ALTHAMMER & KILL

Übersicht Videokonferenz-Tools

Bewertung der Vediso-empfohlenen Werkzeuge aus Datenschutz-Perspektive

Videokonferenz-Tools sind eine sinnvolle Lösung; mit ihnen können Mitarbeitende, Lieferanten und Kunden Meetings abhalten und gemeinsam arbeiten, ohne dafür am selben Ort sein zu müssen – in Zeiten von Ausgangsbeschränkungen vermutlich die einzig praktikable Maßnahme, um weiter kollaborativ arbeiten zu können. Sie tragen damit nicht nur zu einer effizienten standortübergreifenden Zusammenarbeit im Homeoffice oder über große Entfernungen bei, sondern können auch zu kürzeren Reisezeiten sowie verringerten Reisekosten führen.

Doch welche Aspekte sind bei Videokonferenz-Diensten aus Perspektive des Datenschutzes zu beachten? Wir haben die Anbieterübersicht des Vediso unter die Lupe genommen und diese aus dem Blickwinkel des Datenschutzes bewertet. Die folgende Übersicht mit Kurzbeurteilungen zu den gängigen Lösungen bietet Hilfestellung.

Bewertungskriterien

Das Datenschutz-Freundlichkeits-Barometer zeigt Ihnen auf einen Blick, wie die betrachteten Lösungen im Hinblick auf ihre DSGVO-Compliance und der Erfahrungswerte und persönlichen Einschätzungen unserer Berater abschneiden. Andere Kriterien haben wir bewusst nicht mit einfließen lassen, da diese je nach vorgesehenem Einsatzbereich ganz unterschiedlich gewichtet werden müssen. Die Bewertung hängt jedoch nicht zuletzt auch immer von Ihnen selbst ab, d.h. von den Daten, die während einer Videokonferenz ausgetauscht werden. Gehören diese nämlich zu den „besonderen Kategorien“ personenbezogener Daten im Sinne des Datenschutzes (z.B. Gesundheitsdaten), gelten höhere Sicherheitsanforderungen.

Name	Plattformen	Sicherstellung Datenschutzniveau	Lizenz	Vertrag zur Auftragsdatenverarbeitung	Anmerkung	Bewertung
Google Hangouts	Mac/Win/Linux	Privacy Shield	proprietär	in AGB inkludiert	Erhebliche Nachbesserungen durchgeführt	[?]
GotoMeeting	Mac/Win/Linux	Privacy Shield	Proprietär	Data Processing Addendum		[?]
Jitsi Meet	Mac/Win/Linux	On Premise	Apache Licence	-	iOS-App kommuniziert mit Dritten	[?]
Microsoft Teams	Mac/Win/Linux	Privacy Shield	proprietär	Online Services & Terms	Einsatz unter KDG strittig	[?]

Datenschutz-Freundlichkeits-Barometer
[?] empfehlenswert
[?] risikobehaftet
[?] nicht empfehlenswert

Zoom	Mac/Win/ (Linux)	Privacy Shield / EU-Standard-vertragsklau-seln	proprietär	Data Processing Addendum	Öffentliche Kritik bisher nicht ent-kräftet; jüngst großes Daten-leck bekannt geworden.	[?]

Alle Angaben sind ohne Gewähr. Die Situation ist derzeit sehr dynamisch, so dass sich die Einschätzung nahezu täglich ändern kann (Stand 16.04.2020)

Alle Anbieter, die unter den „Privacy Shield“ fallen, haben ihren Firmensitz in den USA. Dies bedeutet keineswegs, dass die Nutzung dieser Lösungen im EU-Raum nicht DSGVO-kompatibel wäre; vielmehr regelt das Privacy Shield Abkommen zwischen EU und Vereinigten Staaten, dass Daten unter strengen Voraussetzungen auch von US-Anbietern gespeichert werden dürfen. „On Premise“ hingegen bedeutet, dass die Daten in der eigenen Organisation verbleiben und dort lokal gespeichert werden, z.B. in einem eigenen Rechenzentrum.

Tipps zur Einführung

- Beteiligen Sie frühzeitig die **Mitarbeitervertretung** und den **Datenschutzbeauftragten**.
- Schließen Sie einen **Vertrag zur Auftragsverarbeitung** ab.
- Erstellen Sie **Leit- und Richtlinien** für Nutzer und führen Sie **Schulungen und Einweisungen** in die Tools durch. Dies sorgt für eine höhere Akzeptanz und schnellere Einarbeitung.
- Regeln Sie von Anfang an, **wofür eine Videokonferenz genutzt** werden darf. Klären Sie die Nutzer auf, wie sie sich zu verhalten haben, um **mögliche Datenabflüsse** zu vermeiden.
- **Reduzieren Sie das Screensharing** auf ein Minimum - einige Tools bieten Weichzeichner, die den Hintergrund unscharf werden lassen – nutzen Sie sie.
- Erstellen Sie für ein selbst gehostetes Videokonferenztool eine **Datenschutzerklärung**.
- Konfigurieren Sie die Software **sorgfältig und datenschutzfreundlich**. Gehen Sie alle Einstellungsmöglichkeiten durch und handeln Sie dabei nach dem **Minimalprinzip**, geben Sie also nur so viel Funktionen frei wie nötig. Im Zweifel können weitere auch später noch freigeschaltet werden.
    - Achten Sie auf eine vollständige **Verschlüsselung der Übertragung**.
    - Prüfen Sie die **Handhabung der Benutzerverwaltung** – bspw. Integrationsmöglichkeiten in bestehende Dienste, wie z.B. Active Directory.
    - Regeln Sie die **Aufzeichnung** von Ton und Bild – diese sollten nur wenn nötig erstellt werden.
    - **Prüfen Sie Logfiles**, in denen personenbezogene Daten gespeichert werden könnten.
    - Schalten Sie das **Profiling der Nutzer** möglichst ab.
    - Prüfen sie die **Transportwege und Speicherorte** und klären Sie wo Daten gespeichert werden wenn diese ausgetauscht werden können.
    - Gäste sollten zunächst in einem **Wartebereich** landen und erst **durch Moderatoren zugelassen** werden.
    - Nehmen Sie **Einstellungen zum Screensharing** vor – die Steuerung sollte nur **nach Freigabe** erfolgen.

Weitere Informationen

Um sie auch während der COVID-19 Pandemie bestmöglich und pragmatisch mit Informationen zu Datenschutz, IT-Sicherheit und IT-Compliance zu unterstützen, stellen wir Ihnen unter www.corona-datenschutz.de verschiedene **Merkblätter, Umsetzungshilfen, Checklisten und Zusatzinformationen** zu den aktuellen Fragestellungen zum **kostenlosen Download** zur Verfügung.

Datenschutz-Freundlichkeits-Barometer
[?] empfehlenswert
[?] risikobehaftet
[?] nicht empfehlenswert

Und denken Sie daran:

Für Rückfragen und Hilfestellungen stehen Ihnen ihr Datenschutzbeauftragter, ihr IT-Sicherheitsbeauftragter, der IT-Systemadministrator und das gesamte Team von Althammer & Kill jederzeit zur Verfügung.

Datenschutz-Freundlichkeits-Barometer

- [?] empfehlenswert
- [?] risikobehaftet
- [?] nicht empfehlenswert