teams (abgekürzt MS Teams oder nur Teams) ist eine von Microsoft entwickelte Plattform, die Chat, Besprechungen, Notizen und Anhänge kombiniert. Der Dienst ist in die Microsoft 365-Suite mit Microsoft Office und Skype/Skype for Business integriert.

Microsoft bietet eine kostenlose Version von Microsoft Teams an, welche die meisten Kommunikationsoptionen der Plattform kostenfrei anbietet, jedoch die Anzahl der Nutzer und die Speicherkapazität begrenzt. 2018 wurde die Plattform dann auch für Externe ohne Microsoft-Account geöffnet. Gastbenutzern steht Microsoft Teams nach wie vor mit einem eingeschränkten Funktionsumfang zur Verfügung.

I. Rechtlich

@Datenschutzerklärung (DSE)

Die äußerst umfangreichen Datenschutzbestimmungen von Microsoft (Stand Juli 2021) sind wegen der Komplexität der angebotenen Dienste und ihrer Verschränkung nur schwer verständlich, viele Angaben bleiben vage und unvollständig. Durch unterschiedliche Versionen (für Nutzer und für Unternehmen/Entwickler) sowie nachträgliche Änderungen (Nachtrag zum Datenschutz für Microsoft-Onlinedienste, Data Protection Addendum DPA) wird die Rechtslage unübersichtlich.

Microsoft behält sich die Nutzung personenbezogener Daten zu eigenen Zwecken vor („Wir verwenden die Daten ebenfalls für unser Unternehmen, inklusive der Analyse und Leistung, der Einhaltung unserer gesetzlichen Verpflichtung, für unsere Belegschaft sowie zur Entwicklung.“) bzw. auch neben der Auftragsverarbeitung für Unternehmer für den “legitime[n] Geschäftsbetrieb” von Microsoft (https://privacy.microsoft.com/de-de/privacystatement#mainenterpriseservicesmodule bzw. https://aka.ms/DPA). Damit wird die Frage, ob Microsoft als Auftragsverarbeiter oder als (gemeinsam?) Verantwortlicher auftritt, klärungsbedürftig.

@Auftragsverarbeitungs-Vertrag (AVV)

Die in die Datenschutzbestimmungen integrierten Regelungen zur Auftragsuverarbeitung verstoßen gegen Art. 28 Abs. 3 UAbs. 1 S. 2 lit. a und g DS-GVO (Weisungsrecht des Verantwortlichen), soweit die Nutzung der Daten auch zu eigenen Zwecken, ihre Weitergabe oder Löschung auch durch (außereuropäisches) anwendbares Recht angeordnet oder zulässig ist. Unklarheiten bestehen auch bei der Art und Weise der Einbeziehung von (neuen) Subunternehmern (Art. 28 Abs. 2, 4 DS-GVO), insbesondere hinsichtlich der vorherigen Zustimmung des Verantwortlichen.

@Drittstaaten-Transfer

Ja. Es obliegt dem Nutzer dafür zu sorgen, dass ausreichende zusätzliche Maßnahmen getroffen werden, um entsprechend der Rechtsprechung des EuGH im Urteil „Schrems II“ das unzureichende Datenschutzniveau der USA auszugleichen.

@Verschlüsselung (Transport / Ende-zu Ende Verschlüsselung)

MS Teams bietet keine Möglichkeit der Ende-zu-Ende-Verschlüsselung. Dadurch ist der Anbieter prinzipiell in der Lage, sowohl Gespräche mitzuhören als auch die Chats mitzulesen.

@Tracking

Es finden zahlreiche Übermittlungen und Verarbeitungen personenbezogener Daten zu eigenen Zwecken des Anbieters ohne erkennbare Rechtsgrundlage statt. Im Rahmen der Analyse waren große Mengen an Tracking-Daten feststellbar, die in dem Umfang weder im Auftragsverarbeitungsvertrag noch in der Datenschutzerklärung genannt werden. So werden Details zum Nutzungsverhalten – wie welcher Nutzer wann welche Funktion genutzt oder wie mit der Software interagiert hat – direkt an den Hersteller übermittelt.

Zu Skype for Business

Kurzbeschreibung des VKS-Angebots

Skype for Busines (vormals Lync, nicht zu verwechseln mit Skype ohne Zusatz for Business) ist eine Software von Microsoft, um verschiedene Kommunikationsmedien inklusive Chat und Videokonferenz unter einer Oberfläche zu vereinen. Skype for Business kann von Verantwortlichen auch auf eigenen Servern (on-prem) betrieben werden, so dass die Kommunikationsdaten nicht zwangsweise über Cloud-Dienste des Anbieters übermittelt werden müssen. Mit Skype for Business Online bot Microsoft auch eine Version mit von Microsoft betriebenen Servern an, diese wurde aber Ende Juli 2021 eingestellt und durch MS Teams ersetzt.

Videokonferenzen sind mit Skype for Business nur über eine spezielle Anwendung, aber nicht per Browser möglich. Die Anwendung übermittelt zahlreiche Telemetrie- und Diagnosedaten an Microsoft. Dies sollte von Verantwortlichen grundsätzlich auf Netzwerkebene unterbunden werden. Für vertrauliche Gespräche sollten Verantwortliche eine genaue Analyse des Datensendeverhaltens der beteiligten Komponenten durchführen.

Microsoft hat Skype for Business in der on-prem Variante ebenfalls abgekündigt, so dass in diesem Papier nicht weiter darauf eingegangen wird.

Zu Zoom

Kurzbeschreibung des VKS-Angebots

Zoom ist ein VKS der „Zoom Video Communications, Inc." mit Hauptsitz in San José, Kalifornien (USA). Das gerade bei großen Nutzergruppen seit 2020 sehr beliebte VKS wird in verschiedenen Varianten angeboten. Die kostenlose Variante begrenzt Video-Gruppenchats auf bis zu 100 Personen und eine Gesprächsdauer von bis zu 40 Minuten. Zoom skaliert gut bei vielen gleichzeitigen Teilnehmern in Videokonferenzen und bietet zahlreiche Komfort-Funktionen. Es kann von Teilnehmern sowohl im Browser als auch mit Smartphone- und Desktop-Anwendungen genutzt werden, wobei die Software im Browser versucht, die Nutzenden zur Desktop Anwendung zu drängen. Das Anlegen von Videokonferenzen kann nur über die Desktop- und Mobil-Apps erfolgen.

I. Rechtlich

Unsere Hinweise beziehen sich auf den Stand 8/20 – mittlerweile liegen aktualisierte Unterlagen von Zoom vor, die wir umgehend prüfen und unsere Handreichung entsprechend anpassen.

@ Datenschutzerklärung (DSE)

Stand 8/2020

Erfüllt Pflichten nach Art. 12/13/14 DS-GVO?

Nein.

- Rechtliche Anforderung aus Art. 13 Abs. 1 lit. d: wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht, die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden;
  ⇨Nicht erfüllt, soweit Angaben zum berechtigten Interesse von Zoom fehlen.
- Rechtliche Anforderung Art. 14 Abs. 2 lit. b:
  ⇨Nicht erfüllt, soweit Angaben zum berechtigten Interesse von Zoom fehlen.
- Rechtliche Anforderung Art. 14 Abs. 2 lit. f: aus welcher Quelle die personenbezogenen Daten stammen und gegebenenfalls ob sie aus öffentlich zugänglichen Quellen stammen;
  ⇨Nicht erfüllt, soweit Angaben von Zoom fehlen.

DSE in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache (Art. 12 Abs. 1 DS-GVO)?

Nein, in den Punkten:

- Zooms DSE: „Dieser Hinweis wird möglicherweise in regelmäßigen Abständen aktualisiert."
- „Darüber hinaus erhalten wir von Dritten Daten über Sie."
- „Je nachdem, wie Sie Ihre Zoom Cookie-Einstellungen konfigurieren, sammeln wir diese Informationen möglicherweise automatisch über unsere Marketing-Seiten und andere Online-Dienste."
- „Daten, die durch die Verwendung von Cookies und Pixeln von Tools (wie Google Analytics und Google Ads), wie zum Beispiel:" (unvollständiger Satz)
- „Es kann sein, dass wir bestimmte Informationen zu Aufzeichnungszwecken oder zur Durchführung von Transaktionen, die Sie vor dem Antrag auf Löschung begonnen haben, aufbewahren müssen."
- „Kunden können ihre eigenen Konten löschen." (Ohne Hinweis, dass dies an der Speicherung durch Zoom nichts ändert.)

Verwirrend:

- E-Mail an privacy@zoom.us geht tatsächlich an support@zoom.us

Verwendung von personenbezogenen Daten zu eigenen Zwecken?

Ja. Laut Datenschutzerklärung sammelt der Dienst viele Daten von Teilnehmenden, zum Beispiel die Namen, Städte, Gesprächsdauer sowie Einstellungen und eindeutige Geräte-IDs aller Teilnehmenden für jedes einzelne Meeting. Inhalte aus der Kommunikation werden nicht gespeichert.

👉 Eine Verwendung personenbezogener Daten der Nutzer zu eigenen Zwecken des Anbieters schließt den Einsatz eines VKS im öffentlichen Dienst (insbesondere an Schulen) aus. Die neben einer Einwilligung nach Art. 6 Abs. 1 lit. a DS-GVO, welche nach EGr. 43 gegenüber Behörden grundsätzlich nicht freiwillig abgegeben werden kann, einzig verbleibende Rechtsgrundlage des berechtigten Interesses nach Art. 6 Abs. 1 lit. f DS-GVO ist für Behörden nicht einschlägig (vgl. Art. 6 Abs. 1 Satz 2 DS-GVO).

@Auftragsverarbeitungs-Vertrag (AVV)

Klärungsbedarf für den Kunden/Nutzende von Zoom: Ist Zoom Auftragsverarbeiter (dann Art. 28-Vertrag) oder (gemeinsam) Verantwortlicher (dann Art. 26-Vertrag)? Das „Zoom Global Data Processing Addendum" (DPA, November 2020) benennt in Ziff. 2 zwar mögliche Verteilungen von Verantwortlichkeit, lässt diese Frage aber letztlich offen.

Das „Zoom Privacy Statement" (August 2020) ist für den Fall der Auftragsverarbeitung unanwendbar („Was diese Erklärung abdeckt - Diese Erklärung gilt für personenbezogene Daten, die wir als für die Datenverarbeitung verantwortliche Stelle verarbeiten, d.h. als die Partei, die bestimmt, welche Daten aus welchem Grund erhoben werden.")

Der Kunde/Nutzende ist dafür verantwortlich, dass die Vorgaben der Art. 26 und 28 DS-GVO eingehalten werden. Dazu wird es erforderlich sein, Teile der Verträge von Zoom abzuändern. So widerspricht die nur eingeschränkte Weisungsbindung des Auftragnehmers Zoom (Ziff. 3.2 DPA) den Anforderungen aus Art. 28 Abs. 3 lit. a DS-GVO, da weisungswidrige Verarbeitungen auch gemäß anderem Recht als dem der Europäischen Union oder der Mitgliedstaaten erlaubt werden.

Gleichgelagerte Probleme ergeben sich hinsichtlich der Löschpflicht von Zoom: Ziff. 3.4 Satz 3 DPA schließt die Löschung der verarbeiteten personenbezogenen Daten nach Vertragsende entgegen Art. 28 Abs. 3 lit. g DS-GVO aus, soweit ein beliebiges anwendbares Recht dies zulässt. Auch mit Blick auf Unter-Auftragnehmer (Ziff. 5 DPA) werden aktuell die Vorgaben des Art. 28 Abs. 2 DS-GVO nicht erfüllt.

Diese Mängel sind zwar behebbar; dies setzt jedoch voraus, dass Zoom sich bereitfindet, geänderte Vertragsbedingungen des Kunden/Nutzenden zu akzeptieren.

@Drittstaaten-Transfer

Bedingt durch Firmensitz und Serverstandorte außerhalb der EU/EWR kommt es bei der Nutzung von Zoom zu Datentransfers, welche nach Art. 44 ff. DS-GVO einer besonderen Rechtsgrundlage bedürfen. Nach der Rechtsprechung des EuGH zur Ungültigkeit des Privacy Shield (vgl. dazu unsere Orientierungshilfe Orientierungshilfe Was jetzt in Sachen internationaler Datentransfer) genügen alleine Standarddatenschutzklauseln nicht, es bedarf vielmehr „zusätzlicher Garantien".

In Betracht kommen etwa technisch-organisatorische Maßnahmen wie eine Ende-zu-Ende-Verschlüsselung (nicht nur der Inhaltsdaten, sondern auch der sog. Meta-Daten und des Anmeldeprozesses), eine Einwilligung nach Art. 49 DS-GVO wird demgegenüber bei wiederkehrenden Datentransfers nicht ausreichen. Daher ist die Angabe von Zoom ("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. In diesen Ländern gelten möglicherweise andere Datenschutzbe stimmungen als in Ihrem Land.") nicht zielführend.

II. Technisch

@Technisch-Organisatorische Maßnahmen (TOM)

Sicherheit: 2019 wurde eine erhebliche Sicherheitslücke bekannt, die es Angreifern ermöglichte, die Kameras von Teilnehmenden zu kapern.
Anfang 2020 erlaubte ein Fehler, dass bestimmte Teilnehmende die Kontaktdaten von anderen fremden Nutzenden lesen konnten.
Seit etwa Sommer 2020 hat Zoom zahlreiche Fortschritte im Bereich der IT-Sicherheit gemacht.

@Verschlüsselung (Transport / Ende-zu-Ende Verschlüsselung)

Seit Ende Oktober 2020 wird eine Ende-zu-Ende-Verschlüsselung (E2EE) für Video-Chats angeboten; diese muss durch Nutzende jeweils aktiviert werden.

@Tracking

Tracking: ja (z.B. Google Analytics)
Desktop und Mobil-Apps übermitteln zum Prüfzeitpunkt soweit ersichtlich keine Tracking-Informationen an Drittanbieter. Allerdings enthalten sowohl die Website als auch verschickte E-Mails inklusive Einladungs-Mails zahlreiche Tracking-Elemente, z.B. für den Versuch der Protokollierung, ob Empfänger die E-Mail gelesen haben.

@Aufnahmemöglichkeit

Aufzeichnung: Ja.
AGB: „Der Host kann sich dazu entscheiden, Zoom Meetings und Webinare aufzuzeichnen. Durch die Nutzung der Dienste geben Sie Zoom Ihr Einverständ-

nis zur Speicherung von Aufzeichnungen für ein oder alle Zoom-Meetings oder Webinare, an dem (denen) Sie teilnehmen, sofern diese Aufzeichnungen in unseren Systemen gespeichert werden. Sie erhalten eine Benachrichtigung (visuell oder auf andere Weise), wenn die Aufzeichnung aktiviert ist. Wenn Sie nicht damit einverstanden sind, aufgezeichnet zu werden, können Sie sich dafür entscheiden, das Meeting oder Webinar zu verlassen."

Videokonferenzsysteme

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg (LfDI) hat Ende August 2021 verschiedene Videokonferenzsysteme (VKS) betrachtet und dazu folgende begleitende Tabelle erstellt. Informationen zum Prüfumfang finden Sie am Ende der Tabelle.

Zum Hauptdokument

	AlfaView	BigBlueButton	Cisco WebEx	GoToMeeting	Jitsi	MS Teams	Zoom
Kurzbeschreibung	[siehe Haupttext]	[siehe Haupttext]	[siehe Haupttext]	[siehe Haupttext]	[siehe Haupttext]	[siehe Haupttext]	[siehe Haupttext]
Maximale Anzahl an Teilnehmer pro Raum	„200+ Teilnehmervideos, 500 Zuschauer“, vgl. alfaview.com	• abhängig von Serverkapazität bei selbstgehostet, typischerweise 150+ • vgl. docs.bigbluebutton.org	abhängig von Lizenz generelle Limits, vgl. www.webex.com	abhängig von Lizenz generelle Limits, vgl. www.goto.com	• abhängig von Serverkapazität bei selbstgehostet • „bis zu 75 Teilnehmer“, vgl. jitsimeet.eu	abhängig von Lizenz generelle Limits, vgl. docs.microsoft.com	abhängig von Lizenz generelle Limits, vgl. support.zoom.us
Rechtlich							
Datenschutzhinweise							
- Links Links zu ggf. datenschutzrechtlichen Mustern/ Informationen des Herstellers bzw.	• alfaview.com • Link zu individuellen Datenschutzhinweisen können als Option	• bei Selbstbetrieb: müssen selbst erstellt werden • bei Fremdgehostet:	Informationen unter: • trustportal.cisco.com • trustportal.cisco.com • trustportal.cisco.com	Informationen unter: www.logmein.com	• müssen selbst erstellt werden • keine Verlinkung DS-Hinweise innerhalb	Informationen unter: • Hinweise bei Auftrags-verarbeitung: privacy.microsoft.com	Informationen unter: • zoom.us • zoom.us

ggf. Informationen über Verarbeitungen des Auftragnehmers als Verantwortlichen für eigene Zwecke bzw. gemeinsame Verantwortlichkeit, die der Verantwortliche für die Erstellung seiner DS-Hinweise nutzen kann.	eingestellt werden („Kontoverwaltung/ Datenschutzhinweise des Gastgebers“)	teilweise Vorlage vom Anbieter • keine Verlinkung DS-Hinweise innerhalb BBB vorhanden (z.B. Button) • Link kann z.B. über Änderung Variable defaultWelcomeMessage eingebunden werden			Jitsi vorhanden (z.B. Button) • Link DS-Hinweise auf Hauptseite muss auch über Änderungen eingebunden werden, vgl. www.kuketz-blog.de↗	• Hinweise für Nicht-Auftrags-verarbeitung (d.h. MS als Verantwortliche): privacy.microsoft.com↗	
- Verwendung von pbD zu eigenen Zwecken	nein [siehe Haupttext]	nein [siehe Haupttext]	ja [siehe Haupttext]	ja [siehe Haupttext]	nein, jedoch variiert bei App (siehe unten) [siehe Haupttext]	ja [siehe Haupttext]	ja [siehe Haupttext]
Auftragsverarbeitung							
- Links	alfaview.com↗		trustportal.cisco.com↗	logmeincdn .azureedge.net↗		aka.ms↗ gültig je nach Lizenz: www.microsoft.com↗	• zoom.us↗ • zoom.us↗ • zoom.us↗
Drittstaaten-Transfer	nein [siehe Haupttext]	keine Angabe bei selbstgehostet [siehe Haupttext]	ja [siehe Haupttext]	ja [siehe Haupttext]	keine Angabe bei selbstgehostet [siehe Haupttext]	ja [siehe Haupttext]	ja [siehe Haupttext]
Technisch							
Verschlüsselung (TLS) Die Transport-verschlüsselung schützt vor dem Abfangen Dritter während der Übertragung.	ja Messung BurpSuite: nur https und weitere Schutzvorkehrungen	ja Messung Browser: nur https oder wss	ja Messung Browser: nur https oder wss	ja • Messung Browser: nur https oder wss • nur AES-128-HMAC-SHA1, laut logmeincdn .azureedge.net↗ (Seite 7)	ja Messung Browser: nur https oder wss	ja Messung Browser: nur https oder wss	ja Messung Browser: nur https oder wss
Möglichkeit, Verschlüsselung Ende-zu-Ende Sie kann auch vor Einblicken des Herstellers schützen. Dieser kontrolliert jedoch auch das System und könnte gezwungen sein, Daten	nein vgl. alfaview.com↗	nein	ja laut Anbieter zumindest teilweise bei bestimmten Produktvarianten	unklar • vgl. www.goto.com↗ • assets.cdngetgo.com↗	ja laut Anbieter zumindest teilweise verfügbar, jitsi.org↗	nein	ja • laut Anbieter zumindest teilweise • Option „End-to-End-Verschlüsselung nutzen“

offenzulegen (z.B. netzpolitik.org↗). Da es insb. bei größeren Gruppen Performance-probleme geben kann, ist sie derzeit (noch) nicht marktgängig.							
Übertragung Passwort bei Login nur als Hash Dies kann vor Einblicken des Herstellers auf das Passwort schützen.	nein Messung BurpSuite: https://production-apis.alfaview.com/authentication.AuthenticationService/authenticate (im POST-Body)	nein Messung Browser: https://bbb.*/b/u/login, Form-Wert „session[password]“	nein Messung Browser: https://idbroker-eu.webex.com/idb/UI/Login, Form-Wert „IDToken2“	nein Messung Browser: https://authentication.logmein.com/login, Form-Wert „password“	entfällt keine Raumverwaltung, der erste Teilnehmer eines Raums erhält automatisch Moderationsrechte	nein Messung Browser: https://login.microsoftonline.com/*/login, Form-Wert „passwd“	nein Messung Browser: https://zoom.us/signin, Form-Wert „password“
Möglichkeit für 2FA Authentifizierung Durch Kombination von Wissen, Besitz oder biometrischen Merkmalen schützt die Zwei-Faktor-Authentisierung durch die zusätzliche Schranke besser als nur ein Merkmal.	nein	nein ja, z.B. mit Nextcloud	ja	nein	nein ja, mit Zusatzkomponente community.jitsi.org↗	ja	ja
Selbstgehostet möglich	nein	ja	nein (bei Neukunden)	nein	ja	nein	nein • Die Verarbeitung von Benutzer- und Meeting-Metadaten erfolgt stets auf den Servern des Anbieters. • Je nach Lizenz besteht die optionale Möglichkeit, die Übermittlung von Video- und Audio-Daten sowie Dateien über eigene Server durchzuführen. • Eine Teilnahme per Web-Browser oder Telefon ist damit nicht möglich. vgl.

							support.zoom.us↗
Fremdgehostet möglich	ja	ja	ja	ja	ja	ja	ja
Verarbeitung nur in Europa Insb. durch Serverstandorte bzw. Zugriffe von (Unter-) Auftragnehmern in/aus Drittstaaten können Anforderungen aus Kapitel 5 DS-GVO zu beachten sein.	ja alfaview.com↗	keine Angabe bei selbstgehostet	nein trustportal.cisco.com↗ (Seite 3)	nein • USA, Europa, Asia-Pacific (APAC) • logmeincdn .azureedge.net↗ (Seite 1)	keine Angabe bei selbstgehostet	nein • u.a. USA • go.microsoft.com↗	nein • USA, Kanada, Europa, Asia-Pacific (APAC) • zoom.us↗
Telefonische Teilnahme möglich	nein	ja mit SIP-Provider	nein ja, je nach Lizenz	ja	nein • nur mit Zusatz-komponente „jigasi“ • mit SIP-Provider	ja	ja
Teilnahme ohne Installation von Anwendung (=Web-Client) Durch die Installation von Anwendungen bzw. Apps wird Code von Dritten auf dem eigenen Gerät ausgeführt und hat i.d.R. umfangreiche Zugriffsmöglichkeiten, teilweise auch bei Nicht-Nutzung. Die Nutzung einer Browser-Version kann hierbei aus Sicherheitsgründen und zur besseren Kontrolle von Datenflüssen vorzugswürdig sein.	nein	ja Nur Web-Client, kein Desktop- oder Mobil-Client vorhanden	ja Download der Desktop-Anwendung startet automatisch.	ja • jedoch nicht mit Safari-Browser • Button „An Meeting Im Browser Teilnehmen“	ja	ja • Button „Stattdessen die Web-App verwenden“ • jedoch nicht mit Safari-Browser mit Standard-Einstellungen, vgl. support .microsoft.com↗	ja umständlich („Meeting eröffnen/ Jetzt herunterladen/ Haben Sie Probleme mit Zoom Client/ Mit Ihrem Browser anmelden“)
Teilnahme ohne Erstellung Account (=Gast) Sofern die Möglichkeit besteht, dass durch den Gastzugang keine Unbefugten teilnehmen können, ist das Angebot eines Gastzugangs als	ja • ok: Gast-Einladung über „Raumverwaltung/ Gruppenlinks“ erstellen • Messung: Einladungs-	ja je nach Administrations-Oberfläche, bei Standard-komponente „Greenlight“ einstellbar	ja • durch Weitergabe Zugangsdaten oder Eintragung E-Mailadresse • Messung: Einladungs-emails enthalten keine	ja Button „Einladungslink verschicken“	ja	ja Button „Einladung teilen/ Besprechungslink kopieren“	ja Einstellung „Nur berechtigte Nutzer können vom Web-Client aus an Meetings teilnehmen“

datenschutzfreundlicher anzusehen, da hier weniger personen-bezogene Daten (z.B. E-Mailadresse) verarbeitet werden.	emails über „Raumverwaltung/ Gastlinks“ enthalten Tracking-Links über *.sendibt3.com und Drittanbieter-Inhalte von fonts.googleapis.com; *.sendibt2.com; *. sendibt3.com; fonts.gstatic.com		Tracking-Links oder Drittanbieter-Inhalte • Gastnutzung einstellbar über Einstellung „Meeting ansetzen/ Registrierung/ Erforderlich“				
Möglichkeit, Teilnahme mit Video/Ton aus (=Zuhörer) Ggf. ist es bei bestimmten Meeting-Formaten ausreichend als Zuhörer teilzunehmen. Die Software sollte dies nicht aktiv unterbinden.	ja Anzeige Videobild anderer Teilnehmer nur möglich, wenn man selbst sein Video aktiviert (verfolgt das Prinzip „Siehst du mich, sehe ich dich“), vgl. support.alfaview.com	ja • Einstellbar pro Raum bei Standard-Admin-Oberfläche „Greenlight“ • Einstellbar global mit Variable „muteOnStart“	ja	ja	ja • Einstellung „Alle Personen treten stumm geschaltet bei“ • Einstellung „Alle Personen treten ohne Video bei“	ja Button „Ohne Audio und Video fortfahren“	ja Einstellung „Teilnehmer beim Beitritt stumm“
Möglichkeit, Hintergründe zu verpixeln Ggf. kann es in einem Meeting ausreichend sein, den Hintergrund auszutauschen bzw. unscharf zu stellen.	nein	nein	nein ja, bei Desktop-Version	nein	ja	nein ja, bei den meisten Desktop-Versionen	ja Button „Settings/ Background“
Möglichkeit, Videobild einzugrenzen Ggf. kann es in einem Meeting ausreichend sein, den Bildausschnitt der Kamera allein auf die Person zu begrenzen.	nein	nein	nein	nein	nein	nein	nein
Möglichkeit, Videobild einzufrieren Ggf. kann es in einem Meeting ausreichend sein, ein Standbild aufzunehmen und für	nein	nein	nein	nein	nein	nein	nein

Zeiträume nur dieses Foto zu übertragen (Avatar).							
Löschfunktion VK-Inhalte (z.B. Chat) z.B. nach Ende	unklar	ja • Chat löschbar während Meeting • Standardmäßig Speicherung viele Logfiles bei BBB docs.bigbluebutton.org↗ • je nach Frontend kann Löschung automatischer Aufnahmen von Meetings notwendig sein docs.bigbluebutton.org↗	unklar Chat nicht löschbar während Meeting	unklar Chat nicht löschbar während Meeting	unklar Chat nicht löschbar während Meeting	unklar Chat nicht löschbar während Meeting	unklar Chat nicht löschbar während Meeting
Möglichkeit zur Auswertung (Stichworte: Analytics, Reporting)	nicht bekannt	nicht bekannt	ja je nach Lizenz Möglichkeit Auswertung Videokonferenz help.webex.com↗	ja verschiedene Möglichkeit Auswertung Videokonferenz support.goto.com↗	nicht bekannt	ja je nach Lizenz Möglichkeit Auswertung Videokonferenz docs.microsoft.com↗	ja je nach Lizenz Möglichkeit Auswertung Videokonferenz support.zoom.us↗
Übertragung Video/Ton ohne Zustimmung Teilnehmer (Unmute)	nicht festgestellt	nicht festgestellt • Serverseitige Einstellung „allowModsTo UnmuteUsers“ erlaubt Unmute durch Moderator (Gefahr: Überwachungs-Sensor) • Mutefunktion wurde erst seit Bugfix (15.09.2020) von Serverseitig auf Clientseitig umgestellt: github.com↗	nicht festgestellt	nicht festgestellt • Funktion „Sprach-erkennung bei Mute“ führt trotz Mute von Mikrofon bei Geräuschen zu Hinweis „Sie sind stummgeschaltet. Um die Stummschaltung aufzuheben, können Sie jederzeit die Mikrofontaste betätigen“ • unklar, ob Erkennung clientseitig/ serverseitig	nicht festgestellt • Funktion „Sprach-erkennung bei Mute“ nach unserem Verständnis clientseitig, vgl. github.com↗. Verwendung Funktion ist auf dem Server einstellbar mit „enableTalk WhileMuted“. • Mod für Unute existiert: community.jitsi.org↗	nicht festgestellt microsoftteams.uservoice.com↗	nicht festgestellt Teilnehmer kann einzeln erklären, dass Dritter unmute durchführen darf, vgl. support.zoom.us↗
Anzeige Teilnehmerliste	ja	ja	ja	ja	ja	ja	ja Button unten „Teilnehmer“

Anzeige Ein/Austritt	ja kein Popup, Information durch Aktualisierung Teilnehmerliste, laut Anbieter ist eine Einstellung zu Ton bei Beitritt vorhanden	ja muss innerhalb eines Meeting vom Teilnehmer einzeln für sich eingestellt werden	ja • ob Tonsignal ertönt ist einstellbar über Einstellung „Teilnehmer-einstellungen/ Ton bei Beitritt und Verlassen“	ja	nein	unklar bei Nutzung Warteraum ertönt jedenfalls ein Tonsignal	unklar • ja, bei Warteraum Popup • ansonsten: kein Popup, Information nur durch Aktualisierung Teilnehmerliste
Darstellung Mikrofon aktiviert Nutzenden wird verständlich dargestellt, dass Ton übermittelt wird.	ja • blauer Rahmen um Videobild, vgl. support.alfaview.com	ja • Mikrofonsymbol in Teilnehmerliste • Anzeige welcher Teilnehmer spricht	ja • Mikrofonsymbol in Teilnehmerliste • Anzeige welcher Teilnehmer spricht	ja • Mikrofonsymbol in Teilnehmerliste • Mikrofonsymbol blau • Mikrofonsymbol oben links	ja Blaue Anzeige Pegel oben rechts	ja Mikrofonsymbol in Teilnehmerliste	ja Mikrofonsymbol unten links mit Anzeige Pegel
Darstellung Kamera aktiviert Nutzenden wird verständlich dargestellt, dass Bilddaten übermittelt werden.	ja Anzeige eigenes Kamerabild	ja Anzeige eigenes Kamerabild	ja • Anzeige eigenes Kamerabild • Kamerasymbol in Teilnehmerliste	ja • Anzeige eigenes Kamerabild • Kamerasymbol in Teilnehmerliste • Kamerasymbol blau	ja Anzeige eigenes Kamerabild	ja Anzeige eigenes Kamerabild	ja • Anzeige eigenes Kamerabild • Kamerasymbol in Teilnehmerliste
Darstellung Aufnahme aktiviert Nicht getestet, daher bei allen VKS die diese Funktion bieten „unklar“.	entfällt Funktion nicht vorhanden	unklar serverseitig deaktivierbar	unklar	unklar	unklar	unklar	unklar laut AGB „Benachrichtigung (visuell oder auf andere Weise)“
Moderatoren-funktionen	ja	ja	ja	ja	ja	ja	ja
- Funktion 'Teilnehmer entfernen'	ja Button „Aus dem Raum entfernen“	ja	ja Button „Ausschließen“	ja	ja	ja Button „Aus Besprechung entfernen“	ja
- Funktion 'Teilnehmer umbenennen'	nein	nein	ja, nur bei Telefonteilnehmern	ja, nur bei Telefonteilnehmern	nein	nein microsoftteams.uservoice.com	ja
- keine Funktion 'Teilnehmer zu	ja	ja	ja	ja	ja	ja	nein

Video auffordern'							Button „Video starten anfordern“
Rollenkonzept Im DSK-Papier zu VKS datenschutzkonferenz-online.de↗ sind verschiedene Rollen aufgeführt, die bei einem VKS vorhanden sein sollten.	ja Rollen: „Admin, Moderator, Teilnehmer, Zuschauer, Gast, kein Zugang“	ja bei Standard-Admin-Oberfläche „Greenlight“ einstellbar	ja help.webex.com↗	ja • Rollen „Organisator/ Moderator“ und Teilnehmer • support.goto.com↗	unklar	ja • Rollen „Organisator, Moderator, Teilnehmer“, vgl. support.microsoft.com↗ • können individuell geändert oder ergänzt werden, vgl. docs.microsoft.com↗	ja • ab höherer Accountstufe (nicht für „Basisplan“) • Rolle „Host“ • support.zoom.us↗
Möglichkeit, Raum per Passwort zu schützen ob ein Passwort als zusätzliche Schranke neben der Eingabe der Einwahldaten erforderlich gemacht werden kann	nein	ja	ja	ja Button „Require a meeting password“	ja	nein microsoftteams.uservoice.com↗	ja
Warteraum einzeln freigeben ob Personen einzeln aus dem Wartebereich in das Meeting hereingelassen werden können	nein keine Warteraumfunktion vorhanden	ja Einstellung „Freigabe durch Moderator bevor der Raum betreten werden kann“ und Fenster „Wartende Teilnehmer“ im Meeting	ja	nein, nur generell möglich Button „Sitzung sperren“, „Es wartet jemand“, „Sitzung entsperren“	ja vgl. community.jitsi.org↗	ja	ja
Möglichkeit, einzuschränken wer Video aktivieren kann	ja als Moderation mit Button „Kamera erlauben“, vgl. support.alfaview.com↗	ja • Button „Teilnehmer-rechte einschränken“ • Button „Teilnehmer-rechte einschränken/ Webcam freigeben/ Teilnehmer freigeben“	unklar Einstellung „Meeting ansetzen/ Meeting-Optionen“	unklar	nein	ja • Festlegung einer „meeting policy“ möglich, docs.microsoft.com↗ • als Moderation mit Button „Kamera deaktivieren“ • Festlegung einer „meeting policy“ möglich, docs.microsoft.com↗	ja • Option „Video Moderator ein/aus“ • Option „Video Teilnehmer ein/aus“
Möglichkeit Beschränkung Teilnehmer auf bestimmte Länder	nein	nein ja, mit Zusatzkomponente	nein	unklar	nein ja, mit Zusatz-komponente	nein abhängig von Lizenz, vgl. techcommunity.microsoft.com↗	ja Option „Genehmigen oder blockieren Sie den Beitritt für Besucher aus bestimmten Ländern/

							Regionen“
Möglichkeit für Drittanbieter-Verknüpfung Durch Einbindung von Drittanbietern kommt es im Regelfall zu zusätzlichen Verarbeitungen und weiteren Empfängern personenbezogener Daten, die zu prüfen sind.	nein	entfällt	Cisco Drittanbieter-Integration help.webex.com↗	GoTo MarketPlace www.goto.com↗	entfällt	Teams App Store docs.microsoft.com↗	Marketplace marketplace.zoom.us↗
- Datenschutz-hinweise im Store Ohne Kenntnis des Sachverhalts kann keine datenschutzrechtliche Prüfung durch den Verantwortlichen erfolgen. Gerade wenn ein VKS einfach per Klick des Admins mit Zusatz-angeboten von Dritten („Apps“) erweitert werden kann, muss der Hersteller als Store-Betreiber sich darum bemühen, dass der Verantwortliche auch über die Verarbeitungen von Zusatzangeboten Dritter Kenntnis erlangen kann (vgl. ec.europa.eu↗, S. 29f.) Aus unserer Sicht ist zwingend vorzuschreiben, dass Datenschutzhinweise (mit Informationen nach DS-GVO) verlinkt werden.	entfällt	entfällt	unklar	unklar	entfällt	ja, verlinkt (zumeist US-Recht) appsource.microsoft.com↗	ja, verlinkt (zumeist US-Recht)
- Berechtigungs-konzept im Store Ergänzend zu vorheriger Zeile bedürfen aus unserer Sicht Stores, die eine	entfällt	entfällt	unklar	unklar	entfällt	ja, teilweise docs.microsoft.com↗	ja, Kategorien

Weitergabe pbD an Dritte (die Zusatzangebote zur Erweiterung des VKS vorsehen) ermöglichen, Kontrollsysteme (z.B. Berechtigungssystem mit Steuerung, welche Datenkategorien aus dem VKS für das Zusatzangebote weitergeben werden oder Historie, welche pbD für das Zusatzangebot an Dritte weitergegeben wurden).							
keine Möglichkeit zur Aufnahme Der Einsatz einer Aufnahmefunktion durch den Verantwortlichen ist neben datenschutzrechtlichen Anforderungen (insb. Rechtsgrundlage) auch mit Hinblick auf die strafrechtliche Norm § 201 StGB zu prüfen.	ja	nein • über eine serverseitige Einstellung bzw. Einstellungen in der Administrations-Oberfläche zur Einrichtung von Meetings (z.B. „Greenlight“) ist eine automatische Aufnahme möglich • vgl. docs.bigbluebutton.org↗	nein vgl. www.webex.com↗	nein Button „Sitzung aufzeichnen“	nein • Option „Aufnahme starten“ • standardmäßig Speicherung nur auf Dropbox möglich, vgl. community.jitsi.org↗, andere Anbieter mit Zusatzkomponente „Jibri“	nein Button „Aufzeichnung beginnen“	nein • Einstellung „Meeting automatisch auf dem eigenen Computer aufzeichnen“ • ab höherer Accountstufe „Cloud Aufzeichnung“ möglich • vgl. auch support.zoom.us↗ ff.
keine Möglichkeit für automatische Transkription Die automatische Transkription bedarf im Regelfall technisch eine Aufnahme des gesprochenen Wortes (s. oben „Möglichkeit zur Aufnahme“) und Verarbeitung als pbD durch Sprach-erkennungssysteme beim Hersteller.	nein vgl. alfaview.com↗	ja	nein vgl. www.webex.com↗	nein • je nach Lizenzmodell • support.goto.com↗	ja	ja für englische Sprache verfügbar, vgl. support.microsoft.com↗	nein • je nach Lizenzmodell • support.zoom.us↗
keine Aufmerksamkeits-erkennung	ja	ja	nein help.webex.com↗	ja	ja	ja	ja „Aufmerksamkeits-

							verfolgung“ wird nicht mehr angeboten, vgl. zoom.us↗
keine Verbindung Browser							
- mit Drittanbietern	entfällt kein Web-Client vorhanden für Desktop-Client: ja, keine Verbindungen mit Drittanbietern bei Messung mit BurpSuite festgestellt	ja Messung Browser	nein Messung Browser bei Nutzung eines Testaccounts: *.amplitude.com, *.appdynamics.com, *.ciscospark.com, *.cloudflare.com, *.cloudfront.net, *.eum-appdynamics.com, *.fontawesome.com, *.googleapis.com, *.jquery.com, *.launch, *.polyfill.io, *.walkmeusercontent.com, *.wbx2.com, *.webex.com	nein Messung Browser bei Nutzung eines Testaccounts • Während Meeting: pusher.com; sentry.io; expertcity.com; getgo.com; goto-rtc.com; gotomeeting.com • Vor/Nach Meeting: appcues.com; appcues.net; castle.io; cloudflare.com; doubleclick.net; google-analytics.com; google.com; google.de; googletagmanager.com; goto.com; gstatic.com; gotomeet.me; imperium.com; jwplatform.com; launchdarkly.com; logmeininc.com; marketo.net; mixpanel.com; mktoresp.com; mxpnl.com; unpkg.com; qualtrics.com	ja	ja, aber viele mit Anbieter Messung Browser: *.aspnetcdn.com; *.live.com; *.microsoft.com; *.microsoftazuread-sso.com; *.microsoftonline.com; *.msauth.net; *.msecnd.net; *.msftauth.net; *.msftauthimages.net; *.office.com; *.office.net; *.sharepointonline.com; *.skype.com; *.unpkg.com; *.visualstudio.com	nein Messung Browser: *.wootrics.com, fonts.gstatic.com, nws.zoom.us, *.sentry.io, *.ada.support, www.google.com (recaptcha), zoom.us, *.cloud.zoom.us
- mit 'bekannten Trackern' Im Allgemeinen fallen darunter Angebote zur Webanalyse, insb. die geräte- und dienstübergreifend pbD verarbeiten oder das Nutzerverhalten erfassen und protokollieren.	nein	nein	ja Messung Browser: zumindest amplitude.com	nein Messung Browser: zumindest google-analytics.com	ja	nein	nein

keine Kenntnis von Einbindung 'bekannter Trackern' in mobiler App Im Allgemeinen fallen darunter Angebote zur Verhaltens-Analyse, insb. solche die geräte- und dienstübergreifend pbD verarbeiten oder das Nutzerverhalten erfassen und protokollieren.	ja laut reports.exodus-privacy.eu.org	entfällt keine Anwendung vorhanden	nein laut reports.exodus-privacy.eu.org	nein laut reports.exodus-privacy.eu.org	variiert • Google Play Store Version: nein • F-Droid Version: ja siehe reports.exodus-privacy.eu.org jeweils zu Version mit „google“ bzw. „froid“	nein laut reports.exodus-privacy.eu.org	nein laut reports.exodus-privacy.eu.org
Beschreibung toM in Auftrags-verarbeitung	ja • Anlage 1 • alfaview.com	keine Angabe bei selbstgehostet	ja • Attachment A • trustportal.cisco.com	unklar Verweisung www.logmein.com Filter nach „GoToMeeting“ auf • logmeincdn .azureedge.net • logmeincdn .azureedge.net • logmeincdn .azureedge.net • logmeincdn .azureedge.net alter Stand 2017: logmeincdn .azureedge.net	keine Angabe bei selbstgehostet	ja • unklarer Verweis auf „eine Microsoft-Sicherheits-richtlinie“ (kein Link) und u.a. Einhaltung ISO-Standards in DPA • aka.ms, Anlage „Anhang A – Sicherheitsmaßnahmen“	ja • EXHIBIT B • zoom.us
Historie, z.B. Presseberichte, CVE-Einträge Hinweise auf Meldungen mit Sicherheitsvorfällen und ähnlichem		• www.cvedetails.com • Pressebericht 21.10.2020 www.golem.de zu verschiedenen Sicherheitsproblemen. Kritikpunkte waren die unsichere Einbindung von LibreOffice, das Setzen von Cookies ohne secure-Flag (beide behoben mit Version 2.2.27) und die Verwendung von Ubuntu 16.04 (Unterstützung bis April 2021) und alten	www.cvedetails.com		www.cvedetails.com	www.cvedetails.com	• www.cvedetails.com • 2019 wurde eine erhebliche Sicherheitslücke bekannt, die es Angreifer*innen ermöglichte, die Kameras von Teilnehmer*innen zu kapern. Anfang 2020 erlaubteb ein Fehler, dass bestimmte Teilnehmer die Kontaktdaten von anderen fremden Nutzer*innen lesen

		Node.js-Versionen.				konnten. • Seit etwa Sommer 2020 hat Zoom zahlreiche Fortschritte im Bereich der IT-Sicherheit gemacht.

Stand 24.08.2021 mit Berichtigung vom 08.12.2021; Sachverhalte können sich seit diesem Datum geändert haben und der Tabelleninhalt veraltet sein. Erläuterungen innerhalb der Tabelle sind mit Ziel der allgemeinen Verständlichkeit verkürzt und nicht vollständig.

Es wurden grundsätzlich die Browser-Versionen getestet, sofern nicht anders angegeben. Nutzende haben in dieser mehr Möglichkeiten der Kontrolle als bei Desktop-Anwendungen oder Mobil-Apps. Grundsätzlich wurde die kostenlose Version der Dienste geprüft und je nach Lizenz kann sich der Funktionsumfang unterscheiden.

Bedeutung der Angaben:
ja: Dargestellte Eigenschaft oder Funktionalität ist vorhanden, das ist in Bezug auf Datenschutz grundsätzlich positiv
nein: Dargestellte Eigenschaft oder Funktionalität ist nicht vorhanden, das ist in Bezug auf Datenschutz grundsätzlich negativ
unklar: Dargestellte Eigenschaft oder Funktionalität wurde nicht abschließend geprüft oder konnte nicht geprüft werden
keine Angabe: z.B. bei selbstgehosteten Diensten ist keine Angabe möglich, da abhängig von Installation
entfällt: Da eine für die Eigenschaft oder Funktionalität notwendige Voraussetzung fehlt, entfällt eine Prüfung

Der Landesbeauftragte für
Datenschutz und
Informationsfreiheit
Baden-Württemberg