Industrie- und Handelskammer Bonn/Rhein-Sieg

Videokonferenz-Tools: Tipps zur Auswahl und Verwendung

Quelle: https://www.datenschutzbeauftragter-info.de/videokonferenz-tools-tipps-zur-auswahl-und-verwendung/

Gerade in der aktuellen Situation arbeiten mehr Arbeitnehmer als bislang aus dem Homeoffice. Auch in den Unternehmen die, zum Beispiel aufgrund Ihrer Tätigkeit Bedeutung für unser Leben haben, wird der persönliche Kontakt auf ein notwendiges Minimum heruntergefahren. Daher ist es besonders wichtig ein Videokonferenz-Tool implementiert zu haben und doch den Schutz von personenbezogenen Daten und auch den von Unternehmensgeheimnissen nicht aus dem Auge zu verlieren.

Datenschutzrechtliche Grundlage und vertragliche Vorkehrungen

Mit der Rechtsgrundlage für den Einsatz im Unternehmen, der Notwendigkeit einer Einbindung des Betriebsrats, sowie dem Erfordernis des Abschlusses einer Vereinbarung über die Auftragsverarbeitung bei SaaS (Software as a Service) –Tools beschäftigten wir uns bereits im letzten Jahr(Artikel vom 23.01.2019 ab Seite 4 des Dokumentes).

Letztlich sollten sich Unternehmen bei der Auswahl einer Software zunächst stets fragen, ob eine On-Premise-Variante (also auf den eigenen Servern gehostete Software) in Frage kommt oder aus unterschiedlichen Gründen (z.B. fehlendes Know-how oder fehlende Kapazität der IT, gerade bei kleineren Unternehmen) eine SaaS-Lösung eingesetzt werden soll.

Dabei ist natürlich immer vorab zu prüfen, ob der SaaS-Dienstleister –der als Auftragsverarbeiter eingesetzt werden soll –für die Verarbeitung geeignete technische und organisatorische Maßnahmen bietet, damit die Verarbeitung datenschutzkonform erfolgt. Dies ergibt sich bereits aus Art. 28 Abs. 1 DSGVO.

Grundsätzlich sollte ein Anbieter aus Deutschland oder dem EWR bevorzugt werden, da bei Auftragsverarbeitern aus einem sog. Drittland zusätzlich zu prüfen ist ob ein angemessenes Schutzniveau besteht.

Welche technischen Möglichkeiten sollte das Videokonferenz-Tool bieten?

Der Verantwortliche wird die technischen Maßnahmen anhand der geplanten Verarbeitung ausrichten müssen. Dabei gilt es zu beachten wie sensibel die Daten sind, die über das Videokonferenz-Tool geteilt werden sollen. Gerade in Zeiten von Corona kann es auch vorkommen, dass Videokonferenz-Tools für zuvor nicht geplante Zwecke verwendet werden und daher eine neue Bewertung der vorher gewählten Maßnahmen notwendig wird.

Der Verantwortliche wird letztlich für die Auswahl des Tools und den damit erreichten Schutz haften. Die DSGVO hat zwar mit den Grundsätzen Privacy by Design und Privacy by Default Regelungen getroffen, die sich offenkundig an Hersteller richten, adressiert diese jedoch nicht, sondern nimmt vor allem den Verantwortlichen in die Pflicht. So stellt auch der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg, in seinen Ergebnissen der Anhörung zur Evaluierung der DSGVO, fest:

„Beim Begriff „Datenschutz durch Technikgestaltung“ (Privacy by Design), der im Artikel 25 Abs. 1 DSGVO für den Verantwortlichen vorgeschrieben ist, stellt sich in der Praxis der Adressatenkreis als nicht weitreichend genug heraus. Da Verantwortliche in der Regel nicht selbst Software entwickeln und in weiten Teilen Standard-und Anwendungssoftware von Herstellern bzw. Anbietern, zum Teil sogar von solchen mit globaler, nationaler oder regionaler Monopol-oder zumindest marktbeherrschender Stellung, beziehen und nutzen müssen, läuft diese Forderung häufig ins Leere.

“Die Ergebnisse der Anhörung des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg vom 28. Juni 2019 bei der IHK Stuttgart zur Evaluierung der DSGVO finden Sie im Anhang des 35. Datenschutz-Tätigkeitsberichts ab Seite 125.

Technische Maßnahmen

Die hier dargestellten technischen Maßnahmen und Einstellungserwägungen sind nicht abschließend, letztlich kommt es dabei (wie oben erläutert) immer auf den Einzelfall an.

Leider werden auch die Voreistellungen der Software nur selten dem Grundsatz Privacy by Default nachkommen, sondern die herstellereigene Vorstellung des Kundenwunsches umsetzen.

- **Verschlüsselung**: Dabei gilt es im Einzelfall zu bestimmen welche Art von Verschlüsselung benötigt wird, dies hängt letztlich von der Art der Daten ab die verarbeitet werden soll.
- **Business-Version**: Für die Verwendung im Unternehmen eignen sich nicht Tools, die für den privaten Einsatz gedacht sind. Zum Beispiel sind Apps wie WhatsApp oder FaceTime grundsätzlich ungeeignet.
- **Beschränkung von Logfiles**: Logfiles sollten nur soweit diese erforderlich sind erstellt werden. 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.
- **Chatverläufe und Dateiaustausch**: Auch hier ist sicherzustellen, dass diese nur für den benötigten Zeitraum zur Verfügung stehen und 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.
- **Möglichkeit, Aufnahmen der Videokonferenz zu regulieren**: Viele Tools bieten mittlerweile die Möglichkeit die Videokonferenz aufzunehmen. Dies dürfte in den meisten Fällen jedoch nur mit einer Einwilligung aller Teilnehmer zulässig sein. 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.
- **Einsatz bei Bewerbungsverfahren**: Auch wenn Bewerbungsverfahren wohl vermehrt nicht mehr aktiv betrieben werden, um eine Verbreitung des Virus zu vermeiden. Sollte ein Unternehmen Bewerbungsgespräche nun via Videokonferenz durchführen wollen, so sollten sie dies im Voraus sorgfältig prüfen. Wir berichteten (wenn auch nach altem Recht).
- **Blurr-Möglichkeit**: Zudem bieten Videokonferenz-Tools teilweise die Möglichkeit, den Hintergrund vollständig auszugrauen. Dies hätte wohl auch Professor Robert Kelly geholfen, dessen Kinder während eines Liveinterviews mit BCC News, dass er aus dem Homeoffice führte, durchs Bild liefen. Dies ist bei geschlossenen Schulen und Kitas wohl auch aktuell in vielen Haushalten nicht ausgeschlossen, kann aber technisch verhindert werden. Hier können Unternehmen mit technischen Mitteln für mehr Datenschutz und Privatsphäre sorgen.
- **Einrichtung von Zugangsbeschränkungen (wie Login, oder bei Gästen nur mit Zustimmung des Organisators):** Vielleicht denken Sie jetzt, dass dies doch selbstverständlich ist und es niemanden gibt der Videokonferenz-Tools ohne diese technische Maßnahme einsetzt. ABER vor gerade einer Woche meldete das Fachmagazin c't: „Ein vom bayerischen Innenministerium genutztes Videokonferenzsystem stand ungeschützt im Netz. So konnte c't an einer internen Sitzung zum Coronavirus mit Bayerns Innenminister Joachim Herrmann teilnehmen."

Organisatorische Maßnahmen

Auch die hier dargestellten organisatorischen Maßnahmen sind nicht abschließend, denn auch dabei kommt es (wie oben) auf den Einzelfall an.

Vor allem sind die Mitarbeiter entsprechend zu informieren und zu sensibilisieren, welche Daten über das Tool (vor allem auch mit Externen) geteilt werden dürfen. Hierzu kann, wie oben bereits erwähnt, auch mit Black- oder Whitelists gearbeitet werden, die der jeweiligen Tätigkeit des Unternehmens angepasst werden.

- **Desktop-Sharing**: Eben eine solche Sensibilisierung gilt es für das Teilen des Desktops herzustellen. Hier 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.
- **Digitale Führungen**: Gerade durch die aktuellen Umstände wird es vorkommen, dass geplante Werksführungen nunmehr digital stattfinden. Dabei gilt es, wie auch beim Desktop-Sharing zu beachten, dass nur notwendige Informationen geteilt werden. Legen Sie also Routen fest, welche Sie abgehen wollen und der Gesprächspartner auch vor Ort gesehen hätte. Informieren Sie in den betroffenen Bereichen auch andere Mitarbeiter über die geplante Führung und gewähren Sie bei Bedenken auch Abwesenheiten zu dieser Zeit.

Weitere technische und organisatorische Maßnahmen zum Schutz von Videokonferenzen vor Störrungen von Außen

- **Verwendung einer eindeutigen Meeting-ID.**
  Die Verwendung einer persönlichen ID oder wiederkehrende IDs für Meetings sollte vermieden werden und es sollte immer eine eindeutige, neu generierte Meeting-ID verwendet werden.
- **Meeting Passwort**
  Fügen Sie für jedes Meeting ein Passwort hinzu, dass Sie an die Meeting Teilnehmer verteilen.
- **Technische Vorgaben machen**
  Um die Übertragen ungebetener Inhalte zu verhindern, können die Organisatoren von Meetings verhindern, dass Kameras der Teilnehmer und Mikrophone aktiviert oder Desktopssharing betrieben werden können. Diese können gegebenenfalls gezielt in einer Besprechung aktiviert werden. Ebenso lässt sich die Chatfunktion und das Einsehen einer Teilnehmerliste unterbinden. Hier kommt es natürlich auf die Art des Videomeetings und die Bekanntheit der Teilnehmer untereinander bzw. mit dem Organisator an.
- **Nur angemeldete Benutzer zulassen.**
  Mit dieser Sicherheitseinstellung spielt es zum Beispiel bei Zoom keine Rolle, ob die Meeting-ID sogar das Kennwort einem Hacker bekannt sind. Diese Einstellung erfordert, dass alle Benutzer mit der E-Mail, über die sie eingeladen wurden, angemeldet sind.
- **Wartezimmer aktivieren.**
  Mit der Einstellung „Wartezimmer“ in Zoom beginnt die Besprechung erst, wenn der Gastgeber eintrifft und alle Teilnehmer zur Besprechung hinzufügt. Die Teilnehmer können nicht miteinander kommunizieren, solange sie sich im Wartezimmer befinden. Dem Gastgeber des Meetings bietet sich somit die Möglichkeit, manuell nochmal zu überprüfen, wer an der Besprechung teilnehmen kann und ungebetene Gäste zu identifizieren.
- **Aktivieren des Signaltons**
  Mit dem beitreten oder dem verlassen eines Meeting erklingt ein Signalton. Dies stellt sicher, dass kein ungebetener Gast unbemerkt an der Besprechung teilnehmen. Dieses akustische Signal ist normalerweise standardmäßig eingeschaltet und sollte in den Einstellungen vor Beginn des Meetings noch einmal überprüft werden.

- **Schließen des virtuellen Meetingraums, sobald das Meeting begonnen hat.** Sobald alle erwarteten Teilnehmer eingetroffen sind, gibt es bei einigen Videokonferenzlösungen die Möglichkeit, daas der virtuelle Meetingraum geschlossen wird. Damit können keine weiteren Personen diesem Meeting mehr beitreten.