FORUM

Vergleich von Videokonferenz-Software

Unter dem Aspekt des Datenschutzes und der IT-Sicherheit

MORGENSTERN Rechtsanwaltsgesellschaft mbH

Sehr geehrte Leserin,
sehr geehrter Leser,

durch die aktuelle Situation der Corona-Krise und die dadurch vermehrte Arbeit im Home-Office, hat sich die betriebsinterne Zusammenarbeit mit Hilfe von Online-Tools verändert.

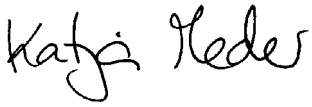
Insbesondere Meeting-Tools werden verwendet, um die Zusammenarbeit von mehr als zwei Personen zu vereinfachen wenn diese sich im Home-Office befinden.

Mittlerweile haben sich einige Anbieter mit Softwareprodukten auf dem Markt positioniert, allerdings eignet sich nicht jedes Tool für alle Zwecke.

In dem nachfolgenden Whitepaper vergleicht der Autor die Video-Software unter Berücksichtigung von Datenschutz und IT-Sicherheit.

Der Inhalt dieses Whitepapers wurde freundlicherweise von der MORGENSTERN Rechtsanwaltsgesellschaft mbH zur Verfügung gestellt.

Freundliche Grüße



Katja Meder
Bereichsleiterin Recht
FORUM · Institut für Management GmbH

Vergleich von Videokonferenz-Software

Viele Unternehmen versuchen, die aktuelle Situation der Corona-Krise mit Hilfe von Online-Tools, insbesondere Meeting-Software abzufedern. Hierdurch kann die betriebsinterne Zusammenarbeit auch mit mehr als zwei Personen nahtlos weitergeführt werden, auch wenn diese sich im Home-Office befinden.

Es haben sich bereits einige Anbieter mit Videokonferenz-Softwareprodukten auf dem Markt positioniert. Allerdings eignet sich nicht jedes Tool für alle Zwecke. Je nach Vertraulichkeit der besprochenen Inhalte sind unterschiedliche Anforderungen zu stellen. Nach Ansicht einiger Aufsichtsbehörden (Berlin und Baden-Württemberg) sind Lösungen, die auf eigenen Rechnern bzw. in eigenen Rechenzentren, also „On-Premise“ verwendet werden soweit möglich vorzuziehen. Außerdem sind laut diesen Aufsichtsbehörden grundsätzlich Telefonkonferenzen vorzuziehen, wenn die Durchführung einer Videokonferenz nicht erforderlich ist. Auch zu beachten ist, dass gerade die technisch gut ausgestatteten Dienste (z. B. Zoom) enormer Kritik in Bezug auf den Datenschutz ausgesetzt sind und von Datenschutzbehörden auch teilweise als datenschutzwidrig angesehen werden. Die gängigsten Tools werden nachfolgend unter Aspekten des Datenschutzes sowie der IT-Sicherheit geprüft.

I. Generelle Vorüberlegungen bei der Verwendung von Videokonferenz-Software

1. Datenschutzrechtliche Aspekte

Die datenschutzrechtliche Zulässigkeit eines Software-Einsatzes kann nicht abstrakt vom jeweiligen Zweck und Einsatzbereich sowie den genutzten Funktionen beurteilt werden. Für jede Software und die darin enthaltenen Funktionen muss der Verantwortliche dokumentiert nachweisen können, dass die Verarbeitung personenbezogener Daten mit der Software auf eine konkrete Rechtsgrundlage gestützt werden kann und mindestens folgende Voraussetzungen erfüllt:

- Der mit dem Einsatz der Software oder der konkreten Funktion verfolgte Zweck ist zulässig und legitim.
- Die Software bzw. Funktion eignet sich, um den verfolgten Zweck zu erfüllen.
- Es gibt keine datenschutzfreundlicheren Alternativen, die ebenso effektiv zum gleichen Ziel führen.
  - Datenschutzfreundlicher können regelmäßig Videokonferenzen mit Standbild statt Videoübertragung, reine Telefonkonferenzen, Messenger, E-Mails, etc. sein.
  - Wenn nur zwei Personen miteinander kommunizieren, kann ein Telefonat oft ausreichen. Bei mehreren Teilnehmern gestalten sich Telefonkonferenzen schwieriger, sodass Videokonferenzen die effektivere Maßnahme darstellen können.
- Es können ausreichende technische und organisatorische Schutzmaßnahmen ergriffen werden, um die Betroffenendaten zu schützen.

Neben diesen allgemeinen Voraussetzungen sind außerdem die spezifischen Anforderungen der jeweiligen Rechtsgrundlage zu beachten, insbesondere, wenn sensible Daten gemäß Art. 9 DS-GVO (z. B. Daten zur Gesundheit, Religion, Gewerkschaftszugehörigkeit) verarbeitet werden sollen. In technischer Hinsicht setzt die DS-GVO voraus, dass der Datenschutz bereits durch die Technikgestaltung und datenschutzfreundliche Voreinstellungen erreicht wird (Art. 25 DS-GVO, Privacy by Design und Privacy by Default). Da Verantwortliche

als Nutzer auf dieser Ebene von den vorhandenen Software-Voreinstellungen abhängig sind, haftet der Verantwortliche für die Auswahl des Tools in Bezug auf das damit erreichte Datenschutzniveau.

- In Anbetracht der unterschiedlichen Anforderungen an die Software, vor allem bezüglich der Vertraulichkeit der besprochenen Inhalte, sollten im Einzelfall unter datenschutzrechtlichen Gesichtspunkten insbesondere folgende Aspekte bei der Software-Auswahl berücksichtigt werden:
- Die Mitteilung welche personenbezogenen Daten setzt die Software zur Teilnahme an einer Konferenz/einem Meeting voraus?
- Wie wird gewährleistet, dass nur die gewünschten Teilnehmer sich in eine Konferenz einwählen können? (Beschränkung des Zugangs)
- Werden Daten vom Anbieter zu eigenen Zwecken genutzt oder an Dritte übermittelt? (insbesondere Daten über den Nutzer, ausgetauschte Daten, Inhaltsdaten wie Video- und Audioströme, Metadaten wie Nutzungszeiten, Kontakte und Aufenthaltsorte der Nutzer). Wird die Software auf EU-Servern betrieben oder in Drittländern? Wenn Betrieb, Übermittlung oder Speicherung in Drittländern: Entspricht das Datenschutzniveau der DS-GVO?
- Wann werden Aufzeichnungen, Chatverläufe, Transkripte oder ausgetauschte Dateien gelöscht? (möglichst nach Ende des Gesprächs bzw. nur so lange, wie sie erforderlich sind)
- Welche Verfahrens- und Einstellungsmöglichkeiten (v.a. in Bezug auf die Datenschutzfreundlichkeit) stehen zur Verfügung?
- Sind die Verantwortlichkeiten und datenschutzrechtlichen Rollen geklärt und entsprechende Verträge abgeschlossen?
  - Immer, wenn die Meeting-Software nicht auf der eigenen IT-Infrastruktur erbracht wird, sondern beim Anbieter (SaaS) kommt das Vorliegen einer Auftragsverarbeitung in Betracht.
    - Liegt eine Auftragsverarbeitung vor, ist ein dem Art. 28 DS-GVO entsprechender Auftragsverarbeitungsvertrag abzuschließen. Seriöse Anbieter bieten eigene Standardverträge an, die den gesetzlichen Anforderungen entsprechen.
  - Wenn der Anbieter die Daten des Verantwortlichen auch zu eigenen Zwecken verarbeitet, kommt das Vorliegen einer gemeinsamen Verantwortlichkeit in Betracht (z. B. für Produktaktualisierungen, zur Problembehandlung, zur Personalisierung von Produkten und Bereitstellung von Empfehlungen).
    - Liegt eine gemeinsame Verantwortlichkeit vor, ist ein dem Art. 26 DS-GVO entsprechender Vertrag abzuschließen.

Wenn die Datenverarbeitung in einem Drittstaat stattfindet, liegt regelmäßig eine Drittstaatenübermittlung vor, weshalb die speziellen Anforderungen der Art. 44 ff. DS-GVO eingehalten werden müssen. Die Drittstaatenübermittlung darf nur erfolgen, sofern eine der folgenden Voraussetzungen erfüllt ist:

- Angemessenheitsbeschluss nach Art. 45 DS-GVO
- Geeignete Garantien nach Art. 46 DS-GVO (z. B. verbindliche interne Datenschutzvorschriften, Standarddatenschutzklauseln, genehmigte Verhaltensregeln

Es gibt auch Fälle, in denen eine Drittstaatenübermittlung ohne besondere Vorkehrungen zulässig ist. Das ist z. B. der Fall, wenn für einen Mitarbeiter ein Hotel in einem Drittstaat gebucht wird, weil dieser dort an einer Konferenz teilnehmen muss. Die Weitergabe der Personenstammdaten des Mitarbeiters ist hier erforderlich, damit dieser seiner Tätigkeit nachkommen kann. Solche Ausnahmen nach Art. 49 DS-GVO sind hier grundsätzlich nicht ersichtlich

Der Anbieter von Meeting-Software sollte also möglichst seinen Sitz entweder in der EU, in einem EWR-Staat oder ein einem Drittstaat mit gleichwertigem Datenschutzniveau haben. Über die Angemessenheit des Datenschutzniveaus i.S.d. Art. 45 DS-GVO entscheidet die EU-Kommission in einem Beschluss. Diese Beschlüsse können unter https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_de abgerufen werden.

Soweit Datenübermittlungen in die USA erfolgen, wird darauf hingewiesen, dass bei Unternehmen, die über ein sog. Privacy-Shield-Zertifikat verfügen, rechtlich von einem angemessenen Datenschutzniveau im Sinne der DS-GVO ausgegangen werden kann. Der Beschluss der EU-Kommission zur Gleichwertigkeit des Datenschutzniveaus in den USA bezieht sich aber nur auf Unternehmen, die sich durch eine Selbstzertifizierung beim US-Handelsministerium zur Einhaltung des EU-US-Privacy-Shields verpflichtet haben. Eine Liste der zertifizierten Unternehmen kann unter www.privacyshield.gov/list aufgerufen werden. Soweit Beschäftigtendaten betroffen sind, sollte darauf geachtet werden, dass das Unternehmen auch für diese zertifiziert ist („Non HR“ oder „HR“). Die Wirksamkeit des EU-US-Privacy-Shields ist umstritten und Gegenstand eines beim EuGH anhängigen Verfahrens gegen Facebook („Schrems II“). Stand jetzt ist es aber gültig und kann als Grundlage für die Übermittlung von personenbezogenen Daten in die USA herangezogen werden.

Trotz Zertifizierung ist der Einsatz eines Dienstleisters in den USA mit einem Restrisiko verbunden, da aufgrund des CLOUD-Acts (Clarifying Lawful Overseas Use of Data Act) für US-Behörden unter bestimmten Voraussetzungen die Möglichkeit besteht, auch auf in der EU gelegene Daten zuzugreifen. Das Gesetz verpflichtet die europäischen Unternehmen dazu, den US-Behörden Zugriff auf die Daten zu gewähren, auch wenn diese in der EU gespeichert sind. Der Zugriff würde z. B. dort gespeicherte Meetings betreffen (Video und Audio). Vor diesem Hintergrund sollten EU-Unternehmen grundsätzlich vorgezogen werden soweit es möglich ist und soweit besonders vertrauliche, sensible oder einem Berufsgeheimnis unterliegende Daten verarbeitet werden.

Aufzeichnungs- und Screensharingoptionen, Tracking- und Beobachtungsfunktionen

Viele Software-Lösungen stellen die Option zur Aufzeichnung oder zum Teilen des Bildschirms zur Verfügung. Die Erforderlichkeit des Einsatzes dieser Funktionen ist immer im konkreten Einzelfall nach den oben beschriebenen Kriterien zu bewerten. Das gilt ebenso für Funktionen zum Tracken und Beobachten der Aktivität der Teilnehmer. Es kann nicht pauschal von einer Unzulässigkeit oder Zulässigkeit ausgegangen werden.

2. Weitere datenschutzrechtliche Pflichten

Rechenschaftspflicht, Art. 5 Abs. 1 DS-GVO: Nach Art. 5 Abs. 2 DS-GVO ist der Verantwortliche verpflichtet, die Einhaltung der Datenschutzgrundsätze nachweisen zu können. Etwaige Erforderlichkeitsprüfungen sollten mit Blick auf die Rechenschaftspflicht des Verantwortlichen dokumentiert werden.

Pflichtinformationen, Art. 13 DS-GVO: Der Verantwortliche ist verpflichtet, die Meeting-Teilnehmer vor dem Einsatz der Meeting-Software gemäß Art. 13 DS-GVO über die Zwecke, Arten und den Umfang der personenbezogenen Daten, die im Rahmen des Meetings konkret verarbeitet werden, zu informieren. Ein weiterer Aspekt ist daher auch, ob es eine Möglichkeit gibt, diese Pflichtinformationen („Datenschutzhinweise“) innerhalb der Software oder anderweitig einzubinden und den Betroffenen rechtzeitig (vor Erhebung der Daten) zugänglich zu machen. Es muss insbesondere darüber aufgeklärt werden, ob eine Drittstaatenübermittlung erfolgt und welche konkreten Maßnahmen zum Datenschutz durchgeführt werden (z. B. Privacy Shield und Standardvertragsklauseln). Die Nutzer müssen sogar die Möglichkeit erhalten, sich diese Maßnahmen durchzulesen.

Verzeichnis von Verarbeitungstätigkeiten: Zur Vervollständigung der Datenschutzdokumentation sind der Einsatz der Meeting-Software und die damit verbundenen Verarbeitungsprozesse in einem Verzeichnis der Verarbeitungstätigkeiten (Art. 30 DS-GVO) aufzunehmen.

Sensibilisierung der Mitarbeiter: Mitarbeiter sind bei der Verwendung der Tools datenschutzrechtlich dahingehend zu sensibilisieren, welche Tools für welche Zwecke verwendet werden dürfen und vor allem welche Daten über die Tools geteilt werden dürfen (z. B. über die Funktion „Desktop/Bildschirm teilen“). Soweit

die Mitarbeiter personenbezogene Daten z. B. zur Anlegung eines Nutzerprofils angeben müssen, sind diese auch darauf hinzuweisen, dass nur die betriebliche E-Mail-Adresse und Telefonnummer anzugeben ist sowie darauf, dass ein sicheres Passwort ausgewählt werden soll.

Datenschutz-Folgenabschätzung, Art. 35 DS-GVO: Im Einzelfall kann ein Verantwortlicher vor dem Einsatz einer Meeting-Software zur Durchführung einer Datenschutz-Folgenabschätzung verpflichtet sein. Das ist dann der Fall, wenn die Datenverarbeitung mit der Meeting-Software voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der Betroffenen mit sich bringt. Das ist im Einzelfall für die konkrete Software und die konkreten Zwecke zu entscheiden. Zu beachten ist, dass die Entscheidung, dass eine Datenschutz-Folgenabschätzung nicht vorgenommen werden muss, zu dokumentieren ist.

Technische und organisatorische Maßnahmen, Art. 32 DS-GVO: Die „datenschutzkonformsten“ Meeting-Lösungen bringen nichts, wenn das Unternehmen nicht auch selbst dafür sorgt, dass geeignete technische und organisatorische Maßnahmen durchgeführt werden. Zwar sollte eine Software die datenschutzfreundlichsten Einstellungen bereits voreingestellt haben (vgl. Art. 25 DS-GVO). Oft müssen aber innerhalb der Software erst Einstellungen und Optionen zum Schutz und der Sicherheit der Daten vorgenommen werden. Zu solchen spezifisch beim Einsatz von Meeting-Software erforderlichen Maßnahmen können folgende gehören:

- Schutz des Meetings durch ein Passwort
- Schließen des Meetings, wenn alle Teilnehmer beigetreten sind
- Kontrolle der beigetretenen Teilnehmer
- Nutzung einer „Warteraum“-Option (wenn vorhanden), um den Zugang zu kontrollieren

Der Umfang der Maßnahmen muss sich immer nach dem konkreten Risiko für die Rechte und Freiheiten der Betroffenen richten. Da vorliegend hauptsächlich vertrauliche Daten verarbeitet werden, ist eine Kombination mehrerer Einstellungen innerhalb der Software mit organisatorischen Maßnahmen dringend zu empfehlen.

Löschung von gespeicherten personenbezogenen Daten: Vor dem Hintergrund des Grundsatzes der Datenminimierung sollte für jede Software in einem Löschkonzept geregelt werden, wie lange welche personenbezogenen Daten gespeichert werden bzw. gelöscht werden.

3. IT-Sicherheit

Gerade bei der Nutzung von Software für die Übertragung von Sprache und Bild sind die IT-Sicherheitsziele Vertraulichkeit und Verfügbarkeit besonders in den Fokus zu rücken. Daher werden die Anbieter von Meeting-Software schwerpunktmäßig auf folgende technische Fragestellungen geprüft:

- Wird die Infrastruktur vom Hersteller oder Drittanbietern betrieben?
- Kann die Software auch On-Premise installiert werden?
- Wie ist die Verfügbarkeit zu beurteilen?
- Ist eine Registrierung oder Einladung der Teilnehmer notwendig oder kann jedermann beitreten?
- Können die virtuellen Seminarräume mit Passwörtern versehen werden?
- Gibt es ein Berechtigungskonzept der Software?
- Werden die Daten verschlüsselt übertragen?
- Werden die Daten verschlüsselt gespeichert?
- Können Daten wieder gelöscht werden?
- Welche Aufzeichnungsfunktionen gibt es?
- Gibt es sonstige Sicherheitsfeatures?
- Gibt es Schwachstellen oder Sicherheitslücken in der Software oder bei den hierfür benötigten Drittprodukten wie zum Beispiel Browser, Betriebssystem, etc.?

4. Weitere Aspekte

Kosten und Funktionsumfang der Software: Neben den Aspekten des Datenschutzes und der Datensicherheit sind auch die Kosten der Software in die Auswahl miteinzubeziehen. Die Lösungen unterscheiden sich in der Regel hinsichtlich der Teilnehmerzahl, den Online-Speichermöglichkeiten und dem Grad der Unterstützung.

Geschäftliche Nutzung: Weiterhin sollte die geschäftliche Nutzung der Software generell erlaubt sein.

Live-Support: Je nach Einsatzgebiet kann es für die Auswahl außerdem von Bedeutung sein, ob der Software-Betreiber einen Live-Support anbietet.

Dauer der beabsichtigten Verwendung: In diesem Zusammenhang sollte man sich schließlich auch fragen, ob die Software für den Dauerbetrieb oder nur für die Zeit der Pandemie eingesetzt werden soll. Hintergrund dieser Überlegung ist, dass datenschutzrechtliche Bewertungen immer eine Abwägung der verschiedenen Interessen des Verantwortlichen sowie der Betroffenen erfordern. In diese Abwägungen sind auch besondere Umstände, wie eine Pandemie, miteinzustellen, die ggfs. ein ansonsten gefordertes Datenschutzniveau überwiegen können. Zu solchen Umständen gehört das Interesse und auch Erfordernis, den Betrieb des Unternehmens sicherzustellen sowie die Mitarbeiter zu schützen. Sollte ein Tool also auch für die Zeit nach der Pandemie weiter eingesetzt werden, dann sollte die Wahl auch jetzt schon eine Software treffen, die datenschutzkonform einsetzbar ist. Wenn aber ein schnelles Handeln es nicht zulässt, die personenbezogenen Daten umfassend zu schützen oder ein ausreichendes IT-Sicherheits-Niveau zu gewährleisten, kann der Einsatz eines bestimmten Tools für eine kurze Zeit gerechtfertigt sein. Diese kurzfristig eingesetzten „nicht datenschutzkonformen“ Lösungen sind aber schnell durch datenschutzgerechte zu ersetzen.

Öffentliche Voreingenommenheit und Sensibilität: Bei der Bewertung eines Dienstes sollte auch immer mitberücksichtigt werden, ob dieser z. B. aufgrund datenschutzrechtlicher Bedenken besondere mediale Aufmerksamkeit erhalten hat und in der Öffentlichkeit möglicherweise ein „schlechtes Licht“ auf den Dienst geworfen wurde. Oft bleibt dieses Bild auch, wenn der Anbieter in Folge der öffentlichen Kritik alle Probleme gelöst hat. Dieses negative Bild des Anbieters muss nicht unbedingt dazu führen, dass der Einsatz der Software eingestellt bzw. unterlassen werden muss. Es muss aber in besonderem Maß darauf geachtet werden, dass die Betroffenen noch transparenter aufgeklärt werden (z. B. in einem zusätzlichen Informationsblatt zu den Pflichtinformationen nach Art. 13 DS-GVO).

II. Konkreter Vergleich einzelner Lösungen

1. Cisco WebEx Meeting

Cisco WebEx Meeting ist eine reine Videokonferenzlösung der Cisco Systems Inc. (Sitz: San José, USA). Es gibt jedoch noch weitere Produkte wie Teams, Events und Training, die ihren eigenen Funktionsumfang haben. Eine On-Premise Variante ist möglich, eine Preisauskunft ist jedoch nicht öffentlich verfügbar. Die Hardware für professionelle Meeting-Räume befindet sich im mittleren Preisspektrum, ist jedoch für die Nutzung optional.

1.1. Datenschutz

Die Datenschutzhinweise für die Webseite und die Lösungen von Cisco sind unter www.cisco.com/c/de_de/about/legal/privacy-full.html abrufbar.

Die Nutzerdaten werden bei deutschen Kunden in Rechenzentren in London, Amsterdam und Frankfurt a. M. gespeichert. Da es sich bei dem Anbieter der Software, die Cisco Systems, Inc., aber um ein US-amerikanisches Unternehmen handelt, ist es nicht ausgeschlossen, dass personenbezogene Daten trotz der Lage der Rechenzentren in die USA übertragen werden. Dies ergibt sich auch aus der Datenschutzerklärung.

Cisco verfügt über ein Privacy-Shield-Zertifikat (auch für Beschäftigtendaten) und hat damit ein ausreichendes Datenschutzniveau im Sinne der DS-GVO.

Der Entwurf eines Auftragsverarbeitungsvertrages ist auf Englisch unter dem folgenden Link abrufbar: https://trustportal.cisco.com/c/dam/r/ctp/docs/dataprotection/cisco-master-data-protection-agreement.pdf.

Die Teilnehmerzahl ist von der jeweiligen Lizenz abhängig. Laut FAQ von WebEx sind bis zu tausende Teilnehmer realisierbar (www.webex.com/de/faqs.html).

Es gibt keine medial bekannten Datenschutzprobleme bei WebEx Meeting.

Eine kritische Funktion stellt aber die Gesichtserkennung dar. Eine Erforderlichkeit der Nutzung kann in der Regel eher nicht begründet werden. Im Ergebnis kommt es aber auf den Einzelfall ein. Die Funktion sollte daher eher nicht genutzt werden, wenn nicht besondere Umstände vorliegen, die eine Gesichtserkennung erforderlich machen. Mehr Informationen zur Funktionsweise gibt es unter folgendem Link: https://help.webex.com/de-de/n3ubk5cb/Sign-Up-for-Face-Recognition-and-Name-Labels.

1.2. IT-Sicherheit

Die Serverinfrastruktur wird durch ein eigenes Rechenzentrum in Frankfurt zur Verfügung gestellt. Ein Backup ist nicht vorhanden. Die Datenhaltung erfolgt ausschließlich in Deutschland. Aussagen über die Auslastung und die Verfügbarkeit können nicht getroffen werden.

Für die Nutzung von cme24 benötigt nur der Gastgeber einen Benutzer-Account, um als Moderator beitreten zu können. Alle anderen Teilnehmer können per Browser teilnehmen. Es können bis zu 250 Teilnehmer teilnehmen. Die Interaktionsmöglichkeiten werden mit verschiedenen Berechtigungen ermöglicht bzw. eingeschränkt.

Die Übertragung der Informationen erfolgt transportverschlüsselt. Teilnehmer- und Logdaten der Meetings werden nach 24 Stunden gelöscht. Es erfolgt keine Datenhaltung im Anschluss an ein Meeting. Die während eines Meetings ausgetauschten bzw. hochgeladenen Dateien werden nach Beenden des Meetings gelöscht. Lediglich nach der Nutzung der Aufzeichnungsfunktion wird die Aufzeichnung für 7 Tage zum Download für den Moderator bereitgestellt. Danach werden auch sämtliche Aufzeichnungsdaten gelöscht. Somit erfolgt eine kaum nennenswerte Datenhaltung.

Die Einwahl per Telefon ist möglich. Die Sprachübertragung zwischen Meeting-Raum und Server erfolgt ebenfalls verschlüsselt. Die Übertragung vom Client bis zum Meeting-Raum erfolgt unverschlüsselt, was ein Risiko für das gesprochene Wort darstellt.

Während des Seminars und auch danach steht ein telefonischer Support zu den Geschäftszeiten (Mo-Fr, 08:00-16:00 Uhr) oder per E-Mail zur Verfügung und ist in den Kosten inbegriffen.

2. Skype / Microsoft Teams

Microsoft ist führender Hersteller für Betriebssysteme und Büroanwendungen. Das Produkt Microsoft Teams ist eher als Collaboration-Plattform im Rahmen der Office 365 Lösung anzusehen. Über die Funktionalität einer Videokonferenz hinaus gibt es einen integrierten Chat, die Integration in Outlook und es können sogar Office-Dokumente ausgetauscht werden. Zudem gibt es noch viele weitere Funktionalitäten, wenn Teams in Kombination mit anderen Office 365 Produkten genutzt wird. Teams kann auch als sogenannte Stand-Alone Lösung genutzt werden, ohne ein Office 365 Abonnement. Dennoch handelt es sicher hierbei um einen reinen Cloud-Dienst. Eine On-Premise Lösung ist nicht verfügbar. Aktuell ist die Nutzung auch für Unternehmen wegen der Corona-Krise kostenlos. Ob dies in Zukunft so bleibt, ist abzuwarten. Ansonsten muss Teams in die Office 365 Landschaft des Unternehmens integriert werden. Skype for Business wird zum 31.07.2021 vollständig eingestellt und durch Microsoft Teams ersetzt.

2.1. Datenschutz

Die Datenschutzhinweise sind unter https://privacy.microsoft.com/de-de/privacystatement abrufbar. Weitere Datenschutzinformationen gibt es unter: https://www.microsoft.com/de-de/trust-center. Microsoft ist auch für Beschäftigtendaten Privacy-Shield-zertifiziert.

Der Auftragsverarbeitungsvertrag wird bei Registrierung mit den sog. Online Service Terms (OST) geschlossen und ist Bestandteil dieser. Die OST sind in deutscher Sprache unter www.microsoft.com/de-de/licensing/product-licensing/products.aspx unter dem Punkt „Bestimmungen für Onlinedienste (OST)“ abrufbar.

Mit der Data Residency-Option kann man als deutsches Unternehmen seit Dezember 2019 festgelegen, dass die Daten in einem neuen Rechenzentrum in Deutschland gespeichert werden. Mehr Informationen unter: https://docs.microsoft.com/de-de/office365/enterprise/moving-data-to-new-datacenter-geos. Aufgrund des Sitzes in den USA ist aber nach wie vor nicht empfehlenswert vertrauliche Daten mit Microsoft Teams zu verarbeiten.

Ohne nähere Begründung hat die Aufsichtsbehörde Berlin Microsoft Teams als nicht datenschutzkonform bewertet (Stand: 02.04.2020). Microsoft stand bekanntlich sehr unter Kritik wegen der zahlreichen Datenschutzprobleme, insbesondere der umfangreichen Datenspeicherung und der Tatsache, dass Microsoft die Daten zu zahlreichen eigenen Zwecken verarbeitet hat sowie die mangelnden Optionen, die Verarbeitung von Diagnosedaten einzuschränken. Dies hatte die niederländische Regierung in einer Datenschutz-Folgenabschätzung festgestellt. Microsoft hat aber reagiert und auch außerhalb der konkreten Vertragsbeziehung zu der niederländischen Regierung auf EU-Ebene ordentlich nachgebessert. Im Ergebnis ist Microsoft Teams zumindest für nicht vertrauliche Daten datenschutzkonform einsetzbar, wenn zusätzlich die vorhandenen Datenschutzoptionen so gewählt werden, dass so wenig Daten wie möglich an Microsoft übermittelt werden (insbesondere betreffend die Diagnosedaten).

2.2. IT-Sicherheit

Die Serverinfrastruktur wird durch eigene Rechenzentren von Microsoft bereitgestellt. Auch eine deutsche bzw. europäische Datenhaltung ist möglich, jedoch ist nicht bekannt, wie die Daten global weiterverteilt werden. Die Verfügbarkeit kann als sehr hoch angesehen werden, da es täglich Millionen von Nutzern gibt und Microsoft als einer der Marktführer auf diesem Gebiet angesehen werden kann. Ausfälle sind medial nicht in Erscheinung treten.

Für die Nutzung von Microsoft Teams benötigt jeder Teilnehmer einen Benutzeraccount. Dieser kann mit Hilfe einer Multifaktor-Authentifizierung abgesichert werden, sodass zusätzlich zum Passwort noch ein weiterer Faktor benötigt wird. Dies können biometrische Merkmale, aber auch spezielle Geräte sein. Ein Berechtigungsmanagement existiert erst bei einer vollständigen Office 365 Nutzung für Unternehmen mit Active Directory Synchronisation.

Die Übertragung der Informationen erfolgt verschlüsselt. Auch die Speicherung der Inhalte kann verschlüsselt erfolgen, benötigt aber etwas Konfiguration. Aufgrund der weiten Verbreitung und der Stellung von Microsoft ist Teams ein lohnendes Ziel für Cyber-Kriminelle. Eine jüngst entdeckte Sicherheitslücke kann dazu führen, dass ein Angreifer sich die Zugangstokens (Schlüsseldateien) von Benutzern einer ganzen Organisation abgreifen kann. Microsoft bietet vergleichsweise schnell Patches an, welche aber von den IT-Verantwortlichen ebenfalls zeitnah implementiert werden müssen. Auch die Abhängigkeit von Microsoft Betriebssystemen sorgt dafür, dass diese ebenfalls entsprechend aktuell gehalten werden müssen. Durch die hohe Integration und die Vielzahl von Schnittstellen zu anderen Produkten sind Seitenangriffe sehr wahrscheinlich und relativ aufwändig im Blick zu behalten.

Microsoft bietet bei Erwerb der entsprechenden kostenpflichtigen Lizenz einen Telefonsupport an. Ansonsten ist ein Support über das Online-Portal oder ein Text-Chat-Tool möglich.

Aus rein technischer Betrachtung kann Microsoft Teams als sicher und dem Stand der Technik entsprechend angesehen werden. Das Auftreten neuer Sicherheitslücken ist sehr wahrscheinlich, da die Software im Fokus vieler Angreifer steht. Das Patchmanagement hat hier einen hohen Stellenwert. Die Verfügbarkeit wird als sehr hoch angesehen.

3. Blizz

BLIZZ ist ein Produkt der Teamviewer Germany GmbH mit Sitz in Deutschland und einer reinen deutschen Datenhaltung. Im Bereich der Fernwartungssoftware genießt der Anbieter einen hohen Marktanteil. Für die Zwecke der Stiftung Kinderhilfe sind die Pakete „Crew“ oder „Company“ zu empfehlen, die 14,00 EUR bzw. 19,00 EUR pro Monat pro Organisator bei jährlicher Zahlung kosten.

3.1. Datenschutz

Die Datenschutzhinweise für die Webseite und die Lösungen von Cisco sind unter www.cisco.com/c/de_de/about/legal/privacy-full.html abrufbar.

Die Nutzerdaten werden bei deutschen Kunden in Rechenzentren in London, Amsterdam und Frankfurt a. M. gespeichert. Da es sich bei dem Anbieter der Software, die Cisco Systems, Inc., aber um ein US-amerikanisches Unternehmen handelt, ist es nicht ausgeschlossen, dass personenbezogene Daten trotz der Lage der Rechenzentren in die USA übertragen werden. Dies ergibt sich auch aus der Datenschutzerklärung. Cisco verfügt über ein Privacy-Shield-Zertifikat (auch für Beschäftigtendaten) und hat damit ein ausreichendes Datenschutzniveau im Sinne der DS-GVO.

Der Entwurf eines Auftragsverarbeitungsvertrages ist auf Englisch unter dem folgenden Link abrufbar: https://trustportal.cisco.com/c/dam/r/ctp/docs/dataprotection/cisco-master-data-protection-agreement.pdf.

Die Teilnehmerzahl ist von der jeweiligen Lizenz abhängig. Laut FAQ von WebEx sind bis zu tausende Teilnehmer realisierbar (www.webex.com/de/faqs.html).

Eine kritische Funktion stellt aber die Gesichtserkennung dar. Eine Erforderlichkeit der Nutzung kann in der Regel eher nicht begründet werden. Im Ergebnis kommt es aber auf den Einzelfall ein. Die Funktion sollte daher eher nicht genutzt werden, wenn nicht besondere Umstände vorliegen, die eine Gesichtserkennung erforderlich machen. Mehr Informationen zur Funktionsweise gibt es unter folgendem Link: https://help.webex.com/de-de/n3ubk5cb/Sign-Up-for-Face-Recognition-and-Name-Labels.

3.2. IT-Sicherheit

Die Serverinfrastruktur wird durch eigene Rechenzentren von Cisco bereitgestellt. Die Verfügbarkeit kann als sehr hoch angesehen werden, da es täglich Millionen von Teilnehmern gibt.

Für die Nutzung von WebEx Meetings benötigt nur der Gastgeber zwingend einen Benutzeraccount, alle anderen können über einen Beitrittslink teilnehmen. Mit Hilfe einer optionalen Zusatzsoftware (Cisco DUO), die ebenfalls von Cisco angeboten wird, kann darüber hinaus eine Multifaktor-Authentifizierung aktiviert werden.

Es ist aber auch möglich dem Meeting per Audiokonferenz beizutreten. Um diesen Vorgang vor unbefugten Zuhörern zu schützen gibt es ebenfalls optional die sogenannte „CANI“ Authentifizierung. Hiermit lässt sich vor dem Beitritt überprüfen, ob die vom Teilnehmer gesendete Rufnummer für den Beitritt freigegeben ist. Dies erfordert natürlich einen hohen Konfigurationsaufwand. Außerdem ist es möglich, durch sogenanntes Rufnummern-Spoofing, diesen Sicherheitsmechanismus relativ leicht zu umgehen.

Die Übertragung der Informationen erfolgt grundsätzlich nur transportverschlüsselt. Alternativ kann die Nutzung einer Ende-zu-Ende Verschlüsselung ermöglicht werden. Diese muss jedoch durch einen Administrator voreingestellt werden. Die Funktion der Ende-zu-Ende-Verschlüsselung ist seit dem 02.05.2020 nur noch „auf Anfrage“ verfügbar laut Hilfeseite von Cisco (https://help.webex.com/nwh2wlx/Enable-End-to-End-Encryption-

Using-End-to-End-Encryption-Session-Types). Bei Verwendung der Ende-zu-Ende Verschlüsselung weist der Anbieter daraufhin, dass folgende Funktionen dann nicht mehr verwendet werden können:

- Beitreten vor dem Gastgeber
- Telepresence Video End Points (sogenannte Cloud-Endpunkte)
- Cisco Mobile WebexMeetings-Web-App
- Linux-Clients
- Netzwerkbasierte Aufzeichnung
- Speichern von Sitzungsdaten, Abschriften, Meetingprotokollen usw.
- Freigabe von Ferncomputern
- Hochladen geteilter Dateien im Meeting-Bereich am Ende von Cisco Webex-Meetings
- PSTN-Einwahl/Rückruf

Auf einen Großteil dieser Funktionen kann, wenn es lediglich um Videokonferenzen geht, verzichtet werden. Inwieweit die Performance unter der Verschlüsselung leidet, ist nicht bekannt. Die Anforderungen der Stiftung Kinderhilfe gehen wohl nicht über eine reine Videotelefonie hinaus. Somit ist die Software für die Anforderungen grundsätzlich geeignet.

Die genannten Sicherheitsaspekte sind sowohl bei der Cloud-Variante, als auch bei einer On-Premise Lösung identisch. Sowohl in der Vergangenheit, als auch aktuell, wurden immer wieder Sicherheitslücken bekannt. Eine Übersicht finden Sie hier:

https://www.cisco.com/c/en/us/support/conferencing/webex-meeting-center/products-security-advisories-list.html.

Da es sich bei dieser Software eher um ein Softwarepaket (also verschiedene Programme kombiniert) handelt, sind die Sicherheitslücken entsprechend verteilt. Unter anderem sind die Serverkomponenten, die Client-Software oder aber auch der „Player“ zum Aufnehmen und Abspielen von Meetings, aktuell im Fokus der Berichterstattung. Das bedeutet, dass die Software zwingend durch entsprechend qualifiziertes IT-Personal konfiguriert und aktuell gehalten werden muss, um hier die sichere Verwendung gewährleisten zu können.

Cisco WebEx Meeting bietet laut FAQ in jedem kostenpflichtigen WebEx Konto technischen Support rund um die Uhr an (www.webex.com/de/faqs.html).

Aus rein technischer Betrachtung kann, mit der entsprechenden Konfiguration, Cisco WebEx Meeting als sicher und dem Stand der Technik entsprechend angesehen werden. Das Auftreten neuer Sicherheitslücken ist aber sehr wahrscheinlich, da die Software im Fokus vieler Angreifer steht. Es erfordert jedoch fachmännische IT-Kenntnisse zur Konfiguration und eine dauerhafte Betreuung. Die Verfügbarkeit wird als sehr hoch angesehen.

4. Zoom

Die Webinar Software Zoom wird von dem amerikanischen Unternehmen Zoom Video Communications Inc. betrieben. Zoom hat sich vor allem durch seine einfache Bedienung und Plattformunabhängigkeit im Rahmen der Corona-Krise schnell zu einem Global Player entwickelt. Durch dieses Wachstum ist die Plattform in den Fokus zahlreicher Sicherheitsforscher und Datenschützer gerückt, aber auch für Cyber-Kriminelle zunehmend interessant geworden.

4.1. Datenschutz

4.1.1. Allgemein

Die Datenverarbeitung findet grundsätzlich in den USA statt, weshalb auch hier die Anforderungen der Drittstaatenübermittlung zu beachten sind. Den Nutzern wird aber die Option bereitgestellt, dass die Daten

ausschließlich in der EU gespeichert werden. Wie auch bei den anderen Lösungen, schließt dies nicht aus, dass Daten in die USA übertragen werden können.

Zoom hält einen eigenen Standardauftragsverarbeitungsvertrag vor, der bei Registrierung eines „Zoom"-Accounts durch Einbeziehung aller Dokumente unter www.zoom.us/legal (unter „Global DPA") geschlossen wird. Das Dokument ist vom Anbieter schon unterzeichnet. Die Regelungen des Vertrags sind grundsätzlich in Ordnung. Alle in Art. 28 DS-GVO vorgegebenen Inhalte werden angesprochen und eine Beschreibung der getroffenen technischen und organisatorischen Maßnahmen ist ebenfalls vorhanden.

Zoom ist derzeit grundsätzlich datenschutzkonform einsetzbar. Ab dem 01.06.2020 wird die Verschlüsselung sogar nachgebessert, so dass die Software grundsätzlich für die Verarbeitung von Betriebs- und Geschäftsgeheimnissen geeignet wäre. Allerdings ist auch hier aufgrund des Sitzes in den USA aktuell davon abzuraten, vertrauliche Daten oder Geschäftsgeheimnisse mit Zoom auszutauschen.

Ohne nähere Begründung hat außerdem die Aufsichtsbehörde Berlin Zoom als nicht datenschutzkonform bewertet (Stand: 02.04.2020).

4.1.2. Besonders kritische Funktionen und die allgemeine Kritik um Zoom

Aufmerksamkeitstracking: Das „Aufmerksamkeitstracking" ist eine Funktion bei Zoom, mit der der Host eines Meetings, also nicht Zoom selbst, die Aufmerksamkeit des Teilnehmers tracken konnte. Diese Funktion ist aufgrund der zahlreichen Kritiken allerdings seitdem 01.04.2020 deaktiviert worden.

4.2. IT-Sicherheit

Die Serverinfrastruktur wird durch eigene Rechenzentren von Zoom bereitgestellt, welche sich weltweit verteilt finden. Auch die Nutzung von Amazon AWS Infrastrukturen zur Lastverteilung wird von Zoom bestätigt. Seit dem 18. April 2020 kann man als zahlender Benutzer die Datenhaltung geografisch auswählen. Jedoch wird aktuell die Region „Europa" angeboten, ohne konkret auf die Standorte nach Ländern aufzuschlüsseln. Inwieweit gespeicherte Daten außerdem in andere Rechenzentren repliziert werden, ist nicht bekannt. Die Verfügbarkeit kann als sehr hoch angesehen werden, da es täglich Millionen von Nutzern gibt und Engpässe bisher nicht medial in Erscheinung getreten sind. Zoom wird als reiner Cloud-Dienst angeboten.

Für die Nutzung von Zoom benötigt nur der Gastgeber einen Benutzer-Account. Dieser kann mit Hilfe einer 2-Faktor-Authentifizierung abgesichert werden, sodass zusätzlich zum Passwort noch ein 6-stelliger Code über ein Smartphone als weiterer Faktor benötigt wird. Bezüglich des Funktionsumfangs hat Zoom ein Berechtigungskonzept integriert, mit dem der Moderator dem Teilnehmer je nach Recht unterschiedlich starke Berechtigungen freigibt.

Die Übertragung der Informationen erfolgt teilweise Ende-zu-Ende verschlüsselt (Chatfunktion), ansonsten zumindest immer übertragungsverschlüsselt zwischen Client und Server. Dies ist davon abhängig, welche Funktion von Zoom genutzt wird. Auch die Speicherung von Daten wird verschlüsselt ermöglicht und laut Hersteller können diese sogar revisionssicher bis zu 10 Jahre aufbewahrt werden. Eine Aufzeichnungsfunktion ist verfügbar und kann sowohl für Teilnehmer als auch Moderatoren freigegeben werden.

Seit der aktuellen Version 5.0 wurde die Verschlüsselung AES ECB auf AES256GCM umgestellt, was die Sicherheit der Verschlüsselung deutlich erhöht. Bei Neuinstallation des Zoom-Clients kommt diese direkt zum Einsatz. Ein Update wird ab dem 30.05.2020 erzwungen.

Aufgrund der aktuellen Situation steht Zoom öffentlich unter massiver Kritik. Forscher und Experten haben es sich zur Aufgabe gemacht, Zoom auf Herz und Nieren zu prüfen. Die gute Nachricht dabei ist, dass so die Lücken schnell geschlossen werden können. Da Zoom ursprünglich für die integrierte Nutzung in homogenen IT-Systemen mit eigener IT-Abteilung, vor allem in den USA, entwickelt wurde, wurden viele Aspekte bei der Entwicklung nicht betrachtet. Jedoch wurden die in den letzten Wochen veröffentlichten Sicherheitslücken geschlossen und die Software bietet weitere Konfigurationsmöglichkeiten, um Unbefugten den Zutritt zu

Meeting-Räumen zu verwehren. Auch ist geplant, die Software innerhalb der nächsten drei Monate noch sicherer und datenschutzfreundlicher zu machen. Vor allem bei der Nutzung der Zoom App und der Nutzung mit iOS Geräten ist aktuell noch Vorsicht geboten.

Zoom bietet in der kostenpflichtigen Variante einen Telefonsupport an. Ansonsten ist ein Support über das Online-Portal oder ein Text-Chat-Tool möglich.

Aus rein technischer Betrachtung kann, mit der entsprechenden Konfiguration, Zoom als sicher und dem Stand der Technik entsprechend angesehen werden. Das Fehlen der Ende-zu-Ende Verschlüsselung und das Problem der Datenhaltung wirken sich (noch) negativ auf die Vertraulichkeit aus. Das Auftreten neuer Sicherheitslücken ist sehr wahrscheinlich, da die Software im Fokus vieler Angreifer und Forscher steht.

5. CME 24

5.1. Kurzbeschreibung des Anbieters

CME 24 („communication made easy“) ist ein Projekt der BBS Büro- und Business-Service-GmbH (Sitz: Karlsruhe). CME 24 bietet webbasierte Webinarsoftware als Full Service Paket an. Die Meetingräume werden durch den Anbieter bereitgestellt und bei Start anmoderiert und dann an den Kunden übergeben. Das Erwerben eines eigenen Servers ist möglich, jedoch nur unter einzelvertraglichen Aspekten machbar. Der große Unterschied zu den anderen Anbietern ist, dass hier keine Software gekauft oder angemietet wird, sondern ein Rund-um-Service gebucht wird.

5.2. Datenschutz

Die Datenschutzhinweise sind für die Datenverarbeitung auf der Webseite hier abrufbar: www.cme24-webinare.de/j/privacy.

Eine Prüfung der konkreten Funktionen kann hier nur anhand eines Demozugangs erfolgen, da es nur wenige Informationen zur Software gibt.

Der Auftragsverarbeitungsvertrag ist nach Registrierung im Kundenkonto abrufbar.

5.3. IT-Sicherheit

Die Serverinfrastruktur wird durch ein eigenes Rechenzentrum in Frankfurt zur Verfügung gestellt. Ein Backup ist nicht vorhanden. Die Datenhaltung erfolgt ausschließlich in Deutschland. Aussagen über die Auslastung und die Verfügbarkeit können nicht getroffen werden.

Für die Nutzung von cme24 benötigt nur der Gastgeber einen Benutzer-Account, um als Moderator beitreten zu können. Alle anderen Teilnehmer können per Browser teilnehmen. Es können bis zu 250 Teilnehmer teilnehmen. Die Interaktionsmöglichkeiten werden mit verschiedenen Berechtigungen ermöglicht bzw. eingeschränkt.

Die Übertragung der Informationen erfolgt transportverschlüsselt. Teilnehmer- und Logdaten der Meetings werden nach 24 Stunden gelöscht. Es erfolgt keine Datenhaltung im Anschluss an ein Meeting. Die während eines Meetings ausgetauschten bzw. hochgeladenen Dateien werden nach Beenden des Meetings gelöscht. Lediglich nach der Nutzung der Aufzeichnungsfunktion wird die Aufzeichnung für 7 Tage zum Download für den Moderator bereitgestellt. Danach werden auch sämtliche Aufzeichnungsdaten gelöscht. Somit erfolgt eine kaum nennenswerte Datenhaltung.

Die Einwahl per Telefon ist möglich. Die Sprachübertragung zwischen Meeting-Raum und Server erfolgt ebenfalls verschlüsselt. Die Übertragung vom Client bis zum Meeting-Raum erfolgt unverschlüsselt, was ein Risiko für das gesprochene Wort darstellt.

Während des Seminars und auch danach steht ein telefonischer Support zu den Geschäftszeiten (Mo-Fr, 08:00-16:00 Uhr) oder per E-Mail zur Verfügung und ist in den Kosten inbegriffen.

Laut Anbieter gibt es Probleme bei der Verwendung der Windows Browser Edge und Internet Explorer. Es wird empfohlen, andere gängige Browser wie Google Chrome, Mozilla Firefox, Safari oder Opera zu verwenden.

Aus rein technischer Betrachtung kann cme24 als sicher und dem Stand der Technik entsprechend betrachtet werden. Das Fehlen eines zweiten Rechenzentrums birgt ein gewisses Ausfallrisiko bezüglich der Verfügbarkeit. Das Auftreten von Sicherheitslücken ist unwahrscheinlich, da die Software nicht im Fokus von Angreifern und Forschern steht. Durch die strenge Löschpolitik ist cme24 aus Datenschutzsicht sehr zu empfehlen. Inwieweit die Vertraulichkeit gerade bei der Übertragung von Sprachdaten per Telefon gegeben ist, kann abschließend nicht beurteilt werden.

6. Edudip

6.1. Kurzbeschreibung des Anbieters

Bei Edudip der edudip GmbH (Sitz: Aachen) handelt es sich um eine Webinar-Software. Die Software ist webbasiert, es ist also keine Installation erforderlich. Die Software kann monatlich abonniert werden für eine Laufzeit von 1, 12 oder 24 Monaten. Es gibt drei Preisstufen, die sich im Wesentlichen in der Teilnehmerzahl, der Anzahl möglicher Moderatoren/Co-Moderatoren und den zusätzlichen Funktionen unterscheiden. In allen drei Preisstufen ist die Webinardauer unbegrenzt. Die Webinare finden auf der Plattform von Edudip statt. Ansprechpartner für individuelle Angebote oder für den Wunsch, eigene Anwendungen mit Edudip zu verbinden (über eine API-Schnittstelle) ist das Sales-Team (sales@edudip.com).

6.2. Datenschutzrelevante Aspekte

Die Datenschutzhinweise sind unter www.edudip.com/de/datenschutz zu finden. Der Auftragsverarbeitung soll wohl im Kundenkonto zu finden sein. Die Daten werden ausschließlich auf deutschen Servern gespeichert.

Der Veranstalter eines Webinars kann selbst bestimmen, welche Daten der Teilnehmer im Anmeldeformular abgefragt werden. Um dem Grundsatz der Datenminimierung der datenschutzfreundlichen Voreinstellungen gerecht zu werden, ist darauf zu achten, dass wirklich nur die für die Teilnahme und Vertragsabwicklung erforderlichen Daten abgefragt werden und Pflichtangaben von freiwilligen Angaben deutlich getrennt werden.

Zur Teilnahme an einem Webinar über die Webinarplattform von Edudip müssen die Teilnehmer sich über ein Anmeldeformular auf der Webseite anmelden. Die Registrierung eines Accounts ist nicht erforderlich. Bei kostenpflichtigen Webinaren wird die Abrechnung außerdem über Edudip durchgeführt, sodass die entsprechenden Zahlungsdaten bei Edudip erhoben werden.

Die Teilnehmerzahl ist je nach Abomodell auf 30, 100, 500 oder 1000 Teilnehmer beschränkt.

6.3. IT-Sicherheit

Die Bereitstellung der Infrastruktur erfolgt ausschließlich über Rechenzentren in Deutschland. Ob diese angemietet sind konnte nicht in Erfahrung gebracht werden. Die Verfügbarkeit liegt laut verschiedener Berichte bei nur ca. 95%, was darauf schließen lässt, dass es keine redundanten Rechenzentren sind.

Es können maximal drei Co-Moderatoren eingesetzt werden. Auch ist es nur maximal vier Teilnehmern möglich, gleichzeitig zu sprechen.

Die Datenübertragung erfolgt über eine HTTPS-Verbindung mit einer 256-Bit TLS-Verschlüsselung. Weitere Informationen über Sicherheitsmechanismen konnten nicht in Erfahrung gebracht werden.

Aktuell können Support-Anfragen aufgrund erhöhten Aufkommens an Anfragen (Stand: 08.05.2020) ausschließlich über ein Rückrufformular gestellt werden.

Aus rein technischer Betrachtung kann edudip nicht abschließend als sicher und dem Stand der Technik entsprechend betrachtet werden, da hierzu weitere Informationen benötigt werden, welche nicht öffentlich verfügbar sind. Die Angabe der Verfügbarkeit mit 95% birgt ein hohes Ausfallrisiko. Da es eine rein

webbasierte Lösung ist, sind vor allem browserbasierte Sicherheitslücken ein Risiko. Die Anwendung selbst ist in Deutschland entwickelt und der Anbieter versichert höchste Qualität bei Sicherheitsmechanismen. Eine für den Benutzer freigegebene Löschfunktion macht aus Datenschutzsicht einen guten Eindruck. Inwieweit die Vertraulichkeit gerade bei der Übertragung von Sprachdaten per Telefon gegeben ist, kann abschließend nicht beurteilt werden. Auch ist unklar, wie und in welchem Umfang, Daten bei dem Anbieter gespeichert werden.

Aufgrund des aktuell beschränkten Support eignet sich Edudip derzeit noch nicht für die Durchführung von kostenpflichtigen Seminare und von Premium-Veranstaltungen, da hier ein Live-Support dringend erforderlich ist.

III. Mitbestimmung des Betriebs- oder Personalrats

Gemäß § 87 Abs. Nr. 6 BetrVG hat der Betriebsrat bei der Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen, mitzubestimmen.

Entgegen des Wortlauts reicht es aber schon aus, wenn die technische Einrichtung dazu **geeignet** ist, die Beschäftigten zu überwachen. Bei Videokonferenz-Software handelt es sich regelmäßig um eine solche technische Einrichtung. Es ist daher darauf zu achten, dass der Betriebsrat ein Mitbestimmungsrecht hat bei der Einführung und der Anwendung von Videkonferenz-Software.

Passende Weiterbildungen finden Sie hier:

Weiterbildung zum Thema Recht

Finden Sie aus unserem breiten, erstklassigen Weiterbildungsangebot die für Ihre Bedürfnisse passende Fortbildung. Profitieren Sie von unseren maßgeschneiderten Seminaren und Lehrgängen mit erfahrenen, hochkarätigen Experten rund um das Thema Recht. Jetzt informieren.

e-Learning – Klicken und Lernen

Das FORUM Institut bietet mit hochwertigen e-Learning-Programmen eine flexible Weiterbildungsform. Entscheiden Sie selbst, wann und wo Sie lernen.
Jetzt testen.

Inhouse-Seminare – Maßgeschneiderte Lösungen

Alle unsere Seminare eignen sich auch hervorragend als Inhouse-Training.
Jetzt individuelles Angebot anfordern.

FORUM · Institut für Management GmbH • Postfach 10 50 60 • 69040 Heidelberg • Germany
Tel. +49 6221 500-500 • Fax +49 6221 500-555 • www.forum-institut.de