DATENSCHUTZ-KONFORME VIDEOKONFERENZ-SYSTEME

Checkliste | Stand 11/2021

Datenschutzkonforme Videokonferenzsysteme – Checkliste

Das Thema Datenschutz und Videokonferenzen hat in den 1,5 Jahren enorm an Bedeutung gewonnen. Immer wieder werden wir von Kunden oder Interessenten gefragt, welche Faktoren man berücksichtigen muss, um datenschutzkonforme Videokonferenzen zu gewährleisten? Daher haben wir zusammen mit unserem externen Datenschutzverantwortlichen eine Checkliste erarbeitet, die alle wesentlichen Punkte berücksichtigt.

Der Gesetzgeber fordert vom Verarbeiter personenbezogener Daten, dass er ein „angemessenes Schutzniveau“ sicherstellt und dass er die Risiken prüft, welche mit der Verarbeitung personenbezogenen Daten einhergehen. Um den Anforderungen der DSGVO gerecht zu werden, müssen also bei jeder Verarbeitung von personenbezogenen Daten die Risiken für die potentiell betroffene Person, die sich aus der Verarbeitung ergeben, betrachtet werden. Der Einsatz eines Videokonferenzsystems stellt so eine Verarbeitung dar.

In der Checkliste wollen wir anhand geeigneter Fragen mögliche Risiken ermitteln und somit versuchen die Anforderungen der DSGVO umzusetzen.

Jedes Nein bedeutet ein potentielles Risiko für die betroffene Person. Ein Risiko sollte durch entsprechende Optionen behandelt werden. Mögliche Optionen können sein:
Akzeptieren, Reduzieren, Abwälzen oder Vermeiden.

Die Festlegung welche der Optionen die richtige ist, bedarf immer einer Einzelfallentscheidung und genauen Abwägung welche der Risiken tragbar sind oder behandelt werden müssen.

I. Auswahl und Überprüfung der Konferenzlösung

1. Wurden die Risiken des Einsatzes von Videokonferenzsystemen betrachtet und analysiert?

☐ Nein ☐ Ja

2. Wurde geprüft, ob eine Datenschutzfolgeabschätzung gemäß Art. 35 DSGVO durchzuführen ist?

(Dies ist insbesondere der Fall, wenn personenbezogene Daten besonderen Kategorien gemäß Art. 9 DSGVO in den Videokonferenzen umfangreich bearbeitet werden.)

☐ Nein ☐ Ja

3. Um welche Art von Videokonferenzsystem handelt es sich?

☐ selbstbetriebenes Videokonferenzsystem
☐ Videokonferenzsystem eines externen IT-Dienstleisters
☐ Online-Dienst (SaaS – Dienstleistung / Tools)

4. Falls es sich um ein Videokonferenzsystem eines externen Dienstleisters handelt: wurde geprüft, ob die vom Dienstleister eingesetzte Software Daten an den Hersteller oder an Dritte weitergibt?

☐ Nein ☐ Ja

5. Hat der Dienstleister seinen Sitz in der Europäischen Union oder einem Land des Europäischen Wirtschaftsraums bzw. ein angemessenes Datenschutzniveau?

(Grundsätzlich gelten Anbieter, die ihren Sitz in der EU haben aus Datenschutzaspekten als sicherer, da ein einheitliches Datenschutzniveau herrscht. Anbieter aus Nicht-EU-Staaten unterliegen meistens Rechtsvorschriften und folglich Zugriffsrechten von Behörden von Drittstaaten, die den datenschutzrechtlichen Anforderungen der DSGVO erschweren oder sogar im Widerspruch stehen können.)

☐ Nein ☐ Ja

5.1. Wurden, falls es sich um ein Videokonferenzsystem handelt, welches zu Übermittlung von Daten in Drittländer führt, die besonderen Bedingungen gemäß Kapitel V, Art. 44 ff. DSGVO eingehalten?

(Zu beachten ist hierbei, dass die EU-Kommission für manche Drittländer ein angemessenes Datenschutzniveau bestätigt hat, für welche keine weiteren Bedingungen gemäß Art.45 DSGVO bezüglich der Zulässigkeit des Datenexports zu erfüllen sind.)

☐ Nein ☐ Ja

5.2. Falls der Anbieter seinen Sitz in der USA oder einem anderen Drittland hat, wurden zusätzliche Garantien für die Sicherheit der Datenverarbeitung geboten?

☐ Nein ☐ Ja

5.3. Falls der Anbieter seinen Sitz in der USA oder einem anderen Drittland hat, wurden bei der Verwendung von Standardvertragsklauseln und anderen vertraglichen Garantien für die Übermittlungen personenbezogener Daten zusätzliche Maßnahmen ergriffen, die sicherstellen, dass für Daten bei und nach ihrer Übermittlung ein im Wesentlichen gleichwertiges Schutzniveau wie das in der EU gewährleistet wird?

☐ Nein ☐ Ja

6. Wurden die technischen und organisatorischen Maßnahmen des Anbieters bzw. des Dienstleisters des Videokonferenzsystems geprüft?

☐ Nein ☐ Ja

6.1. Sicherheit der Verarbeitung

(a) Wurde beim Videokonferenzsystem eine Verschlüsselung implementiert, welche dem Stand der Technik entspricht (bspw. kryptographische Verfahren)?

☐ Nein ☐ Ja

(b) Gewährt die Verschlüsselung die Vertraulichkeit, Integrität und Authentizität aller übertragenen Daten?

☐ Nein ☐ Ja

6.2. Nutzerauthentifizierung

(a) Können nur berechtigte Personen auf eine Videokonferenzsitzung und deren Daten zugreifen?

☐ Nein ☐ Ja

(b) Wurde die Mindeststärke der Authentisierung an die Schwere der Risiken, welche sich bei einem Bruch der Vertraulichkeit und Integrität ergeben angepasst?

(Bei geringen Risiken sollte mindestens eine Authentisierung mit Nutzernamen und geeignetem Passwort gewährleistet sein. Bei hohen Risiken sollte eine 2FA nach dem Stand der Technik erfolgen.)

☐ Nein ☐ Ja

(c) Ist das Authentifizierungsprotokoll so ausgestattet, dass Passwörter weder übertragen noch beim Dienstleister gespeichert werden?

☐ Nein ☐ Ja

(d) Zugangsbeschränkungen (wie Login, oder bei Gästen nur mit Zustimmung des Organisators)

☐ Nein ☐ Ja

(e) Beschränkung von Logfiles: Werden Logfiles erstellt?

(Diese sollten nur erstellt werden, soweit diese erforderlich sind. Diese können auch für die Fehlerbehebung durch den Dienstleister notwendig sein. Es kommt jedoch darauf an, dass die Daten dann nur zu diesem Zweck verwendet werden und nach Wegfall des Zwecks wieder gelöscht werden.)

☐ Nein ☐ Ja

6.3. Installation und Softwareaktualisierung

(a) Kann gewährleistet werden, dass das System/die Software jederzeit auf dem neusten Stand ist?

☐ Nein ☐ Ja

(b) Wurde der Zeitrahmen festgelegt, in dem technische Schwachstellen und Sicherheitslücken behoben werden müssen, bevor es zu einem nicht mehr vertretbaren Verarbeitungsrisiko kommt?

☐ Nein ☐ Ja

(c) Ist sichergestellt, dass im Falle einer webbasierten Lösung stehts eine aktuelle Webbrowserversion verwendet wird?

☐ Nein ☐ Ja

6.4. Ermöglicht das Videokonferenzsystem eine Rollentrennung bzw. Zuweisung von Berechtigungen während einer Konferenz?

☐ Nein ☐ Ja

6.5. Datensparsamkeit

(a) Werden nur die für die Bereitstellung des Dienstes erforderlichen Daten verarbeitet?

☐ Nein ☐ Ja

(b) Chatverläufe und Dateiaustausch

(Dürfen nur für den benötigten Zeitraum zur Verfügung stehen und müssen danach automatisch gelöscht werden. Beim Chat dürfte dies nach Ende der Videokonferenz der Fall sein. Bei Dateiaustausch kann z. B. ein Zeitraum von wenigen Stunden oder einem Tag gewählt werden, innerhalb dessen die Mitarbeiter Zeit haben die Daten herunterzuladen und anderweitig abzulegen. Ergänzend sollte als organisatorische Maßnahme geregelt werden welche Arten von Dokumenten (nicht) über das Tool geteilt werden dürfen. Dies kann sowohl als Black- oder als Whitelist ausgestaltet werden.)

☐ Nein ☐ Ja

(c) Aufnahmen der Videokonferenz

(Aufnahmen sind nur mit einer Einwilligung aller Teilnehmer zulässig. Daher sollte das Tool so eingestellt werden können, dass vor Start der Aufnahme bei allen Teilnehmern eine Nachricht mit den nötigen Informationen erscheint sowie die Option zuzustimmen oder abzulehnen. Mit Ihrem DSB können Sie dazu abstimmen, ob und wie dabei die Anforderungen der DSGVO an eine Einwilligung erfüllt werden können. Zudem wird eine Aufzeichnung wohl stets den Ton umfassen und wird damit bei fehlender Zustimmung sogar regelmäßig wegen der Verletzung der Vertraulichkeit des Wortes nach § 201 Abs. 1 StGB strafbar sein.)

☐ Nein ☐ Ja

(d) Desktop-Sharing

(Es sollte nur gezeigt werden was auch für die Besprechung erforderlich ist. Daher sollte der Desktop ohne Dateisymbole gezeigt werden, solange diese für die Videokonferenz nicht erforderlich sind. Auch sollten keine Benachrichtigungen über neue Mails auf dem geteilten Bildschirm erscheinen. Entweder kann dies grundsätzlich oder für die jeweilige Konferenz unterbunden werden. Des Weiteren ist es möglich bei Verwendung von mehreren Monitoren nicht den als Hauptanzeige konfigurierten Bildschirm auszuwählen.)

☐ Nein ☐ Ja

7. Wurde bereits mit einem Anbieter der Videokonferenzlösung ein Auftragsverarbeitungsvertrag abgeschlossen?

(Falls es sich nicht um ein selbstbetriebenes Videokonferenzsystem handelt, muss mit dem Dienstleister gemäß DSGVO Artikel 28 Abs. 3 ein Auftragsverarbeitungsvertrag geschlossen werden.)

☐ Nein ☐ Ja

7.1. Falls ja, wurde dieser vor dem Urteil des EuGHs in der Rechtssache Schrems II abgeschlossen und folglich vor Ungültigkeit des EU-US Privacy Shield?

☐ Nein ☐ Ja

7.2. Falls ja, wurden nachträglich Maßnahmen ergriffen, die sicherstellen, dass für diese Daten auch bei und nach ihrer Übermittlung ein im Wesentlichen gleichwertiges Schutzniveau wie das in der EU gewährleistet wird?

☐ Nein ☐ Ja

II. Datenschutzverantwortliche

1. Wurden die Risiken des Einsatzes von Videokonferenzsystemen betrachtet und analysiert?

☐ Nein ☐ Ja

2. Erfüllt der Verantwortliche beim Betrieb oder der Nutzung eines Videokonferenzdienstes die Pflichten gemäß DSGVO?

☐ Nein ☐ Ja

2.1. Werden den an der Konferenz teilnehmenden Personen Informationen über die mit der Nutzung des Dienstes verbundene Datenverarbeitung nach Art. 12, 13, 14 DSGVO verständlich zur Verfügung gestellt?

☐ Nein ☐ Ja

2.2. Werden alle sonstigen Informationspflichten gemäß Art. 13, 14, 21 eingehalten?

(Hierzu zählen beispielsweise Informationen darüber, zu welchen Zwecken und auf welcher Grundlage welche personenbezogenen Daten verarbeitet werden, für welche Zeitdauer eine Speicherung nach Abschluss einer Videokonferenz erfolgt und ob personenbezogene Daten in ein Drittland übermittelt werden. Zudem muss beispielsweise auf das Widerspruchsrecht hingewiesen werden.)

☐ Nein ☐ Ja

2.3. Werden Betroffenenrechte aus Art. 15 bis 21 DSGVO gewährleistet?

☐ Nein ☐ Ja

2.4. Wurden Vorkehrungen getroffen, um die Meldepflicht bei Datenpannen und insbesondere bei Verletzung des Schutzes personenbezogener Daten gemäß Art. 33 und 34 DSGVO zu gewährleisten?

☐ Nein ☐ Ja

III. Datenschutzeinstellungen

1. Werden Videotelefonie und Videokonferenzen über verschlüsselte Kanäle abgewickelt?

☐ Nein ☐ Ja

2. Werden Aufzeichnungen sowie Protokolle nach Beendigung des Meetings gelöscht?

☐ Nein ☐ Ja

3. Erfüllt das Videokonferenzsystem datenschutzfreundliche Voreinstellungen gemäß Art. 25 DSGVO?

(Kamera, Mikrofon und das Teilen des Bildschirms von Teilnehmern müssen vor Eintritt in die Konferenz standardmäßig ausgeschaltet sein, damit Personen entscheiden können, wann sie diese Geräte und Funktionen einschalten wollen.)

☐ Nein ☐ Ja

4. Um den Datenschutz der Teilnehmer zu wahren, sollten weder Tracking noch andere Analyse-Tools eingeschaltet sein. Wird dies gewährleistet?

☐ Nein ☐ Ja

HINTERGRUNDINFORMATIONEN ZUM „SCHREMMS URTEIL“

Warum ist die Nutzung von US-Tools wie Zoom und Teams datenschutzrechtlich schwierig?

Bei der Nutzung von Videokonferenzsystemen amerikanischer Dienstleister werden in der Regel personenbezogene Daten auch an die Muttergesellschaften in den USA übermittelt. Der Europäische Gerichtshof hat mit dem Urteil vom 16.07.2020 klargestellt, dass personenbezogene Daten von EU-Bürgern nur an Drittländer übermittelt werden dürfen, wenn sie in diesem Drittland einen im Wesentlichen gleichwertigen Schutz genießen wie in der EU. Für die USA und ggf. auch für Datenübermittlungen in weitere Drittländer wurde ein solches angemessenes Schutzniveau verneint. Einige der Anbieter, die technisch ausgereifte Lösungen bereitstellen, erfüllen die datenschutzrechtlichen Anforderungen nicht. Dies trifft derzeit (Stand 3. Juli 2020) z. B. auf die Dienste Blizz, Cisco WebEx, Cisco WebEx über Telekom, Google Meet, GoToMeeting, Microsoft Teams, Skype, Skype for Business Online und Zoom zu.

Der EuGH erklärte zudem das Privacy Shield Abkommen für unwirksam. Mit der Unwirksamkeit des Privacy Shield Abkommens waren viele Datentransfers nicht mehr zulässig, weil die sich auf das Privacy Shield als Rechtsgrundlage zur Datenübermittlung gestützt hatten.

Was sind die fundamentalen Unterschiede der US-Gesetze zum Datenschutz und europäischen Gesetzen zum Datenschutz?

Der EuGH hat das Privacy Shield für ungültig erklärt, weil das durch den EuGH bewertete US-Recht kein Schutzniveau bietet, das dem in der EU im Wesentlichen gleichwertig ist. Das US-Recht, auf das der EuGH Bezug genommen hat, betrifft z. B. die nachrichtendienstlichen Erhebungsbefugnisse nach Section 702 FISA und Executive Order 12333. Amerikanische Internet-Firmen und IT-Dienstleister müssen US-Behörden Zugriff auf gespeicherte Daten geben. Dies gilt auch wenn die Speicherung der Daten nicht in den USA erfolgt. Dies widerspricht der Charta der Grundrechte der Europäischen Union in den Art. 7 Achtung des Privat- und Familienlebens, Art. 8 Schutz personenbezogener Daten und Art. 47 Recht auf einen wirksamen Rechtsbehelf und ein unparteiisches Gericht.

Warum ist MVC „sicher besprechen“ die ideale Plattform für datenschutzkonforme Videokonferenzen?

Die Videokonferenzplattform „sicher besprechen“ sowie das dazugehörige Managementportal MVC 360° werden komplett von MVC betrieben. Die Rechenzentren sind ISO-zertifiziert und befinden sich ausschließlich in Deutschland und der Schweiz. Alle Daten werden verschlüsselt und die Speicherung der Daten ist konform im Hinblick auf die DGSVO sowie das TKG. Der Betrieb, das Management und der Support der virtuellen Konferenzräume erfolgt ausschließlich das deutsche Unternehmen MVC Mobile VideoCommunication GmbH. Hinter dem Unternehmen steht keine US-Muttergesellschaft – es fließen keinerlei Daten an Dritte weiter.

MVC Mobile VideoCommunication GmbH
Campus Kronberg 7
D-61476 Kronberg im Taunus
Telefon: +49 69 633 99 100
E-Mail: info@mvc.de
www.mvc.de