Mittelstand 4.0
Kompetenzzentrum
Chemnitz

Betrieb 4.0
machen!

Recht behalten!

Nachgelesen

Business-Guide: Datenschutz in Videokonferenzen

Michael Rätze

Mittelstand-Digital

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

Das Arbeiten außerhalb einer Betriebsstätte oder von Büroräumlichkeiten nimmt stetig zu. Sei es aus der Bestrebung, den Arbeitnehmern eine flexiblere Gestaltung ihrer Work-Life-Balance zu ermöglichen oder sei es aufgrund einer epidemischen Lage, welche ganze Nationen und damit auch das Arbeitsleben betrifft. Um trotz räumlicher Trennung in der Gruppe kommunizieren zu können, erfreuen sich Videokonferenzen (Online-Meetings, Webkonferenzen, etc.) großer Beliebtheit. Der Markt bietet vielerlei Angebote. Von kostenpflichtigen bis kostenlosen Angeboten ist alles erhältlich. Hier gilt es, den für sich richtigen Anbieter auszuwählen. Auch wenn die Wahl manchmal schnell gehen muss, darf der Datenschutz nicht vernachlässigt werden. Was Sie bei der Wahl des richtigen Anbieters u. a. aus datenschutzrechtlicher Sicht zu beachten haben, erläutern wir nachfolgend.

Verantwortlichkeit

Der Unternehmer ist grundsätzlich Verantwortlicher im Sinne des Art. 4 Abs. 7 DSGVO für die Verarbeitung der personenbezogenen Daten seiner Arbeitnehmer und seiner Kunden. Dies gilt auch bei der Nutzung von Videokonferenzen. Eine Verschiebung der Verantwortlichkeit hin zum Anbieter der Videokonferenzen findet nicht statt. Daher sollten Sie als Unternehmen die folgenden Punkte beachten.

On-Premise vs. SaaS

Bei der Speicherung der Daten kann technisch zwischen zwei Alternativen unterschieden werden. Den sog. On-Premise-Lösungen und den sog. SaaS-Lösungen. Bei den On-Premise-Lösungen wird eine Software etwa als Lizenz- und Nutzungsmodell erworben und auf firmeneigenen Servern gehostet, also untergebracht. Dies bietet den Vorteil der Kontrolle des Speicherortes und bringt so ein großes Stück Datenhoheit. Außerdem lässt sich dies besser an die individuellen Bedürfnisse anpassen. Der Nachteil liegt in der Notwendigkeit der Bereitstellung entsprechender IT-Infrastruktur, d. h. der Betrieb eigener Server inklusive deren Wartung, wofür regelmäßig ein IT-Techniker nötig wird. Da dies für viele

Unternehmen nicht realisierbar ist, bietet sich der Rückgriff auf die sog. SaaS-Lösungen an. Bei diesen „Software-as-a-Service"-Lösungen erwirbt man das Recht der Nutzung der Software sowie das entsprechende Hosting (Bereitstellen) auf Servern des Anbieters, oft in Form eines Abonnements. Der Start ist somit sehr leicht, da keine eigene IT angeschafft werden muss und auch die spätere Wartung entfällt. Dies sorgt für einen günstigen Einstieg und hohe Flexibilität. Meist werden unterschiedliche vordefinierte Pakete angeboten oder man kann bestimmte Optionen dazu buchen bzw. abwählen, um den jeweiligen Anforderungen gerecht zu werden. Bei dieser recht bequemen Lösung muss jedoch beachtet werden, dass die Daten beim Anbieter als Auftragsverarbeiter gem. Art. 28 Abs. 1 DSGVO verarbeitet werden. Der Verantwortliche (der Unternehmer) muss prüfen, ob der Anbieter geeignete technische und organisatorische Maßnahmen für eine datenschutzkonforme Verarbeitung bietet. Welche Variante zu bevorzugen ist, muss jedes Unternehmen nach seinen Möglichkeiten und Anforderungen entscheiden.

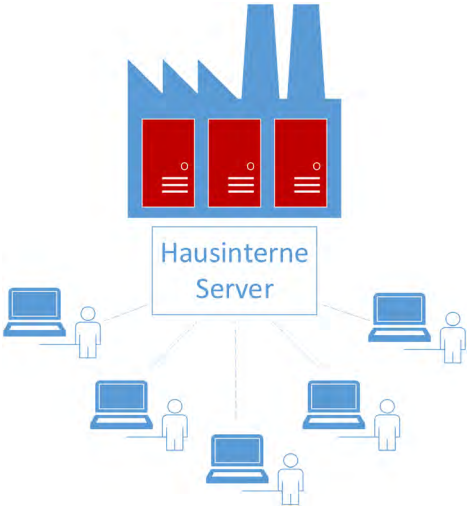

Abbildung 1: On-Premise-Lösung

Business-Versionen

Bei der Wahl des entsprechenden Anbieters sollten Sie darauf achten, die jeweiligen Business-Versionen zu nutzen. Also die Versionen, die für den gewerblichen Bereich gedacht sind. Software, die lediglich für den privaten Gebrauch vorgesehen sind, sollten Sie meiden. Dazu zählen bspw. die Video-Funktion bei WhatsApp, Facetime von Apple oder Skype in der privaten Version. Insbesondere WhatsApp überträgt bei der Installation alle gespeicherten Kontaktdaten auf die eigenen Server, unabhängig davon ob die jeweiligen Personen selbst WhatsApp nutzen. Auch die Zugehörigkeit zu Facebook und die evtl. Weitergabe der Daten von

WhatsApp zu Facebook ist sehr intransparent. Ein weiteres Problem bei diesen Anbietern ist, dass die Server in den USA stehen und somit außerhalb des Geltungsbereich der EU und damit der DSGVO. Darin läge eine Datenübertragung in ein Drittland, die nur unter bestimmten Voraussetzungen möglich ist. Die Unternehmen müssten garantieren, das gleiche Datenschutzniveau zu gewährleisten, wie es in Europa der Fall ist. Dies kann bspw. durch eine sog. Privacy-Shield-Zertifizierung geschehen.

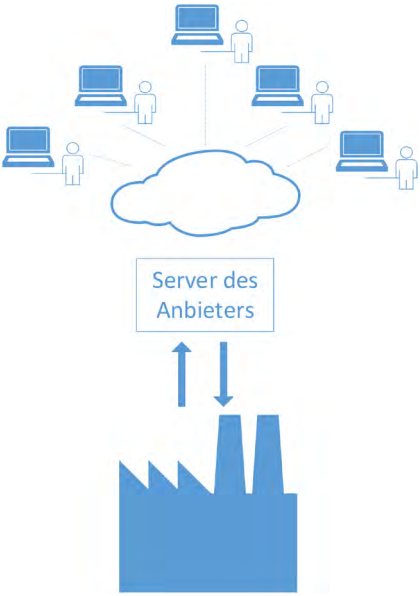

Abbildung 2: SaaS-Lösung

Logfiles

Sogenannte Logfiles protokollieren in Computer- oder Netzwerksystemen verschiedene Prozesse, daher werden sie auch Protokolldateien genannt. Bei Videokonferenzen sollten Sie darauf achten, dass der Anbieter nur Logfiles erstellt, soweit diese nötig sind. Dies kann etwa für die anbieterseitige Fehlerbehebung der Fall sein. Fällt dieser Zweck weg, sind die Dateien durch den Anbieter zu löschen. Werden Sie nach solchen Logfiles gefragt oder können Sie diese in den Einstellungen ändern, sollten Sie diese eingeschränkte Nutzung wählen.

Chatverläufe

Chatverläufe müssen nach Beendigung der Videokonferenz automatisch gelöscht werden. Ist der Inhalt ggf. länger relevant, weil er etwa auch geteilte Dateien beinhaltet, muss zumindest ein bestimmter Zeitraum festgelegt werden. In diesem Zeitraum können die Beteiligten die Dateien noch herunterladen, bevor sie gelöscht werden.

Aufzeichnung

Viele Programme bieten eine Möglichkeit, die Videokonferenz aufzuzeichnen. Dies ist nur mit der Einwilligung der Beteiligten rechtmäßig, soweit keine Ausnahme greift. Eine Einwilligung ist gem. Art. 4 Nr. 11 DSGVO jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung. Das Merkmal der Freiwilligkeit ist nur gegeben, wenn der Betroffene ohne jeden Zwang zustimmt. Problematisch kann das in Konstellationen werden, in denen es zu der aufzuzeichnenden Videokonferenz keine Alternativen gibt. Dem Betroffenen würde also ein Nachteil entstehen, wenn er sich gegen die Aufzeichnung ausspricht und daher nicht teilnehmen kann. Als Verantwortlicher müssen Sie dafür Sorge tragen, dass dies nicht geschieht. Das kann dadurch geschehen, dass alle Informationen der Videokonferenz an die nichtteilnehmenden Betroffenen weitergeleitet werden.

Zugangsbeschränkungen

Sie sollten darauf achten, dass nur diejenigen teilnehmen, die auch teilnehmen sollen. Die Zugangsdaten zur Videokonferenz sollten daher gezielt an die Teilnehmer versendet werden oder der Zugang zur Videokonferenz durch den Organisator freigegeben werden.

Desktop-Sharing

Das sog. Desktop-Sharing ist eine Funktion, die viele Programme bieten, um den eigenen Bildschirm den Teilnehmern sichtbar zu machen. So lassen sich verschiedenste Inhalte darstellen, um besprochen zu werden. Dabei sollten Sie beachten, dass nur die Sachen gezeigt werden, die für die Konferenz wichtig sind. Das bedeutet, dass auf dem Desktop keine Dateisymbole sichtbar sein sollten. Weiter sollten keine Benachrichtungen angezeigt werden, da diese sonst auch für die anderen Teilnehmer sichtbar werden. Zu denken ist hierbei etwa an Benachrichtungen durch das installierte E-Mail-Programm. Oft werden durch diese Programme neue E-Mails durch ein kleines Fenster unten rechts angezeigt. In diesem Fenster stehen meist der Absender, der Betreff und teilweise schon der Beginn der E-Mail. Gleiches gilt für Ordner oder Akten im Hintergrund, die evtl. zu erkennen sind.

Betriebsrat

Noch ein arbeitsrechtlicher Hinweis zum Schluss. Die Nutzung von Videokonferenzen unterliegt der Mitbestimmung des Betriebsrats gem. § 87 Abs. 1 Nr. 6 BetrVG. Die Zustimmung des Betriebsrats wird danach notwendig für die Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen. Die Rechtsprechung legt diesen Mitbestimmungstatbestand sehr weit aus. Es ist demnach nicht zwingend, dass die Maßnahme zur Überwachung der Mitarbeiter bestimmt ist. Es genügt, wenn sie dafür geeignet ist. Die Videokonferenz dürfte somit

Abbildung 2: Betriebsrat

darunterfallen, da die Teilnehmer in nahezu allen Programmen angezeigt werden und es so möglich ist, nachzuvollziehen, wer teilnimmt und wer nicht. Aber auch durch das Videobild als solches, Wortmeldungen oder Beiträge im Chat, lässt sich auf die Anwesenheit oder Abwesenheit einzelner Arbeitnehmer schließen, was eine Überwachung im Sinne des § 87 Abs. 1 Nr. 6 BetrVG darstellt. Letztlich zählt auch das Erheben personenbezogener Daten zum Überwachen und da auch die IP-Adresse ein personenbezogenes Datum darstellt[1], ist das Merkmal der Überwachung auch dann erfüllt, wenn der Arbeitnehmer ohne Bild und mit geändertem Namen an der Videokonferenz teilnimmt.

Anmerkungen

[1] BAG 13.12.2019 – 1 ABR 7/15, NZA 2017, 657, Rn. 40.

Autoren

Michael Rätze ist wissenschaftlicher Mitarbeiter an der Professur für Privatrecht und Recht des geistigen Eigentums von Prof. Dr. Dagmar Gesmann-Nuissl an der Technischen Universität Chemnitz. Im Mittelstand 4.0- Kompetenzzentrum Chemnitz ist er als Fachkoordinator Recht 4.0 tätig.

michael.raetze@betrieb-machen.de

Weitere Informationen

Das Mittelstand 4.0-Kompetenzzentrum Chemnitz gehört zu Mittelstand-Digital. Mit Mittelstand-Digital unterstützt das Bundesministerium für Wirtschaft und Energie die Digitalisierung in kleinen und mittleren Unternehmen und dem Handwerk.

Was ist Mittelstand-Digital?
Mittelstand-Digital informiert kleine und mittlere Unternehmen über die Chancen und Herausforderungen der Digitalisierung. Die geförderten Kompetenzzentren helfen mit Expertenwissen, Demonstrationszentren, Best-Practice-Beispielen sowie Netzwerken, die dem Erfahrungsaustausch dienen. Das Bundesministerium für Wirtschaft und Energie (BMWi) ermöglicht die kostenfreie Nutzung aller Angebote von Mittelstand-Digital.

Der DLR Projektträger begleitet im Auftrag des BMWi die Kompetenzzentren fachlich und sorgt für eine bedarfs- und mittelstandsgerechte Umsetzung der Angebote. Das Wissenschaftliche Institut für Infrastruktur und Kommunikationsdienste (WIK) unterstützt mit wissenschaftlicher Begleitung, Vernetzung und Öffentlichkeitsarbeit.

Weitere Informationen finden Sie unter www.mittelstand-digital.de

IMPRESSUM:

Herausgeber:
Mittelstand 4.0-Kompetenzzentrum Chemnitz
Geschäftsstelle
c/o Technische Universität Chemnitz
Prof. Dr.-Ing. habil. Ralph Riedel
DE – 09107 Chemnitz
Tel: 0371 531 19935
Fax: 0371 531 819935
E-Mail: info@betrieb-machen.de
Web: www.betrieb-machen.de
www.kompetenzzentrum-chemnitz.digital

Redaktion & Gestaltung
Michael Rätze & Anikó Lessi

Bildnachweis Titel:
Chris Montgomery auf Unsplash