IWW INSTITUT
INFORMATIONSDIENSTE

DATENSCHUTZ

Zoom, Teams, Skype & Co.: Videokonferenz-Tools im datenschutzrechtlichen Fokus

von RA Christian Galetzka, LL.M. und Dipl. Jur. Sophie Garling, Würzburg

| Aufgrund der Corona-Pandemie rücken viele Tätigkeiten in die Isolation ins Homeoffice. Der Bedarf an Web-Meetings und Visualisierungs-Tools für einen möglichst persönlichen Kundenkontakt ist exponentiell gestiegen und steigt weiter. Von Microsoft Teams und Skype, über Zoom bis hin zum Hosting einer eigenen Web-Meeting-Plattform – die Angebote sind schier unerschöpflich. In diesem Zusammenhang tauchen immer wieder datenschutzrechtliche Fragestellungen und teils überzogen geäußerte Bedenken auf. Personenbezogene Daten würden durch das gesprochene Wort und Chatverläufe über die Teilnehmer gesammelt, das unbefugte Mithören, Aufzeichnen und Auswerten der Inhalte sei möglich etc. Aber halten diese Bedenken einer gewissenhaften datenschutzrechtlichen Prüfung tatsächlich Stand? |

1. Videokonferenz-Tools – was sagt der Datenschutz?

Mit der Übertragung von Bild und Ton werden automatisch, ganz unabhängig von Chatinhalten, bei jeder Videokonferenz personenbezogene Daten i. S. v. Art. 4 Nr. 1 DS-GVO übermittelt. Da bei der Nutzung von Videokonferenz-Tools im geschäftlichen Umfeld der einer datenschutzrechtlichen Regulierung weitgehend entzogene Privatbereich verlassen wird, ist der Anwendungsbereich der DS-GVO unproblematisch eröffnet. Damit stellt sich die Frage nach den Anforderungen an eine datenschutzkonforme Ausgestaltung für das Unternehmen, das das Videokonferenz-Tool seiner Wahl für die Kommunikation einsetzen möchte. Im Wesentlichen ergibt sich ein dreistufiges Prüfprogramm als Checkliste, um den Einsatz des Videokonferenz-Tools datenschutzrechtlich in den Griff zu bekommen:

1. Auffinden einer geeigneten Rechtsgrundlage für die datenschutzrechtliche Rechtfertigung (Art. 6, 9 DS-GVO)

2. Erfüllung von Informationspflichten gegenüber den Teilnehmern der veranstalteten Videokonferenz (Art. 13, 14 DS-GVO)

3. Absicherung des Verhältnisses zum Anbieter des jeweiligen Videokonferenz-Tools einschließlich Prüfung der vom Anbieter getroffenen technischen und organisatorischen Maßnahmen (regelmäßig: Auftragsverarbeitung nach Art. 28 DS-GVO)

a) Rechtsgrundlage

Die Rechtsgrundlage für den Einsatz von Videokonferenz-Tools ist essenziell für die datenschutzrechtliche Absicherung, aber schlussendlich nicht schwer zu finden. Auch abseits der Einwilligung – regelmäßig impraktikabel, insbesondere bei Konferenzen mit einem sehr großen Teilnehmerkreis – wird der Verantwortliche regelmäßig die Erfüllung eines Vertrags (Art. 6 Abs. 1 lit. b DS-GVO) oder berechtigte Interessen (Art. 6 Abs. 1 lit. f DS-GVO) als Rechtsgrundlage anführen können.

Auch bei der Nutzung von Konferenztools zur Arbeitsüberwachung, um z. B. durch Anwesenheitsangaben (Anwesend/Beschäftigt/Abwesend) Arbeitszeitkontrollen durchzuführen, kann als Rechtsgrundlage auf Art. 6 Abs. 1 lit. f DS-GVO zurückgegriffen und eine Interessenabwägung geführt werden. Zu beachten ist in diesem Fall allerdings, dass gem. § 87 Abs. 1 Nr. 6 BetrVG dem Betriebsrat, sofern es ihn gibt, ein Mitbestimmungsrecht bei der Einführung technischer Unterstützung zur Arbeitnehmerüberwachung zusteht.

Häufiger werden jedoch Fälle sein, in denen lediglich die unternehmensinterne Kommunikation erleichtert werden soll. Hier dürfte das unternehmerische Interesse überwiegen bzw. sogar die Kommunikation zwischen Arbeitgeber und Arbeitnehmern als essenzieller Bestandteil der Abwicklung des Beschäftigungsverhältnisses angesehen und damit auf die vertragliche Rechtsgrundlage des Art. 6 Abs. 1 lit. b DS-GVO gestützt werden können.

Funktionen wie das Aufmerksamkeitstracking, die Aufzeichnung von Konferenzen, Screen-Sharing oder der Mitschnitt von Ton werden i. d. R. stets einer Einwilligung gem. Art. 6 Abs. 1 lit. a DS-GVO bedürfen. Aufgrund des schweren Datenschutzeingriffs ist darüber hinaus in jedem dieser Einzelfälle zu prüfen, ob die Funktion tatsächlich erforderlich ist.

b) Transparenz- und Informationspflichten (Art. 12 bis 14 DS-GVO)

Nach Art. 12 bis 14 DS-GVO muss der Verantwortliche, also das Unternehmen, den Konferenzteilnehmern die wesentlichen Informationen über die Verarbeitungen, die über das Videokonferenz-Tool stattfinden, zur Verfügung stellen. Informiert werden muss in „präziser, transparenter, verständlicher und leicht zugänglicher Form“ (Art. 12 Abs. 1 S. 1 Hs. 1 DS-GVO). Da dies zum Zeitpunkt der Erhebung von personenbezogenen Daten erfolgen muss, werden die Informationen am besten in der elektronischen Einladung per E-Mail oder Messenger, in speziellen Datenschutzinformationen zum eingesetzten Videokonferenz-Tool erteilt. Im Wesentlichen müssen die Datenschutzinformationen die Art, die Zwecke und den Umfang der Verarbeitung der personenbezogenen Daten transparent darstellen. Hierzu zählen auch Angaben zur Person des Verantwortlichen sowie Speicher- bzw. Löschfristen und Betroffenenrechte.

c) Datenschutzrechtliche Absicherung des Verhältnisses zum Anbieter des Videokonferenz-Tools

Als Auftragsverarbeiter sind Dienstleister anzusehen, die weisungsgebunden im Rahmen des Auftragsverhältnisses personenbezogene Daten verarbeiten. Auch wenn für die Anbieter kein primär eigenes Interesse an der Verwendung der Daten besteht, haben sie doch i. d. R. technisch die Möglichkeit, auf Daten Zugriff zu nehmen. Die Beteiligten müssen daher nach Maßgabe des Art. 28 DS-GVO einen Auftragsverarbeitungsvertrag (AVV) abschließen. Dieser muss insbesondere die Dauer, Art der personenbezogenen Daten, Art und Zwecke der Verarbeitung sowie die Rechte und Pflichten der Verantwortlichen zum Inhalt haben.

Zu den Pflichten zählt nach Art. 28 Abs. 3 lit. c DS-GVO vor allem die Sicherheit der Verarbeitung gem. Art. 32 DS-GVO. Nach Art. 32 Abs. 1 lit. a DS-GVO sind von den Plattformanbietern technische Maßnahmen zum Schutz der Da-

ten zu ergreifen. Dabei muss sich der Verantwortliche, der auf den angebotenen Dienst des Plattformanbieters angewiesen ist, auf die getroffenen technischen und organisatorischen Maßnahmen (TOMs) verlassen, das entsprechende Schutzniveau aber bei der Auswahl des geeigneten Anbieters im Vorfeld überprüfen. Die TOMs müssen zwar den aktuellen Stand der Technik berücksichtigen, doch sind darüber hinaus Einzelfallprüfungen u. a. in Bezug auf die Implementierungskosten, Art und Umfang sowie Umstände und Zwecke der Verarbeitung im Verhältnis zu dem bestehenden Risiko für die zu schützenden Daten zu beachten.

2. Aktuelle Entwicklungen

Im Zusammenhang mit den dargestellten datenschutzrechtlichen Aspekten lohnt es sich, einen Blick auf die Sicht der Aufsichtsbehörden und die damit einhergehenden aktuellen Entwicklungen zu werfen.

a) Aufsichtsbehörden

Die Aufsichtsbehörden der Länder verfolgen zum Thema Videokonferenz-Tools interessanterweise keine einheitliche Linie. Dies mag auch (aber nicht nur) dem föderalen Prinzip der datenschutzrechtlichen Regulierung in Deutschland – Datenschutz für nicht öffentliche Stellen ist Ländersache – geschuldet sein.

Im Norden und in Nordrhein-Westfalen stehen die Aufsichtsbehörden für den Datenschutz dem Einsatz von Videokonferenz-Tools sehr kritisch gegenüber. Die Berliner Datenschutzbehörde empfiehlt, nach Möglichkeit gänzlich auf Videokonferenz-Tools zu verzichten und auf die altbekannte Telefonanlage zurückzugreifen, da diese datenschutzrechtlich einfacher zu behandeln sei. Diese Aussage ist einigermaßen erstaunlich und zeugt nicht gerade von einem ausgeprägten technischen Sachverstand. Sollte ein Verzicht nicht möglich sein, solle für Videokonferenzen am besten die On-Premise-Variante (das Hosting auf eigenen Servern) gewählt werden. Sollte dies aufgrund des enormen technischen Aufwands ebenfalls keine Option sein, sollten nur Anbieter genutzt werden, die über eine hinreichende Verschlüsselung verfügen. Dieser Ansicht folgt auch die Datenschutzbehörde des Landes Nordrhein-Westfalen. Auf welche Art von Verschlüsselung, z. B. Transport- oder Inhaltsverschlüsselung, in einem solchen Fall zurückgegriffen werden sollte, wird allerdings nicht näher erläutert.

Ferner würden aus Sicherheitsgründen, so die Datenschutzbehörden in Berlin und NRW, bestenfalls Anbieter mit Sitz in der EU oder einem Land der EFTA (Europäische Freihandelsassoziation) gewählt. Allerdings akzeptieren die Aufsichtsbehörden neben Anbietern aus den oben genannten Ländern ausdrücklich auch solche aus Drittstaaten, wenn sie ein gleichwertiges Datenschutzniveau aufweisen. Neben durch die EU-Kommission ausgewählten Staaten sei nach wie vor das EU-US Privacy-Shield eine wichtige Grundlage für die Datenübermittlung in die USA und genüge bis dato den gesetzlichen Anforderungen.

Nach einer Prüfung auf Vertrauenswürdigkeit, Verschlüsselungsart und ausreichende Datensicherheit (z. B. durch Zertifizierungen) sei das Schließen eines AVV notwendig, sodass der Betreiber keine Angaben über die Beschäftigten und deren Kommunikation oder die Nutzung der Software für eigene Zwecke verarbeiten könne. Hierzu empfehlen die Behörden die Standardvertragsklauseln der EU-Kommission zu nutzen.

MERKE | Ob das EU-US Privacy-Shield gekippt wird und ob die Standardvertragsklauseln der EU in dieser Form bestehen bleiben, liegt derzeit dem EuGH als Vorabentscheidungsersuchen vor. Die Urteilsverkündung ist für den 16.7.20 geplant.

Dass auf der anderen Seite ggf. überhaupt keine Pflicht zum Abschluss eines AVV bestehen könnte, da aufgrund der Verschlüsselung ein Zugriff für den Videodienstanbieter auf die Daten unmöglich sein könnte, wurde nicht in Betracht gezogen.

Besonders risikoreich sei der Mitschnitt von Konferenzen, unabhängig davon, ob dieser durch Dritte oder die Konferenzteilnehmer selbst geschehe. Insbesondere bei außereuropäischen Dienstleistern sei hierbei ein erhöhtes Risiko zu verzeichnen. Ob Hintergrund des Misstrauens die Art der Verschlüsselung oder das unterschiedliche Datenschutzniveau ist, lässt sich den Papieren der Aufsichtsbehörden nicht entnehmen.

In Schleswig-Holstein dagegen ist das ULD (Unabhängiges Landeszentrum für Datenschutz) etwas liberaler. Dies ist erfreulich und zeugt von größerem technischen Sachverstand und dogmatischer Fundiertheit. Der Einsatz von Videokonferenz-Tools wird qualifizierter geprüft und nicht von vornherein „verteufelt". Besonderen Wert legt das ULD auf die Nutzung datenschutzrechtlicher Voreinstellungen vor dem Einsatz von Videokonferenz-Tools. Insbesondere solle das sog. Aufmerksamkeitstracking vermieden werden. Die Funktion soll es ermöglichen, zu erkennen, ob Teilnehmer der Videokonferenz folgen oder nicht. Überdies solle insbesondere auf den zur Verfügung gestellten Passwortschutz zurückgegriffen werden, um Unbefugten die Teilnahme an der Konferenz zu erschweren. Eine grundsätzliche datenschutzrechtliche Unzulässigkeit von Videokonferenz-Tools wird aber nicht geäußert.

b) Marktakteure

Nachdem die Berliner Datenschutzbehörde die „Checkliste für die Durchführung von Videokonferenzen während der Kontaktbeschränkungen" veröffentlicht und vor dem Einsatz von Zoom, Microsoft Teams und Skype gewarnt hatte, setzte sich Microsoft mittels einer Abmahnung zur Wehr – ein erfreuliches Novum, die Aufsichtsbehörde direkt anzugreifen, deren Äußerungen durchaus wettbewerbsrechtliche Bedenken aufgeworfen haben. In dem Schreiben von Anfang Mai soll Microsoft die Behörde

1. zum Entfernen der Checkliste aufgefordert sowie
2. gefordert haben, dass der Inhalt zurückgenommen wird.

Wie t-online.de berichtete, enthielt das Schreiben keine finanziellen Forderungen und wurde nun von der Berliner Behörde geprüft.

Die Geschäftsleitung von Microsoft Deutschland warf der Datenschutzbehörde vor, dass mehrere Annahmen „faktisch oder rechtlich unzutreffend" seien. Die Checkliste deute an, dass Microsoft mit seinen Produkten nicht nur gegen die DS-GVO verstoße, sondern auch, dass „Videokonferenzen das Risiko bergen, unbefugt, auch im Auftrag von Dritten, mitgehört und aufgezeichnet zu werden", was strafrechtliche Bedenken gegenüber Microsoft suggeriere. Ferner sei das Unternehmen vor Veröffentlichung nicht zu dem Thema angehört worden.

Die Berliner Landesdatenschutzbeauftragte und Verfasserin der Checkliste hat ihre Aussage bisher nicht zurückgenommen. Die Sachlage sei ausführlich geprüft worden und die Checkliste wurde mit „einigen geringfügigen Konkretisierungen an den Texten" wieder verfügbar gemacht. Diese enthält aber immer noch die Aussage, dass (u. a.) Microsoft nicht den genannten Vorstellungen entspreche.

FAZIT | Videokonferenz-Tools für per se datenschutzwidrig zu erklären, erscheint übertrieben und bei genauerer datenschutzrechtlicher Analyse auch unzutreffend. Durch den Rückgriff auf datenschutzrechtliche „Bordmittel" ist der Einsatz von Zoom & Co. „DS-GVO-konform" möglich. Hierzu zählen insbesondere der Abschluss eines AVV mit dem Anbieter des Videokonferenz-Tools der eigenen Wahl sowie das Einhalten von Informationspflichten gegenüber den Konferenzteilnehmern. Die jeweiligen Informationspflichten sollten am besten in die eigene Datenschutzerklärung mit aufgenommen und als Link oder PDF mit der Einladung zum Meeting an die Teilnehmer versendet werden.

Ferner können einige Bedenken auf dem Gebiet des Datenschutzes vom jeweiligen Konferenzveranstalter selbstständig in den Einstellungen der Toolanbieter angepasst und jederzeit geändert werden (Privacy by Default). Hierzu gehört bei Zoom mittlerweile sogar die Wahl des Serverstandorts, weshalb eine Datenübermittlung ins Ausland nun nicht mehr unbedingt notwendig sein dürfte.

Dass sich Marktakteure gegen eher fragliche Behördenpositionierungen zur Wehr setzen, zeigt: Aufsichtsbehörden sind bezüglich ihrer Äußerungen und Empfehlungen von der Rechtsordnung nicht unantastbar. Amtshaftungsansprüche erscheinen in solchen Fällen ebenfalls prüfenswert.