Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder

Orientierungshilfe Videokonferenzsysteme

Stand 23.10.2020

Inhalt

1 Einleitung

In Situationen wie der Corona-Krise können Videokonferenzdienste eine zentrale Bedeutung für unsere Kommunikation erlangen. Mit diesen Diensten kann neben Videoanrufen auch eine Gruppenkommunikation ermöglicht werden. Die vorliegende Orientierungshilfe erläutert datenschutzrechtliche Anforderungen an die Durchführung von Videokonferenzen durch Unternehmen, Behörden und andere Organisationen.

Im Rahmen von Videokonferenzen werden personenbezogene Daten der teilnehmenden Personen verarbeitet. Aufgrund der schon hohen und noch wachsenden Funktionsvielfalt heutiger Videokonferenzlösungen und der Vielzahl weiterer IT-Dienste, die als sogenannte Umsysteme an die Videokonferenzsysteme angebunden sind, ist die Bandbreite der zu berücksichtigenden personenbezogenen Daten groß.

Betroffen sind inhaltliche Äußerungen und die Übertragung von Ton und Bild der teilnehmenden Personen und ggf. ihres Umfeldes, wie etwa ihrer Wohnung, ihres Arbeitsplatzes oder sonstigen Aufenthaltsorts (Inhaltsdaten). Bild und Ton der Teilnehmenden enthalten auch genügend Information, um diese anhand ihrer Stimme oder ihrer Gesichtsmerkmale identifizieren zu können. Je nach Art des Dienstes sind aber daneben auch Äußerungen in Form von grafischen oder textlichen Chatnachrichten oder die Anzeige des eigenen Bildschirms für einzelne oder alle Teilnehmer möglich; die Zuordnung dieser Nachrichten oder Anzeigevorgänge zu den teilnehmenden Personen, die sie geäußert, präsentiert oder rezipiert haben, ist als personenbezogen zu betrachten.

Weiterhin können Metadaten über die Durchführung der Kommunikation, Daten über die beruflichen Kontakte, über Arbeitszeiten und über die Arbeitsleistung anhand der Daten einer oder mehrerer Videokonferenzen verarbeitet werden (Rahmendaten).

Ferner können personenbezogene Daten in Text-Beiträgen der teilnehmenden Personen und den im Rahmen von Videokonferenzen erörterten und sichtbar gemachten Dokumenten enthalten sein. Diese Daten können sich auf die Konferenzteilnehmenden selbst, aber auch auf nicht teilnehmende Personen innerhalb und außerhalb der Institutionen beziehen.

Zudem können auch personenbezogene Daten von Personen aus dem Umfeld der teilnehmenden Personen betroffen sein, deren Bild oder Ton unter Umständen von dem Konferenzsystem mitverarbeitet wird. Beispiel: eine Person aus dem Haushalt des Konferenzteilnehmers läuft durch das Bild oder spricht im Hintergrund.

Der für die Durchführung der Videokonferenz Verantwortliche ist verpflichtet zu prüfen, inwieweit er zur Verarbeitung befugt ist. Dabei hat er insbesondere den Grundsatz der Datensparsamkeit zu beachten. Deshalb muss er prüfen, inwieweit die mit dem konkreten Einsatz des Konferenzsystems verbundene Datenverarbeitung durch die Auswahl der eingesetzten Systeme sowie durch technische und organisatorische Maßnahmen auf das zur Zweckerreichung Erforderliche begrenzt werden kann. Soweit er Tools eines Anbieters verwendet, muss er die datenschutzrechtliche Beziehung zu diesem klären. Er hat auch dann darauf zu achten, dass die zum Schutz der jeweiligen Daten erforderlichen technischen und organisatorischen Maßnahmen ergriffen werden. Ferner hat er über die Datenverarbeitung in der gebotenen Form zu informieren. Diese Handreichung soll den Verantwortlichen hierzu eine Hilfestellung bieten.

2 Betriebsmodelle

Der Verantwortliche hat grundsätzlich drei Möglichkeiten ein Videokonferenzsystem zu betreiben: Entweder nutzt er einen Online-Dienst (Software as a Service), betreibt das System selbst oder lässt das System bei einem externen IT-Dienstleister betreiben.

2.1 Selbst betriebener Dienst

Eine Institution (Unternehmen, Behörde o. ä.), die einen Videokonferenzdienst selbst betreiben will, kann sich hierfür freier (Open Source) oder anderer Software bedienen und hat damit selbst in der Hand, welche Software zum Einsatz kommt und zu welchen Datenverarbeitungen dies führt.

Die Software selbst zu betreiben hat den Vorteil, dass sich Fragen nach der Notwendigkeit des Abschlusses eines Auftragsverarbeitungsvertrags (Art. 28 DS-GVO)[1] oder einer Vereinbarung zur gemeinsamen Verantwortung (Art. 26 DS-GVO)[2] ebenso wenig stellen, wie die nach einer evtl. gemeinsamen Haftung.

Zugleich wird auf diese Weise sichergestellt, dass Daten genauso verarbeitet werden, wie gewünscht. Der Betrieb von Videokonferenzsystemen auf einer selbst betriebenen Infrastruktur hat den Vorteil, dass nur dem Verantwortlichen eine Analyse und Kontrolle der Inhalts- und Rahmendaten der Systeme ermöglicht wird, da nur er auf die hierfür erforderlichen Daten zugreifen kann.

---

1 https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_13.pdf
2 https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_16.pdf

Verantwortliche müssen dann freilich für Betrieb und Wartung über ausreichende technische und personelle Kapazitäten verfügen und geeignete technische und organisatorische Maßnahmen zum Schutz der Daten ergreifen. Das ist von großen und leistungsfähigen Institutionen zu erwarten, kann bei kleineren Verantwortlichen aber eine personelle und technische Herausforderung darstellen.

Daher kommt auch eine Beauftragung von Dienstleistern in Betracht.

2.2 Betrieb durch einen externen IT-Dienstleister

Wer eine Software präferiert, sie aber nicht selbst betreiben kann, kann hierfür einen Dienstleister beauftragen. Bleibt die Datenverarbeitung beim Dienstleister auf die Erfüllung dieses Auftrags beschränkt, so liegt Auftragsverarbeitung vor. Hierfür ist ein Vertrag zur Auftragsverarbeitung nach Art. 28 Abs. 3 DS-GVO abzuschließen.

Die Datenschutz-Aufsichtsbehörden empfehlen insbesondere der öffentlichen Verwaltung, derartige Systeme selbst zu betreiben oder zentral (landesweit bzw. bundesweit) einen oder mehrere Videokonferenzdienste bereitzustellen. Durch die jeweiligen von den Ländern bzw. vom Bund verpflichteten Dienstleister können Systeme ggf. auf die Bedürfnisse der jeweiligen Sektoren und Einsatzzwecke, insbesondere des Schulsystems angepasst werden.

Dabei ist zu beachten, dass die eingesetzte oder Teilnehmern angebotene Software auf Datenabflüsse an den Hersteller und dritte Stellen zu untersuchen ist. Dies schließt Diagnose- und Telemetriedaten oder sonstige Datenabflüsse ein.

Entsprechende Datenabflüsse müssen unterbunden werden, soweit nicht eine Rechtsgrundlage hierfür besteht.

2.3 Online-Dienst

Anstatt das Videokonferenzsystem selbst zu betreiben oder von einem Dienstleister nach eigenen Vorstellungen betreiben zu lassen, gibt es auch die Möglichkeit, bestehende Online-Dienste zu verwenden.

Für die Entscheidung für einen Online-Dienst spricht zunächst die einfache Bereitstellung des angebotenen Videokonferenzsystems. Der Verantwortliche schließt in diesem Fall einen Vertrag mit dem Anbieter. In Abhängigkeit von der konkreten Ausgestaltung des Online-Dienstes sind im Anschluss zentrale Konfigurationsoptionen (z. B. Datenabflüsse, Zugriffsrechte) zu prüfen und ggf. anzupassen. Danach melden bei Bedarf die dafür autorisierten Personen eine

Videokonferenz beim Anbieter an und laden die teilnehmenden Personen ein. Der Verantwortliche muss zumindest einen Auftragsverarbeitungsvertrag schließen (siehe Abschnitt 3.5.2).

Der Verantwortliche muss die Einhaltung der Datenschutzgrundsätze durch Auswahl eines geeigneten Anbieters sicherstellen (vgl. hierzu die Anforderungen des Art. 28 Abs. 1 DS-GVO) sowie entsprechende Anweisungen an den Diensteanbieter erteilen und eigene Vorkehrungen treffen.

Dazu hat der Verantwortliche die vom Auftragsverarbeiter vorgelegten Auftragsverarbeitungsverträge, Nutzungsbedingungen und Sicherheitsnachweise und auch dessen Datenschutzerklärung zu prüfen.

Ganz grundsätzlich ist bei der Auswahlentscheidung für einen Anbieter darauf zu achten, dass dieser geeignete technische und organisatorische Maßnahmen ergreift, dass die Verarbeitung im Einklang mit den Anforderungen der DS-GVO erfolgt und der Anbieter hierfür hinreichende Garantien bietet. Die größten und bekanntesten Anbieter von Videokonferenzprodukten haben ihren Firmensitz allerdings in den USA und verarbeiten dort die Daten. Bei Datenübermittlungen in die USA oder andere Drittstaaten sind die Anforderungen des Kapitels V der DS-GVO einzuhalten (siehe den folgenden Absatz sowie Abschnitt 3.5.6). Bei der Verwendung von Standardvertragsklauseln als Instrument zur Rechtfertigung des Datenexports ist unter anderem zu beachten, dass der Verantwortliche vor Beginn der Übermittlung die Rechtslage im Drittland im Hinblick auf behördliche Zugriffe und Rechtsschutzmöglichkeiten für betroffene Personen analysieren muss. Bei Defiziten sind zusätzliche Maßnahmen erforderlich; ggf. muss der Datenexport unterbleiben.

Durch das Urteil des EuGH in der Rechtssache Schrems II vom 16.07.2020 (C-311/18) wurde der Angemessenheitsbeschluss zum EU-U.S. Privacy Shield für ungültig erklärt. Das Privacy Shield steht daher als Instrument für die Sicherstellung eines angemessenen Schutzes in die USA übermittelter Daten nicht mehr zur Verfügung. Bei der Verwendung von Standardvertragsklauseln und anderen vertraglichen Garantien als Grundlage für Übermittlungen personenbezogener Daten in die USA sind nach der Entscheidung des EuGH zusätzliche Maßnahmen zu ergreifen, die sicherstellen, dass für diese Daten auch bei und nach ihrer Übermittlung ein im Wesentlichen gleichwertiges Schutzniveau wie das in der EU gewährleistet wird. Es bedarf noch weiterer Analysen, um im Lichte dieser vom EuGH klargestellten Anforderungen konkretere Aussagen dahingehend treffen zu können, ob und unter welchen zusätzlichen Schutzvorkehrungen personenbezogene Daten in die USA oder an US-Anbieter übermittelt werden können. Aus diesem Grund empfiehlt die DSK derzeit die Nutzung von Videokonferenzprodukten

US-amerikanischer Anbieter sorgfältig zu prüfen. Dies gilt auch, wenn Vertragspartner eine europäische Tochtergesellschaft ist. Das gleiche gilt für europäische Anbieter, sofern sie ihrerseits personenbezogene Daten in die USA übermitteln.

3 Rechtliche Anforderungen

Vor dem Betrieb oder der Nutzung eines Videokonferenzdienstes sind die Rollen und Verantwortlichkeiten der Beteiligten klar zu verteilen und eindeutig festzulegen, um die Einhaltung der Regelungen der DS-GVO zu gewährleisten (siehe dazu auch Abschnitt 4.4). Verantwortlicher ist nach Art. 4 Nr. 7 DS-GVO diejenige Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung entscheidet. Verantwortlichkeit ist nicht gleichbedeutend mit dem Bestehen einer Befugnis zur Datenverarbeitung. Das Konzept der Verantwortlichkeit stellt nur klar, dass die Stelle, die gemäß Art. 4 Nr. 7 DS-GVO über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet, die aus der DS-GVO resultierenden datenschutzrechtlichen Verpflichtungen des Verantwortlichen zu erfüllen hat.

3.1 Selbst betriebener Dienst

Betreiben z. B. ein Arbeitgeber oder eine Schule ein Videokonferenzsystem, sind der Arbeitgeber oder die Schule als Veranstalter der Videokonferenz Verantwortliche im Sinne der DS-GVO, da er oder sie im Rahmen des Einsatzes dieses Systems über die Zwecke und Mittel der Verarbeitung bestimmen. Das gilt insbesondere für Daten, die unmittelbar im Rahmen der Nutzung des Videokonferenzsystems ausgetauscht werden (Inhaltsdaten, z. B. zentral auf dem Server gespeicherte Chats, geteilte Dokumente, Aufzeichnungen der Konferenz), aber auch für Rahmendaten, insbesondere Metadaten, die zur Aufrechterhaltung des Systems erforderlich sind.

3.2 Betrieb durch einen externen IT-Dienstleister

Der Betreiber des Videokonferenzsystems kann als Auftragsverarbeiter im Auftrag des Verantwortlichen personenbezogene Daten verarbeiten. Bedient sich der Verantwortliche etwa eines Dienstleisters, der die technische Infrastruktur stellt und kein eigenes Interesse an den personenbezogenen Daten hat, ist mit diesem ein wirksamer Vertrag zur Auftragsverarbeitung nach Art. 28 DS-GVO abzuschließen (siehe Abschnitt 3.5.2). Bei der Auswahl des Auftragsverarbeiters ist darauf zu achten, dass dieser hinreichende Garantien zu den erforderlichen technischen und organisatorischen Maßnahmen bietet. Da die entsprechenden Verträge in der Praxis häufig auf Musterverträgen der Dienstleister beruhen, sollte besonders darauf geachtet werden,

dass die Weisungsgebundenheit des Auftragsverarbeiters umfassend geregelt wird und dass dem Verantwortlichen hinreichende Kontrollbefugnisse eingeräumt werden.

3.3 Online-Dienst

Verarbeitet der Anbieter des eingesetzten Dienstes personenbezogene Daten der Teilnehmer auch zu eigenen Zwecken oder Zwecken Dritter (z. B. Verarbeitung von Daten zum Nutzerverhalten, Einsatz von Analysetools, Tracking zu Werbezwecken), so ist zu beachten, dass der Veranstalter für jede Offenlegung personenbezogener Daten an den Anbieter ebenso eine Rechtsgrundlage benötigt wie der Anbieter für jede Verarbeitung personenbezogener Daten in eigener – ggf. gemeinsamer – Verantwortlichkeit. Dies trifft häufig auf Online-Dienste zu.

Eine Rechtsgrundlage für die Offenlegung personenbezogener Daten an den Anbieter des Dienstes ist allerdings regelmäßig schwierig zu begründen (siehe dazu Abschnitt 3.4.6).

Verarbeitet der Anbieter personenbezogene Daten, die im Rahmen der Nutzung des Videokonferenzdienstes anfallen, auch zu eigenen Zwecken oder zu Zwecken Dritter, ist eine gemeinsame Verantwortlichkeit nach Art. 26 DS-GVO zu prüfen. Liegt eine gemeinsame Verantwortlichkeit vor, muss insbesondere eine entsprechende Vereinbarung geschlossen werden. Diese Vereinbarung ersetzt nicht die Rechtsgrundlage, die jeder der gemeinsam Verantwortlichen benötigt, sondern stellt eine zusätzliche Anforderung dar.

Gegenüber den betroffenen Personen muss stets transparent gemacht werden, wer in welcher Rolle welche personenbezogenen Daten verarbeitet. Der Veranstalter muss als Verantwortlicher mit Nennung der Kontaktdaten und ggf. des Datenschutzbeauftragten und seiner Kontaktdaten klar aus der Information über die Datenverarbeitung hervorgehen. Das gilt auch für den ggf. gemeinsam verantwortlichen Anbieter des Dienstes, wobei auch klar darüber informiert werden muss, welche Daten in gemeinsamer Verantwortlichkeit verarbeitet werden. Ist der Anbieter hingegen Auftragsverarbeiter, muss er nur bei den Empfängern der Daten genannt werden, nicht jedoch als Verantwortlicher.

3.4 Rechtsgrundlage für den Verantwortlichen und Zweckbindung

Zur rechtmäßigen Verarbeitung der personenbezogenen Daten der an der Konferenz teilnehmenden Personen benötigt der Verantwortliche eine Rechtsgrundlage gemäß Art. 6 DS-GVO.

3.4.1 Zur Struktur der Rechtsgrundlagen

Je nach Kontext der Verarbeitungssituation kann sich eine Befugnisnorm aus Art. 6 Abs. 1 lit. a, b, e, f DS-GVO, gegebenenfalls auch in Verbindung mit dem nationalen Recht, ergeben. So kann die Datenverarbeitung auf eine wirksame, d. h. freiwillige und informierte Einwilligung gestützt werden. Außerdem kommt Art. 6 Abs. 1 lit. b DS-GVO (Vertragserfüllung) als Rechtsgrundlage in Betracht. Bestehen im Rahmen der Vertragserfüllung grundsätzlich Alternativen zur Videokonferenz oder nehmen Beschäftigte anderer Unternehmen und sonstige Personen an einer Videokonferenz teil, können auch berechtigte Interessen nach Art. 6 Abs. 1 lit. f DS-GVO die Datenverarbeitung legitimieren, wobei zu beachten ist, dass der Verantwortliche in diesem Falle gemäß Art. 21 Abs. 4 DS-GVO auf das Widerspruchsrecht hinweisen muss.

Allerdings können sich Behörden bei der Erfüllung ihrer Aufgaben nicht auf Art. 6 Abs. 1 lit. f DS-GVO berufen (Art. 6 Abs. 1 Satz 2 DS-GVO). Im Falle von Behörden kommt jedoch als Rechtsgrundlage grundsätzlich Art. 6 Abs. 1 lit. e DS-GVO in Verbindung mit der jeweils einschlägigen Norm des deutschen Rechts, etwa aus dem Schulrecht, in Betracht.

3.4.2 Einwilligung

Sofern als Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten Einwilligungen der betroffenen Personen verwendet werden sollen, ist auf Folgendes hinzuweisen:

Eine Einwilligung ist nur wirksam, wenn sie in informierter Weise und freiwillig abgegeben wurde (vgl. Art. 4 Nr. 11 DS-GVO). Von einer Freiwilligkeit ist nur auszugehen, wenn eine echte Wahlmöglichkeit hinsichtlich der Teilnahme an der Videokonferenz besteht.

Gerade im beruflichen oder im schulischen Kontext ist die Freiwilligkeit oftmals zweifelhaft, insbesondere dann, wenn Informationen, die für die Durchführung der beruflichen Tätigkeit oder für den Schulunterricht unverzichtbar sind, ausschließlich im Rahmen einer Videokonferenz mitgeteilt werden. Dann wird regelmäßig die Freiwilligkeit der Teilnahme an der Videokonferenz nicht gegeben sein, sodass die Einwilligung der betroffenen Personen als Rechtsgrundlage ausscheidet. In solchen Fällen kommt eine wirksame Einwilligung nur in Betracht, wenn die Freiwilligkeit durch zusätzliche Maßnahmen sichergestellt wird, etwa indem denjenigen, die nicht an Videokonferenzen teilnehmen wollen, das relevante Wissen in gleichwertiger Form auch auf anderem Wege bereitgestellt wird bzw. andere Wege der Kommunikation angeboten werden (z. B. eine Teilnahme an der Konferenz per Telefon).

Sofern die Freiwilligkeit nicht durch solche Maßnahmen sichergestellt werden kann, kann der Einsatz der Videokonferenz nicht auf Einwilligungen als Rechtsgrundlage gestützt werden, so

dass der Verantwortliche prüfen muss, ob er den Einsatz auf eine andere Rechtsgrundlage stützen kann (siehe Ziff. 3.4.1).

3.4.3 Arbeitgeber als Verantwortliche

Ist der datenschutzrechtlich Verantwortliche zugleich auch Arbeitgeber, der seine Beschäftigten zur Nutzung des Videokonferenzsystems zum Zweck der Erfüllung ihrer arbeitsvertraglichen Aufgaben veranlasst, kommt als Rechtsgrundlage für die Datenverarbeitung § 26 Abs. 1 Satz 1 BDSG oder die entsprechende landesrechtliche Vorschrift im öffentlichen Bereich in Betracht. Dabei ist allerdings stets die Erforderlichkeit der Übertragung auch von Bilddaten zu prüfen.

Im Beschäftigungskontext besteht die Möglichkeit, die Verarbeitung von Beschäftigtendaten spezifischer durch Kollektivvereinbarungen zu regeln. Betriebs- und Dienstvereinbarungen können insbesondere genutzt werden, um die allgemeinen Rechtsvorschriften in bestimmten Anwendungsfällen zu konkretisieren, also ob und wie Videokonferenzen durchgeführt werden. Dabei darf allerdings das Schutzniveau der DS-GVO nicht unterschritten werden.

3.4.4 Verarbeitung besonderer Kategorien personenbezogener Daten

Sofern besondere Kategorien personenbezogener Daten, wie Gesundheitsdaten, in der Videokonferenz thematisiert werden, muss diese Datenverarbeitung auch nach Art. 9 Abs. 2 DS-GVO, ggf. in Verbindung mit einem nationalen Gesetz, zulässig sein. Ähnliches gilt, wenn schon der Anlass der Videokonferenz Bezug zu Daten im Sinne des Art. 9 DS-GVO hat, etwa im Religionsunterricht oder Theologiestudium.

Soweit bei der Videokonferenz besondere Kategorien personenbezogener Daten verarbeitet werden, kann nach Art. 9 Abs. 2 lit. a DS-GVO eine ausdrückliche gesonderte Einwilligung erforderlich sein. Wirksam ist sie indes nur, wenn es sich um eine ausdrücklich, informiert, freiwillig, vorherig, aktiv, für den konkreten Einzelfall und separat erklärte sowie jederzeit zumutbar widerrufliche Einwilligung handelt.

3.4.5 Teilnahme aus Privatwohnungen

Soweit die Beschäftigten aus ihrem Home-Office teilnehmen, stellt sich das Problem, dass andere Teilnehmende ohne Einwilligung der Beschäftigten keine Einblicke in deren Privatsphäre durch Bild oder Ton erhalten dürfen. Der Arbeitgeber muss daher mit technischen und organisatorischen Maßnahmen (Art. 25 Abs. 1 DS-GVO) sicherstellen, dass derartige Einblicke nicht möglich sind, etwa durch Ausrichtung der Kamera oder Bereitstellung eines Paravents oder –

soweit vom Anbieter des Videokonferenzsystems angeboten – durch Einblendung eines virtuellen Hintergrunds. Alternativ zu solchen technischen und organisatorischen Maßnahmen ist eine Einwilligung der Beschäftigten (§ 26 Abs. 2 BDSG) denkbar, wobei hier insbesondere die Freiwilligkeit der Einwilligung sichergestellt sein muss.

Verantwortliche sollten ihre Mitarbeiter und andere Teilnehmer von Videokonferenzen, die aus Privatwohnungen heraus teilnehmen (können), über die diesbezüglichen Risiken informieren. Unvorteilhafte Kameraausrichtung, Mitnahme der Geräte in ungeeignete oder von Dritten belegte Räume, das unvorbereitete optische und/oder akustische Erscheinen Dritter in der Videokonferenz und ähnliche „Pannen" sind zu vermeiden.

3.4.6 Verarbeitungen durch Anbieter zu eigenen Zwecken

Sollte ein Anbieter personenbezogene Daten zu eigenen Zwecken verarbeiten, so kann er sich hierfür nicht auf die Rechtsgrundlage berufen, auf die der Veranstalter die Verarbeitung stützt, sondern benötigt selbst – als Verantwortlicher im datenschutzrechtlichen Sinne (Art. 4 Nr. 7 DS-GVO) eine Rechtsgrundlage. So regelt z. B. § 26 BDSG nur die Verarbeitung personenbezogener Daten durch Arbeitgeber, nicht aber die Datenverarbeitung durch den Anbieter zu eigenen Zwecken. Gleiches gilt für die Regelungen aus den Schulgesetzen der Länder. Die Offenlegung personenbezogener Daten an den Anbieter des Dienstes zu dessen eigenen Zwecken ist mit einer Änderung des Verarbeitungszwecks verbunden. Eine solche Zweckänderung ist nur in den engen Grenzen von Art. 5 Abs. 1 lit. b, Art. 6 Abs. 4 DS-GVO zulässig. Eine Vereinbarkeit der Zwecke im Sinne dieser Anforderungen wird dabei regelmäßig nicht vorliegen. Zudem muss auch die Offenlegung an den Anbieter auf eine Rechtsgrundlage gestützt werden können.

Gegenüber einem Auftragsverarbeiter ist im Auftragsverarbeitungsvertrag sicherzustellen, dass dieser die personenbezogenen Daten der teilnehmenden Personen nur auf Weisung des Verantwortlichen und nicht für eigene Zwecke verarbeitet.

3.4.7 Verarbeitung von Daten Dritter

Wenn personenbezogene Daten Dritter, die nicht an der Videokonferenz teilnehmen, erörtert und somit auch im Rahmen der Konferenz verarbeitet werden, sind hierfür die allgemeinen Rechtsgrundlagen heranzuziehen.

3.4.8 Transparenz, Aufzeichnungen von Videokonferenzen

Weiterhin müssen Art und Zweck der Verarbeitung der personenbezogenen Daten klar definiert sein, um den Transparenzanforderungen zu entsprechen. Die Verarbeitung ist grundsätzlich auf den Zweck der Videokonferenz zu beschränken, da weitergehende Verarbeitungen und Auswertungen der Konferenzdaten in der Regel nicht erforderlich sind. Dies gilt insbesondere für Aufzeichnungen. Für diese ist die Rechtsgrundlage gesondert zu prüfen. Ausnahmen sind für offene Veranstaltungen oder Publikumsseminare und öffentliche Vorträge denkbar, bei denen eine Aufzeichnung des Vortragenden im Einzelfall erforderlich sein kann. Gibt es kein besonderes Dokumentationserfordernis, ist daher regelmäßig eine (ggf. weitere, unabhängig von der Einwilligung in die mit der Teilnahme an der Videokonferenz verbundene Datenverarbeitung zu erteilende) Einwilligung in die Aufzeichnung und die weitere Verarbeitung erforderlich. Die Aufzeichnungsmöglichkeit ist bei der Erfüllung der Informationspflichten zu erwähnen (siehe auch Abschnitt 4.6).

Die Audio- und Videodaten sowie die Rahmendaten der Konferenz dürfen nur solange und soweit verarbeitet werden, wie es für die Übermittlung von Nachrichten durch einen Dienstleister oder im Rahmen einer notwendigen Dokumentation erforderlich ist. Eine über die Konferenz hinausgehende Speicherung ist regelmäßig weder erforderlich noch mit dem Erhebungszweck vereinbar, Art. 5 Abs. 1 lit. b, Art. 6 Abs. 4 DS-GVO. Dies bedeutet, dass eine etwa bestehende Aufzeichnungsfunktion in der Voreinstellung deaktiviert sein muss.

Die Nutzer sollten darüber belehrt werden, dass das (gerade auch heimliche) Mitschneiden von Video- und/oder Audiodaten, das Speichern und das Verbreiten solcher Aufnahmen strafbar sein kann.

3.5 Pflichten des Verantwortlichen

Beim Betrieb oder der Nutzung eines Videokonferenzdienstes hat der Verantwortliche als Veranstalter u. a. die nachfolgend genannten Pflichten nach der DS-GVO zu erfüllen.

3.5.1 Informationspflichten und Betroffenenrechte

Verantwortliche müssen den an der Konferenz teilnehmenden Personen klare und eindeutige Informationen über die mit der Nutzung des Dienstes verbundene Datenverarbeitung gem. Art. 13, 14 DS-GVO zur Verfügung stellen. Um die Transparenz der Verarbeitung sicherzustellen, müssen die Informationen so dargestellt werden, dass sie für einen durchschnittlichen Nutzer des Dienstes ohne übermäßigen Aufwand verständlich sind (Art. 12 und Art. 5 Abs. 1

lit. a DS-GVO). Übermäßig komplexe Formulierungen und technische oder juristische Fachbegriffe sollten vermieden werden. Soweit die Verwendung von Fachbegriffen unvermeidbar erscheint, müssen diese verständlich erläutert werden. Insbesondere bei umfangreichen Datenschutzerklärungen ist zudem darauf zu achten, dass die Übersichtlichkeit durch eine nachvollziehbare Gliederung und aussagekräftige Überschriften gewahrt bleibt, so dass es für die betroffenen Personen möglich ist, gezielt bestimmte Informationen (z. B. zur Aufzeichnung der Konferenzen oder zur Übermittlung von Daten an Dritte) herauszusuchen.

Zu den Informationspflichten nach Art. 13, 14 DS-GVO zählen insbesondere Informationen darüber, zu welchen Zwecken und auf welcher Rechtsgrundlage welche personenbezogenen Daten verarbeitet werden, ob der Anbieter des Videokonferenzdienstes bzw. der -software von diesen Kenntnis erlangen kann, ob und ggf. für welche Zeitdauer eine Speicherung personenbezogener Daten nach Abschluss einer Konferenzsitzung erfolgt und ob personenbezogene Daten in ein Drittland übermittelt werden sollen. Mit Blick auf die Transparenzpflichten des Verantwortlichen (Art. 5 Abs. 1 lit. a DS-GVO) sollten diese die teilnehmenden Personen auch darüber informieren, ob und wenn ja welche Art der Verschlüsselung[3] bei Betrieb des Systems zum Einsatz kommt. Diese Information ist von besonderer Bedeutung für die teilnehmenden Personen, die auf der Basis der Einwilligung an einer Videokonferenz teilnehmen.

Daneben muss der Verantwortliche die teilnehmenden Personen auch über die Rechtsgrundlagen der einzelnen Verarbeitungsvorgänge und – soweit er sich auf Art. 6 Abs. 1 lit. f DS-GVO beruft – über die verfolgten berechtigten Interessen informieren. Zudem muss in diesem Fall die teilnehmende Person gemäß Art. 21 Abs. 4 DS-GVO auf ihr Widerspruchsrecht hingewiesen werden. Kommen verschiedene Befugnisnormen zur Anwendung, sollte insbesondere deutlich werden, ob und wenn ja, welche Verarbeitungsvorgänge auf die Einwilligung der teilnehmenden Person gestützt werden. Denn nur wenn die teilnehmenden Personen sich ihrer Dispositionsbefugnis über die eigenen Daten bewusst sind, können sie diese auch ausüben (weiß z. B. ein Arbeitnehmer nicht, dass die Nutzung der Videofunktion im Rahmen von dienstlichen Besprechungen freiwillig ist, so entfaltet diese Freiwilligkeit für ihn keine Schutzwirkung). Aus Sicht des Verantwortlichen besteht bei einwilligungsbasierten Verarbeitungsvorgängen zudem das Risiko, dass eine unzureichende Information der teilnehmenden Personen zur Rechtswidrigkeit der Datenverarbeitung führt, da nur eine informierte Einwilligung die Datenverarbeitung rechtfertigen kann (vgl. Art. 4 Nr. 11 DS-GVO).

---

[3] Notwendig ist nicht die Angabe des kryptografischen Verfahrens, sondern inwieweit die Verschlüsselung geeignet ist, die verschlüsselten Daten gegenüber Dritten und gegenüber dem Betreiber des Dienstes geheim zu halten, und auf welche Daten sie sich erstreckt.

Verarbeitet der Anbieter des Dienstes – soweit das überhaupt zulässig ist (siehe Abschnitt 3.4.6) – Daten zu eigenen Zwecken, treffen die Informationspflichten grundsätzlich (auch) den Anbieter selbst. Der Veranstalter der Videokonferenz muss die teilnehmenden Personen im Rahmen des Art. 13 Abs. 3 DS-GVO grundsätzlich auch selbst über solche Verarbeitungsvorgänge informieren und kann nicht lediglich auf die Datenschutzbestimmungen des eingesetzten Dienstes verweisen. Zudem sollte der Veranstalter die teilnehmenden Personen darüber informieren, welche Möglichkeiten für sie bestehen, im Rahmen der Privatsphäre-Einstellungen des Dienstes selbst auf den Schutz ihrer personenbezogenen Daten hinzuwirken (z. B. durch Nutzung eines Pseudonyms, Einstellen eines künstlichen Hintergrunds). Dabei sollten die teilnehmenden Personen insbesondere auch darüber informiert werden, ob eine Aufzeichnung der Konferenz durch den Veranstalter möglich ist und wodurch die teilnehmenden Personen bei Aktivierung der Aufnahmefunktion auf die laufende Aufzeichnung hingewiesen werden.

Zudem sind die Betroffenenrechte aus Art. 15 bis 21 DS-GVO zu gewährleisten. Soweit der Veranstalter der Konferenz auch für Daten verantwortlich ist, die durch den Dienst erhoben werden, ggf. auch ohne dass der Veranstalter selbst auf diese zugreifen kann, sollte er bei der Auswahl des Dienstes darauf achten, inwieweit dieser es ermöglicht, sowohl Inhaltsdaten als auch Rahmendaten gezielt oder allgemein zu löschen. Die Löschung der Inhalts- und Rahmendaten der beendeten Konferenz hat auch unabhängig von einem Antrag der betroffenen Personen nach Art. 17 DS-GVO regelmäßig unverzüglich nach dem Abschluss der Videokonferenz zu erfolgen, da dann der Zweck der Verarbeitung der personenbezogenen Daten erreicht wurde und eine weitere Aufbewahrung der Daten nicht aufgrund einer rechtlichen Verpflichtung, der der Verantwortliche nach dem Unionsrecht oder dem Recht seines Mitgliedstaats unterliegt, erforderlich ist.

3.5.2 Auftragsverarbeitungsvertrag

Die DS-GVO bietet ein hohes Datenschutzniveau. Dieses darf nicht durch die Einschaltung von Dienstleistern gefährdet werden. Wird das Videokonferenzsystem durch den Anbieter betrieben oder hat dieser die Möglichkeit, auf personenbezogene Daten zuzugreifen, ist mit ihm ein Auftragsverarbeitungsvertrag abzuschließen. Eine solche Zugriffsmöglichkeit kann je nach eingesetzter Lösung auch bei durch den Verantwortlichen selbst betriebenen Systemen bestehen. Das Kurzpapier Nr. 13 der Datenschutzkonferenz (Auftragsverarbeitung)[4] ist zu beachten. Der Verantwortliche muss nach Art. 5 Abs. 2 DS-GVO jederzeit nachweisen können, dass er die Datenschutzgrundsätze einhält. Daher muss der Auftragsverarbeitungsvertrag ohne jeden Zweifel

[4] https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_13.pdf

sämtliche Anforderungen des Art. 28 DS-GVO abdecken. Unklarheiten im Auftragsverarbeitungsvertrag sind daher regelmäßig Ausschlusskriterium für die Nutzung des jeweiligen Anbieters.

3.5.3 Verarbeitungsverzeichnis

Die Veranstaltung der Videokonferenz(en) ist in das Verzeichnis der Verarbeitungstätigkeiten gemäß Art. 30 DS-GVO aufzunehmen. Das Kurzpapier Nr. 1 der Datenschutzkonferenz (Verzeichnis von Verarbeitungstätigkeiten)[5] ist zu beachten.

3.5.4 Meldepflicht bei Datenpannen

Der Verantwortliche hat im Fall einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit der Videokonferenz die Pflichten aus Art. 33 und 34 DS-GVO einzuhalten.

3.5.5 Datenschutz-Folgenabschätzung

Der Verantwortliche hat zu überprüfen, ob eine Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO durchzuführen ist. Dies kann insbesondere dann der Fall sein, wenn besondere Kategorien personenbezogener Daten der teilnehmenden Personen oder anderer Personen nach Art. 9 DS-GVO in der Videokonferenz umfangreich verarbeitet werden. Das Kurzpapier Nr. 5 der Datenschutzkonferenz (Datenschutz-Folgenabschätzung)[6] ist zu beachten.

3.5.6 Besonderheiten bei Übermittlungen an Drittländer

Die DS-GVO bietet ein hohes Datenschutzniveau. Die Verordnung gilt unter den in Art. 3 Abs. 2 DS-GVO geregelten Voraussetzungen auch für Anbieter von Videokonferenzsystemen, die außerhalb der EU niedergelassen sind. Anbieter aus Nicht-EU-Staaten unterliegen in aller Regel auch den Rechtsvorschriften ihres Heimatstaates und damit unter Umständen Zugriffsrechten von Behörden von Drittstaaten, die eine Einhaltung der datenschutzrechtlichen Anforderungen der DS-GVO erschweren oder zu letzteren im Einzelfall im Widerspruch stehen können.

Werden Videokonferenzsysteme ausgewählt, die zu Datenübermittlungen in Drittländer, also in Länder außerhalb der EU bzw. des Europäischen Wirtschaftsraums führen, muss die Übermittlung besondere Bedingungen einhalten (Kapitel V, Art. 44 ff. DS-GVO, siehe dazu auch Kurzpapier Nr. 4 der Datenschutzkonferenz[7]). Solche Übermittlungen kann es insbesondere bei

---

5 https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_1.pdf
6 https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_5.pdf
7 https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_4.pdf

Anbietern geben, die selbst im Drittland ihren Sitz haben oder Unterauftragnehmer aus Drittländern einsetzen. Eine Datenübermittlung in Drittländer liegt auch dann vor, wenn der Anbieter oder ein Unterauftragsverarbeiter aus dem Drittland heraus auf in der EU verarbeitete Daten zugreift (z. B. zu Wartungs- oder Supportzwecken).

Für manche Drittländer hat die EU-Kommission beschlossen, dass dort ein angemessenes Datenschutzniveau vorliegt. Dann sind für die Zulässigkeit des Datenexports keine weiteren Bedingungen zu erfüllen (Art. 45 DS-GVO).

Da mit dem Urteil C-311/18 der EuGH (Schrems II) der Beschluss der EU-Kommission zum sog. EU-U.S. Privacy Shield für ungültig erklärt wurde, steht dieser, wie unter 2.3 erläutert, als Mittel zur Sicherstellung eines angemessenen Schutzniveaus in den USA nicht mehr zur Verfügung.

Die Bedingungen aus Kapitel V der DS-GVO können sonst z. B. durch die Standardvertragsklauseln der EU-Kommission eingehalten werden, die der Verantwortliche mit dem Anbieter als Auftragsverarbeiter abschließt.

Allerdings wirkt sich das Urteil des EuGH zu Schrems II, wie bereits unter 2.3. erwähnt, auch auf die datenschutzkonforme Verwendungsmöglichkeit der anderen Instrumente zur Übermittlung im internationalen Datenverkehr nach Art. 46 DS-GVO, wie z. B. Standardvertragsklauseln und Verbindliche interne Datenschutzvorschriften (BCRs), aus. Diese Auswirkungen ergeben sich nicht nur im Hinblick auf Datenübermittlungen in die USA, sondern auch in andere Drittländer. Auch hier müssen die Verantwortlichen prüfen, ob die gewählten Transferinstrumente gewährleisten, dass die personenbezogenen Daten, die in das Drittland übermittelt werden sollen, während der Übermittlung und im Drittland selbst einen im Wesentlichen gleichen Schutz genießen wie in der EU und, wenn notwendig, zusätzliche Maßnahmen ergreifen, um diesen Schutz herzustellen. Wenn das unzureichende Schutzniveau aus behördlichen Zugriffsmöglichkeiten herrührt, sind ausreichende zusätzliche Maßnahmen im Bereich von Videokonferenzdiensten schwer denkbar, denn mindestens bestimmte Rahmendaten der Konferenzen müssen dem Anbieter aus technischen Gründen zugänglich sein. Verantwortliche, die Videokonferenzdienste nutzen, müssen nach Art. 5 Abs. 2 DS-GVO nachweisen können, dass sie diese Prüfung vorgenommen haben und die Daten im Drittland nach diesen Maßstäben ausreichend geschützt sind. Zu den Auswirkungen des Urteils generell und den Konsequenzen für die

einzelnen Übermittlungsinstrumente hat der Europäische Datenschutzausschuss (EDSA) bereits am 23.07.2020 FAQs beschlossen.[8]

4 Technische und organisatorische Anforderungen

Das Videokonferenzsystem ist gemäß Art. 24, 25 DS-GVO durch Auswahl und Umsetzung geeigneter technischer und organisatorischer Maßnahmen so einzurichten, dass es den Anforderungen der DS-GVO an die Verarbeitung personenbezogener Daten genügt. Hinweise zur Umsetzung dieser Anforderungen finden sich in den nachfolgenden Abschnitten.

4.1 Sicherheit der Übertragung

Videokonferenzsysteme müssen eine Verschlüsselung nach dem Stand der Technik implementieren. Hierzu liefert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zu geeigneten kryptographischen Verfahren[9].

Für die Übertragung von Videokonferenzdaten ist mindestens eine Transportverschlüsselung entsprechend den einschlägigen Technischen Richtlinien des BSI[10] erforderlich. Die Transportverschlüsselung muss die Vertraulichkeit, Integrität und Authentizität aller übertragenen Daten gewährleisten: der Inhaltsdaten wie auch der Rahmendaten[11].

Insbesondere wenn die Verarbeitung von Daten im Rahmen einer Videokonferenz zu einem hohen Risiko für betroffene Personen führen kann, müssen der Verantwortliche und ggf. der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen treffen, um insbesondere die Vertraulichkeit der übermittelten Inhaltsdaten auf zentralen Servern und den anderweitig beteiligten IT-Komponenten sicherzustellen. Dies kann beispielsweise über eine Ende-zu-Ende-Verschlüsselung und eine Verschlüsselung gespeicherter Daten sichergestellt werden. Eine wirksame Ende-zu-Ende-Verschlüsselung setzt voraus, dass die Endgeräte der Teilnehmenden sich gegenseitig nachprüfbar authentisieren und für jede Konferenz neue flüchtige Verschlüsselungsschlüssel unter Kontrolle der Konferenzteilnehmer so erzeugt, ausgehandelt bzw. verteilt werden, dass dem Betreiber keine Kenntnisnahme des Schlüsselmaterials möglich ist. Zum Zeitpunkt der Erstellung dieses Papiers waren Ende-zu-Ende-verschlüsselnde Lösungen,

---

8 https://edpb.europa.eu/our-work-tools/our-documents/ovrigt/frequently-asked-questions-judgment-court-justice-european-union_en

9 https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html

10 ebd.

11 zur Definition siehe Abschnitt 1

die diese Anforderungen erfüllen und die Videokonferenzen für eine höhere Anzahl von teilnehmenden Personen auch dann ermöglichen, wenn den teilnehmenden Personen an den von ihnen genutzten Endpunkten nur eine geringe oder variierende Bandbreite und Rechenleistung zur Verfügung steht, noch nicht marktgängig. Unter den beschriebenen Umständen kann daher eine Transportverschlüsselung zur Erfüllung der gesetzlichen Verpflichtungen genügen, sofern durch kompensierende Maßnahmen ein dem Risiko angemessenes Schutzniveau gewährleistet wird. Die kompensierenden Maßnahmen müssen sich auf die Sicherheit der Dienste und Systeme des Betreibers – also des Diensteanbieters oder des für das Hosting des Dienstes in Anspruch genommenen Auftragnehmers – erstrecken (zusätzliche Härtung) und auch organisatorische Maßnahmen des Betreibers einschließen, die eine Kenntnisnahme der verarbeiteten Daten durch Beschäftigte des Betreibers erschweren.

Ist im Zuge der Durchführung von Videokonferenzen ein unbefugter Abfluss personenbezogener Daten zu befürchten, dann sollte der Nutzen der Inanspruchnahme von bestimmten Funktionalitäten des Dienstes (insbesondere private Chats, Screensharing und die Bereitstellung von Dokumenten in einem allen Teilnehmenden offenstehenden Arbeitsbereich) mit den hierbei verbundenen Risiken abgewogen und sollten ggf. die Funktionalitäten unterbunden werden. Wenn der Veranstalter zentral für alle teilnehmenden Endgeräte entsprechende Funktionalitäten zuverlässig technisch deaktivieren kann, so ist dies hilfreich. Eine geeignete Maßnahme zur Aufdeckung derartiger Abflüsse kann auch in einer Protokollierung der Inanspruchnahme der genannten Funktionalitäten liegen. Die Transparenz einer solchen Protokollierung für die Teilnehmenden ist zu wahren.

Der Einsatz der einzelnen Funktionalitäten eines eingesetzten Videokonferenzsystems sollte separat und im Kontext betrachtet werden. So kann bei einem Verantwortlichen bspw. ein Dokumentenmanagementsystem (DMS) im Einsatz sein. Hier wäre zu prüfen, ob dieses System einer Dokumentenaustauschfunktionalität des Videokonferenzsystems vorzuziehen ist. Bei der Prüfung sind insbesondere auch die Risiken für Rechte und Freiheiten der betroffenen Personen zu berücksichtigen.

Betreibt der Verantwortliche (oder ein für das Hosting des Dienstes in Anspruch genommener Auftragnehmer) Serversoftware für den Betrieb oder stellt der Verantwortliche den Teilnehmenden (mobile) Anwendungen zur Verfügung, für die er von einem Dritten Nutzungsrechte erworben hat, ist er ebenfalls verpflichtet, sicherzustellen, dass der Hersteller und andere Dritte keinen Zugriff auf die verarbeiteten Daten erhalten, auch nicht auf einzelne Teile wie Nutzungsdaten.

4.2 Nutzerauthentifizierung

Nur berechtigte Personen sollten auf eine Videokonferenzsitzung und deren Daten zugreifen können. Hierzu müssen sich die teilnehmenden Personen gegenüber dem Videokonferenzdienst authentisieren.

Die benötigte Mindeststärke der Authentisierung hängt von der Schwere der Risiken für die Rechte und Freiheiten der betroffenen Personen ab, die sich bei einem Bruch der Vertraulichkeit oder Integrität der Inhaltsdaten ergeben können.

4.2.1 Normale Risiken

Bei normalen Risiken genügt eine Authentisierung mit Nutzername und geeignetem Passwort. Das Authentifizierungsprotokoll soll so ausgestaltet sein, dass Passwörter weder übertragen noch bei dem Dienstleister gespeichert werden. Dem Stand der Technik entsprechende Authentifizierungsverfahren verhindern, dass aus dem Passwort abgeleitete Daten, die im Zuge eines Authentifizierungsvorgangs übertragen wurden, für einen zweiten Authentifizierungsvorgang wiederverwendet werden können. Sie verhindern ferner, dass die bei dem Verantwortlichen oder die bei dem Auftragsverarbeiter, der die Authentifizierung durchführt, gespeicherten Verifikationsdaten für eine Anmeldung verwendet werden können, um die Folgen einer Kompromittierung dieser Daten zu minimieren.

4.2.2 Hohe Risiken

Sind mit dem Bruch der Vertraulichkeit der voraussichtlich in den Inhaltsdaten der Konferenz enthaltenen Angaben über natürliche Personen hohe Risiken für die Rechte und Freiheiten dieser Personen verbunden, muss zumindest eine Zwei-Faktor-Authentisierung nach dem Stand der Technik erfolgen. Dafür kommen je nach Höhe des Risikos insbesondere Softwaretoken bzw. Hardwaretoken in Frage.

4.2.3 Authentifizierungsdienst

Um eine konsistente Verwaltung der Nutzungsberechtigungen zu gewährleisten, ist Verantwortlichen dringend empfohlen, die Nutzerauthentifizierung auf Verfahren zu stützen, die bereits für andere Verfahren genutzt werden. Bei einer Entscheidung über eine etwaige Anbindung sind der konkrete Einsatzkontext und die mit der Anbindung verbundenen Risiken zu berücksichtigen. Bei einer Anbindung des Videokonferenzdienstes an einen Verzeichnisdienst über LDAP werden die Nutzerpasswörter in der Regel im Klartext verarbeitet. Deshalb eignet sich dieses Verfahren in erster Linie für selbst betriebene Videokonferenzsysteme. Bei nicht

selbst gehosteten Videokonferenzsystemen kann stattdessen beispielsweise OpenID Connect benutzt werden. Der Identity Provider muss die Integrität des Authentifizierungsvorgangs und die Nichtverkettung verschiedener Nutzungsvorgänge gewährleisten.

Für die Authentifizierung von Personen außerhalb der Institution des Verantwortlichen kann auf die Authentifizierung durch einen Identitätsdiensteanbieter zurückgegriffen werden, wenn sich der Verantwortliche von den relevanten Aspekten der Identität der oder des Teilnehmenden im Vorlauf zur oder im Zuge der ersten Videokonferenz überzeugt.

Bei Anwendungsfällen, die eine vorherige Identifikation der Nutzer erfordern und voraussichtlich zu einer Übermittlung von besonders schutzwürdigen personenbezogenen Daten über Dritte führen, müssen geeignete Verfahren implementiert sein, um die Authentizität der Nutzer im Nachhinein nachvollziehen zu können.

4.2.4 Gastteilnahme

Unter den folgenden Bedingungen dürfen Videokonferenzsysteme einen Gastzugang anbieten, der keine vorherige Identifizierung des Nutzers voraussetzt:

- Der Gastzugang muss für den jeweiligen Anwendungsfall erforderlich sein.
- Die Risiken für betroffene Personen, die durch eine nicht autorisierte Teilnahme entstehen, sind geringfügig.
- Es ist gewährleistet, dass nur Personen teilnehmen, die untereinander bekannt sind.
- Nicht autorisierte Personen werden erkannt und können aktiv ausgeschlossen werden, noch bevor sie aktiv an der Videokonferenz teilnehmen können.

Ein Gastzugang kann in den gängigen Systemen beispielsweise über einen Einladungslink ermöglicht werden, der den Gästen im Vorfeld zur Videokonferenzsitzung mitgeteilt wird und bei denen die Gäste vor Beginn der Videokonferenz lediglich ein Pseudonym für sich vergeben müssen. Die Empfänger dieses Links sind auf die Folgen einer nicht autorisierten Weitergabe des Links hinzuweisen. Die Übergabe des Links muss die Vertraulichkeit auf angemessenem Niveau wahren.

4.3 Installation und Softwareaktualisierung

Technische Schwachstellen und sonstige Sicherheitslücken in Videokonferenzsystemen können nach Bekanntwerden eventuell zu einem nicht mehr vertretbaren Verarbeitungsrisiko und damit zu einem Nutzungsstopp führen. Sie müssen in einem angemessenen Zeitraum behoben

werden, bei hohen Risiken unverzüglich. Dies muss durch den Softwarehersteller bzw. den Anbieter des Dienstes erfolgen; Verantwortliche haben dies sicherzustellen. Funktionale Ergänzungen sollten, wenn es der Anwendungsfall zulässt, mittels betriebssystemeigener Aktualisierungsmethoden (Paketverwaltungen) erfolgen. Falls die Videokonferenzsysteme in einer administrierten Umgebung arbeiten, sollte eine zentrale Aktualisierung der zugehörigen Software erfolgen.

Alle Komponenten, die für die Teilnahme an einer Videokonferenz auf einem Client installiert werden, müssen ebenso einfach und vollständig wieder deinstalliert werden können.

Auch im Fall einer nur einmaligen Nutzung eines nativen Clients durch eine teilnehmende Person muss sichergestellt sein, dass keine nicht gewartete Software auf dem System verbleibt und ein mögliches Sicherheitsrisiko darstellt.

Sofern webbasierte Videokonferenzsysteme genutzt werden, muss für einen sicheren Betrieb stets eine aktuelle Webbrowser-Version eingesetzt werden. Dasselbe gilt für ggf. erforderliche Browser-Erweiterungen.

4.4 Rollentrennung

Videokonferenzsysteme für größere Zahlen an Teilnehmenden sollten die Einrichtung mindestens folgender Rollen ermöglichen:

1. administrierende Personen:

   Diese Rolle verfügt typischerweise über die Berechtigung zur Festlegung von Parametern der durchzuführenden Konferenzen (z. B. Erlaubnis oder Verbot von Aufzeichnungen und Chats parallel zur Videokonferenz) und die Zuweisung der Moderationsrolle.

2. moderierende Personen:

   Diese Rolle verfügt typischerweise über die Berechtigung, Videokonferenzen anzuberaumen, teilnehmende Personen einzuladen oder auszuschließen, den Zutritt zu einer Konferenz zu eröffnen oder zu schließen, ggf. teilnehmende Personen Gruppen zuzuweisen, in denen ein separierter Austausch stattfindet, und die Präsentationsrolle einzelnen teilnehmenden Personen zuzuweisen.

3. präsentierende Personen:

Diese Rolle verfügt typischerweise über die Berechtigung, audiovisuelle Medien und Dokumente für die Kenntnisnahme der teilnehmenden Personen bereitzustellen und deren Wortmeldungen zu steuern.

4. teilnehmende Personen:

   Diese Rolle verfügt typischerweise ausschließlich über die Berechtigung, die eigenen Aufzeichnungs- und Wiedergabegeräte zu steuern.

Die Rollen können ggf. auch anders zugeschnitten werden, soweit die Verantwortung für die Steuerung der implizit vorgenommenen Verarbeitung von personenbezogenen Daten klar zugewiesen bleibt.

Jede teilnehmende Person muss ihr Mikrofon und ihre Kamera jederzeit deaktivieren können. Ohne die Zustimmung der teilnehmenden Person darf deren Mikrofon und deren Kamera nicht aktiviert werden können.

Bei Anwendungen mit hohem Risiko ist eine Nutzerverwaltung, die die Autorisierung der teilnehmenden Personen zur Übernahme einer der o. g. Rollen sicherstellt, verpflichtend vorzusehen (siehe auch Abschnitt 4.2).

4.5 Datensparsamkeit

Videokonferenzdienste sollten nur die für die Bereitstellung des Dienstes zwingend erforderlichen technischen und sonstigen Informationen verarbeiten. Insbesondere sollten die Protokolldaten nur für den Zweck der Konferenz verarbeitet werden. Analysen des Nutzungsverhaltens und die Verarbeitung personenbezogener Diagnose- und Telemetriedaten durch den Anbieter des eingesetzten Dienstes zu eigenen Zwecken widersprechen dem Grundsatz der Datensparsamkeit (siehe Abschnitt 3), sofern sie nicht für die Diensterbringung erforderlich sind und eine eigene Rechtsgrundlage haben. Ein Beispiel für eine kritische Datenverarbeitung wäre die Verkettung von Nutzungen eines Nutzungskontos, das an Konferenzen verschiedener Konferenzveranstalter teilnimmt.

Videokonferenzsysteme müssen die Grundsätze des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen erfüllen (Art. 25 DS-GVO). So müssen im Sinne der Datensparsamkeit jedenfalls die Kamera, das Mikrofon und das Teilen des Bildschirms von Teilnehmern vor Eintritt in die Konferenz standardmäßig ausgeschaltet sein. Damit

die teilnehmenden Personen entscheiden können, wann sie diese Geräte und Funktionen einschalten, muss ihnen transparent sein, wer bzw. welche Arten von Teilnehmern sie sehen und hören können.

4.6 Transparenz

Zur Ergänzung der rechtlich gebotenen Hinweise in den Datenschutzbestimmungen, die von den Betreibern der Videokonferenzsysteme erteilt werden (siehe Abschnitt 3.5.1), sollten auch die Hersteller der Systeme Aussagen über die technischen Implementierungen, die eingesetzten Standards, Software-Bibliotheken und Lizenzen treffen.

Für die teilnehmenden Personen muss leicht verständlich und an einer prominenten Stelle erkennbar sein, ob und ggf. welche Datenverarbeitungsvorgänge über den eigentlichen Anwendungszweck der Videokonferenz hinaus erfolgen. Insbesondere Funktionen wie Video- und/oder Tonaufzeichnungen sowie Aufmerksamkeitsanalysen müssen, sofern sie überhaupt zulässig sind, den teilnehmenden Personen nachweislich vor Beginn der Verarbeitung angekündigt werden und dürfen erst nach Freischaltung dieser Funktion aktiviert werden. Zudem sind die rechtlichen Anforderungen einzuhalten.

Quelloffene Systeme können Transparenz fördern, da hier technische Experten tiefergehende Analysen einzelner Funktionsaufrufe durchführen können als in proprietärer Software. Technische Papiere wie White Paper können die technische Struktur und die wichtigsten Komponenten der Videokonferenzsysteme systematisch offenlegen. Berichte über Sicherheitsprüfungen sollten – ggf. nach einer angemessenen Zeit zur Beseitigung aufgefundener Sicherheitsprobleme – frei zugänglich veröffentlicht werden.

4.7 Aufzeichnungen

Sind Aufzeichnungen der Videokonferenz nicht zulässig (siehe Abschnitt 3.4.8), so sind die Möglichkeiten der Aufzeichnung durch teilnehmenden Personen technisch zu unterbinden, soweit der Verantwortliche hierauf Einfluss hat (also im Rahmen seiner eigenen Organisation). Wenn dies durch eine Konfigurationseinstellung geschieht, darf diese nur ein Administrator zurücknehmen können. Die Teilnehmer der Videokonferenz sind darauf hinzuweisen, dass eine Aufzeichnung unzulässig ist.

Soweit Aufzeichnungen ausnahmsweise zulässig sind, dürfen sie nur durch besonders privilegierte Nutzer, beispielsweise Moderatoren, aktivierbar sein. Es muss für die Teilnehmenden

einer Videokonferenz entweder durch einen expliziten und durch die Teilnehmenden zu bestätigenden Hinweis oder durch Kennzeichnung innerhalb der Benutzerschnittstelle darauf hingewiesen werden, wenn eine Videokonferenz ganz oder in Teilen aufgezeichnet wird.

Aufzeichnungen von Videokonferenzen sollten verschlüsselt gespeichert werden. Bei hohem Risiko ist dies zwingend vorzusehen.

4.8 Intervenierbarkeit

Teilnehmende müssen die technische Möglichkeit haben, zumindest zeitweise an Konferenzen lediglich empfangend, aber nicht sendend teilzunehmen, d. h. Kamera und Mikrofon auszuschalten, wobei getrennte Deaktivierungsmöglichkeiten für Audio- und Videoübertragung vorzusehen sind.