Die Landesbeauftragte für den
Datenschutz Niedersachsen

Fragen und Antworten zu Videokonferenzsystemen (August 2020)

Durch die Corona-Pandemie hat der Bedarf an Videokonferenzen im beruflichen Alltag enorm zugenommen. Zugleich stellten und stellen sich zahlreiche Fragen zum Einsatz der Konferenzsysteme, die letztlich alle darauf hinauslaufen, welches Produkt die datenschutzrechtlichen Anforderungen erfüllt.

Verantwortliche Stellen sehen sich dabei einer grundsätzlichen Herausforderung gegenüber: Während die Datenschutz-Grundverordnung (DS-GVO) von ihnen verlangt, Datenschutz schon bei der Produktauswahl (Privacy by Design) und in den Voreinstellungen dieser Produkte (Privacy by Default) angemessen zu berücksichtigen, gelten diese Verpflichtungen bedauerlicherweise nicht für die Produkthersteller und Diensteanbieter. Die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder haben sich in der Datenschutzkonferenz (DSK) dafür ausgesprochen, die Hersteller mehr in die Pflicht zu nehmen. Doch kurzfristig dürfte sich nichts an der gesetzlichen Ausgangslage ändern.

Umso wichtiger ist es für die Aufsichtsbehörden, die Verantwortlichen bei der Auswahl der richtigen Videokonferenzsysteme zu beraten. Ein konkretes Produkt können sie nicht benennen, ohne unsachgemäß in den Wettbewerb einzugreifen. Aber sie können und müssen Hinweise zur Auswahl datenschutzfreundlicher Angebote und zur praktischen Durchführung von Videokonferenzen geben.

Allgemeine Fragen

1. Welche Arten von Videokonferenztechnologien müssen aus datenschutzrechtlicher Sicht unterschieden werden?

Dem Verantwortlichen stehen zwei grundsätzliche Möglichkeiten zur Verfügung ein Videokonferenzsystem zu betreiben:

1. Er kann das System über einen externen IT-Dienstleister nutzen. In diesem Fall handelt es sich um einen cloudbasierten Online-Dienst („Software-as-a-Service“).

2. Alternativ kann die Videokonferenz-Software auf eigenen Servern installiert werden. Diese Lösung wird als „On-Premises“ bezeichnet.

2. Wer ist Verantwortlicher bei einer cloudbasierten Videokonferenz?

Verantwortlicher ist jede Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (Art. 4 Nr. 7 DS-GVO). Über die Zwecke der Verarbeitung entscheidet, wer den Anlass zu einer Verarbeitung gegeben und den Grund für die Verarbeitung bestimmt hat. Der Veranstalter einer Videokonferenz ist daher immer als Verantwortlicher anzusehen (ggf. gemeinsam mit anderen), da er die Datenübermittlung per Videokonferenz veranlasst hat.

Der Anbieter der cloudbasierten Videokonferenz-Software („Software-as-a-Service“-Architektur) ist regelmäßig nicht als Verantwortlicher, sondern als Auftragsverarbeiter anzusehen. Er verarbeitet nach den Weisungen des Verantwortlichen personenbezogene Daten auf Grundlage eines Vertrages gemäß Art. 28 Abs. 3 DS-GVO. Verwendet der Anbieter der Konferenztechnik die per Videokonferenz übermittelten Daten jedoch zu eigenen Zwecken (z. B. Übergabe von Nutzungsdaten an Dritte oder Verwendung für Werbezwecke) ist er insoweit selbst für diese Datenverarbeitungen als Verantwortlicher anzusehen.

3. Auf welche Rechtsgrundlage kann die Durchführung einer Videokonferenz gestützt werden?

Für die rechtmäßige Verarbeitung der personenbezogenen Daten der Konferenzteilnehmenden bedarf es einer Rechtsgrundlage. Es kommt auf die Umstände des Einzelfalls an, welche Rechtsgrundlage in Frage kommt. Wird eine Videokonferenz über eine cloudbasierten Videokonferenztechnik organisiert, um einen kostenpflichtigen Online-Kurs durchzuführen, kann die Verarbeitung personenbezogener Daten etwa zur Erfüllung eines Vertrags nach Art. 6 Abs. 1 lit. b DS-GVO erforderlich sein. Je nach Einzelfall kann eine Videokonferenz gemäß § 26 Abs. 1 Satz 1 BDSG auch zur Durchführung des Beschäftigungsverhältnisses erforderlich sein (siehe hierzu Frage Nr. 17).

In vielen Fällen wird eine Videokonferenz auf der Grundlage einer Einwilligung des Betroffenen gemäß Art. 6 Abs. 1 lit. a DS-GVO durchgeführt werden. Eine zusätzliche Rechtsgrundlage ist erforderlich, wenn die Videokonferenz beispielsweise aufgezeichnet werden soll.

Eine zusätzliche Rechtsgrundlage ist außerdem erforderlich, wenn personenbezogene Daten in Drittländer übermittelt werden (siehe Frage Nr. 7).

4. Welche Anforderungen gelten für eine Einwilligung im Zusammenhang mit einer Videokonferenz?

Eine Einwilligung muss gemäß Art. 6 Abs. 1 lit. a i. V. m. Art. 4 Nr. 11 DS-GVO freiwillig und auf informierter Grundlage unmissverständlich erteilt werden. Insbesondere die Aufzeichnung einer Videokonferenz wird in aller Regel nur über eine Einwilligung zulässig sein. Die Einwilligung kann grundsätzlich auch elektronisch gegeben werden, etwa durch das Anklicken eines Kästchens (z. B. „*Hiermit willige ich ein, dass meine personenbezogenen Daten wie oben angegeben, verarbeitet werden.*“). Allerdings kann die Freiwilligkeit einer Einwilligung insbesondere bei Erteilung im beruflichen oder schulischen Kontext problematisch sein (vgl. Fragen Nrn. 19 und 22).

Überdies kann es Konstellationen geben, in denen nicht nur der Veranstalter der Konferenz, sondern auch der Anbieter der Videokonferenz-Software eine Einwilligung des Betroffenen für die Verarbeitung personenbezogener Daten einholt. Ein Grund hierfür mag sein, dass der Software-Anbieter bestimmte Daten des Betroffenen zu eigenen Zwecken verwenden oder mit Dritten teilen möchte. Datenschutzrechtlich wäre für einen solchen Fall ein ausdrücklicher Hinweis auf die Einwilligung und eine unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder eindeutigen Handlung erforderlich, etwa in Form eines anzuklickenden Kontrollkästchens mit dem Text „Ich willige ein, dass…“. Auf keinen Fall dürfen Einwilligungserklärungen in Software-Nutzungsbedingungen oder in einer (zu akzeptierenden) Datenschutzerklärung „versteckt“ werden. Denn das genügt nicht den bestehenden Transparenzanforderungen.

5. Welche datenschutzrechtlichen Pflichten hat ein Verantwortlicher, der eine Videokonferenz veranstaltet?

Der Verantwortliche muss dafür sorgen, dass die **datenschutzrechtlichen Voraussetzungen** für die Durchführung einer Videokonferenz erfüllt sind, wie das Vorliegen einer Rechtsgrundlage (siehe oben Frage Nr. 3). Darüber hinaus muss der Verantwortliche angemessene und **ausreichende technisch-organisatorische Maßnahmen** ergreifen. So ist eine Transportverschlüsselung heute für netzbasierte Anwendungen selbstverständlich und muss daher grundsätzlich auch von jedem Videokonferenzsystem erfüllt werden. Aufgrund des besonderen Schutzbedarfs für die meisten Kommunikationsinhalte sollte außerdem standardmäßig eine Ende-zu-Ende-Verschlüsselung eingesetzt werden. Bei der technischen Umsetzung ist der Stand der Technik zu berücksichtigen. „Stand der Technik“ ist die derzeit beste auf dem Markt verfügbare Technik, analog zum englischen „State of the Art“. Jeder Verantwortliche, der auf eine Ende-zu-Ende-Verschlüsselung verzichtet, muss diese Entscheidung nach den Art. 5, 24 Abs. 1, 25 Abs. 1 und 32 DS-GVO sorgfältig begründen und dokumentieren.

Weiter muss der Veranstalter einer Videokonferenz Auskunftsanfragen betroffener Personen beantworten und die Informationspflichten gemäß Art. 13f. DS-GVO gegenüber allen Betroffenen erfüllen. Hinzu kommt die Rechenschaftspflicht nach Art. 5 Abs. 2 DS-GVO, wonach der Verantwortliche die Einhaltung der Datenschutzgrundsätze jederzeit nachweisen können muss. Der Nachweis wird erbracht durch eine Dokumentation, die insbesondere

- eine schriftliche Festlegung von Rechtsgrundlagen und Zwecken für die Verarbeitung,
- ein Verzeichnis der Verarbeitungstätigkeiten,

- eine durchgeführte Datenschutz-Folgenabschätzung (s. Frage 19),
- eingeholte Einwilligungen,
- Art und Weise der Erfüllung der Informationspflichten und Betroffenenrechte sowie
- ergriffene technische und organisatorische Maßnahmen mit Begründung

enthält. Daneben sind ggf. Verträge etwa zur Auftragsverarbeitung zu schließen.

6. Genügt es für den Verantwortlichen, dass der Diensteanbieter in seiner Datenschutzerklärung angibt, wie die personenbezogenen Daten der Konferenzteilnehmer verarbeitet werden, um die Informationspflichten gemäß Art. 13 DS-GVO zu erfüllen?

Nein, die datenschutzrechtlichen Hinweise des Service-Providers (Diensteanbieters) in der Datenschutzerklärung können nicht die Informationspflichten des Verantwortlichen ersetzen, der die Videokonferenz organisiert. Der Verantwortliche muss für seinen Verantwortungsbereich die Informationspflichten gemäß Art. 13 DS-GVO gegenüber allen betroffenen Personen erfüllen und deren Betroffenenrechte umsetzen. Es empfiehlt sich, den Teilnehmenden einer Videokonferenz im Vorfeld per E-Mail die Informationen zur Verfügung zu stellen. Insbesondere ist darüber zu informieren, wer Verantwortlicher ist, zu welchen Zwecken und auf welcher Rechtsgrundlage die personenbezogenen Daten verarbeitet werden und wer diese empfängt. Dabei ist auch anzugeben, wenn eine Übermittlung in Drittländer erfolgt (z. B. Verarbeitung der Daten durch einen Anbieter einer cloudbasierten Videokonferenz-Software mit Sitz in den USA) und ob diese Übermittlung auf einen Angemessenheitsbeschluss der EU-Kommission oder andere Garantien gestützt wird. Werden Daten gespeichert, muss angegeben werden, wie lange dies geschieht. Weiter ist über die Betroffenenrechte (u. a. Recht auf Auskunft, Löschung, Berichtigung oder Widerspruchsrecht; Hinweis auf das Widerrufsrecht bei erteilten Einwilligungen) und das Beschwerderecht bei der Aufsichtsbehörde zu informieren. Weitere Einzelheiten zu den Informationspflichten finden Sie hier.

7. Welche Auswirkungen hat das EuGH-Urteil vom 16.07.2020 in Sachen Facebook ./. Schrems auf die Durchführung von Videokonferenzen?

Bei zahlreichen cloudbasierten Produkten fanden bisher Datenübermittlungen in die USA gestützt auf das sog. Privacy Shield statt. Der Europäische Gerichtshof (EuGH) hat in seinem Urteil vom 16.07.2020 (Rs. C-311/18) diesen Angemessenheitsbeschluss der Europäischen Kommission zur Übermittlung personenbezogener Daten in die USA für unwirksam erklärt. Eine Übergangsfrist gewährte der EuGH nicht. Verantwortliche können sich bei der Veranstaltung von Videokonferenzen, bei denen personenbezogene Daten in die USA übermittelt werden, folglich nicht mehr darauf berufen, dass die Anbieter der eingesetzten Produkte unter dem Privacy Shield zertifiziert sind. Die Durchführung von Videokonferenzen, bei denen die Datenübermittlung in die USA *ausschließlich* auf Privacy Shield gestützt wird, ist daher unzulässig und muss sofort eingestellt werden. Verantwortliche, die weiterhin Videokonferenzen durchführen möchten, müssen prüfen, welche alternativen Übermittlungsinstrumente in Betracht kommen.

8. Dürfen bei der Veranstaltung von Videokonferenzen Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer verwendet werden?

Der EuGH hat im Urteil vom 16.07.2020 (Rs. C-311/18) die Standardvertragsklauseln zwar weiterhin für gültig befunden. Grundsätzlich können daher Verantwortliche weiterhin auf dieser Grundlage Videokonferenzen betreiben. Neu ist allerdings, dass der Verantwortliche künftig vorab prüfen muss, ob die Rechte der betroffenen Personen im Drittland ein Schutzniveau genießen, das dem in der Europäischen Union (EU) / im Europäischen Wirtschaftsraum (EWR) durch die DS-GVO garantierten Niveau gleichwertig ist. Das garantierte Niveau der DS-GVO steht auch im Lichte der EU-Grundrechtecharta. Für die Prüfung des Rechtssystems des Drittlandes gilt derselbe Maßstab wie für Angemessenheitsentscheidungen der Kommission nach Art. 45 Abs. 2 DS-GVO. Sofern der Verantwortliche zu dem Ergebnis gelangt, dass kein gleichwertiges Schutzniveau besteht und auch nicht durch zusätzliche Maßnahmen gewährleistet werden kann, darf keine Übermittlung personenbezogener Daten erfolgen. Eine bestehende Datenübermittlung ist auszusetzen oder zu beenden.

9. Gibt es Besonderheiten für Videokonferenzen, bei denen personenbezogene Daten in die USA übermittelt werden?

Ja. Zunächst gilt das zu Frage 7 Gesagte. Allerdings hat der EuGH in dem Urteil vom 16.07.2020 (Rs. C-311/18) bereits festgestellt, dass das US-Recht kein Schutzniveau gewährleistet, das dem in der EU / im EWR gleichwertig ist. In der Praxis wird es daher darauf ankommen, ob und inwieweit Verantwortliche die in den Standarddatenschutzklauseln enthaltenen Garantien bei Datenübermittlungen in die USA durch zusätzliche Maßnahmen ergänzen können, um die Einhaltung eines gleichwertigen Schutzniveaus zu gewährleisten. Der Europäische Datenschutzausschuss (EDSA) prüft derzeit, worin zusätzliche Maßnahmen liegen könnten. Denkbar sind rechtliche, technische oder organisatorische Maßnahmen. Der EDSA hat angekündigt, hierzu weitere Hilfestellungen zu entwickeln. Im Zweifel empfiehlt es sich, Videokonferenzsysteme zu nutzen, bei denen sich der Server innerhalb von EU/EWR befindet und keine Notwendigkeit besteht, personenbezogene Daten in die USA zu übermitteln.

10. Dürfen bei Videokonferenzen personenbezogene Daten ausnahmsweise auch ohne geeignete Garantien im Sinne des Art. 46 DS-GVO in die USA oder andere Drittländer übermittelt werden?

Im Einzelfall kann die Übermittlung personenbezogener Daten auf Ausnahmen nach Art. 49 DS-GVO gestützt werden. Aus datenschutzrechtlicher Sicht sollte es deshalb vermieden werden, Videokonferenzen **regelmäßig** auf Art. 49 DS-GVO zu stützen, weil dann Verbindungs- und Inhaltsdaten ins Drittland übermittelt werden, ohne dass geregelt wäre, wie der Empfänger im Drittland mit diesen Daten umzugehen hat. Daher sind vor allem die Hürden für eine Einwilligung nach Art. 49 Abs. 1 Satz 1 lit. a DS-GVO sehr hoch gesetzt – diese muss „ausdrücklich“, auf freiwilliger Basis und in Kenntnis dessen erteilt werden, dass die Daten im Drittland mehr oder weniger schutzlos sind. Zudem ist die Einwilligung jederzeit widerrufbar. Hinzu kommt, dass viele Tatbestände in Art. 49 DS-GVO auch nicht für wiederkehrende Übermittlungen konzipiert sind. Für die Anwendung des Art. 49 DS-GVO gelten weiterhin die Leitlinien 2/2018 des Europäischen Datenschutzausschusses zu den Ausnahmen nach Art. 49 der Verordnung 2016/679 vom 25.05.2018.

11. Muss ein Verantwortlicher Aspekte des internationalen Datenverkehrs beachten, wenn an einer Videokonferenz ausschließlich Personen aus Deutschland oder der EU teilnehmen?

Das hängt von der eingesetzten Software ab. Bei vielen cloudbasierten Diensten finden zum Gesprächsaufbau Datenübermittlungen in die USA statt, auch wenn die Teilnehmenden sich alle innerhalb der Europäischen Union befinden. Dann müssen die Aspekte des internationalen Datenverkehrs beachtet werden.

Befinden sich dagegen die eingesetzten Server ausschließlich innerhalb der EU bzw. des EWR, besteht keine Notwendigkeit, personenbezogene Daten an Drittländer zu übermitteln, sofern sich alle Teilnehmenden ebenfalls in der EU oder im EWR befinden.

12. Müssen die spezifischen Datenschutzvorschriften des Telekommunikationsgesetzes (TKG) beachtet werden?

Endnutzer von Videokonferenzsystemen sind nicht verpflichtet, datenschutzrechtliche Vorgaben des TKG einzuhalten. Stattdessen sind für sie die DS-GVO, das BDSG und die Landesdatenschutzgesetze maßgeblich.

Technischer und organisatorischer Datenschutz

13. Reicht es aus, wenn ich auf die vom Hersteller zugesicherten technischen Eigenschaften des Produktes oder die „ordentliche" Qualität des Dienstes eines Anbieters vertraue, weil diese als selbstverständlich datenschutzkonform gelten müssen?

Nein. Personenbezogene Daten müssen u. a. nach den Grundsätzen des Art. 5 lit. f) sowie nach Art. 24, 25 und 32 DS-GVO in einer Weise verarbeitet werden, die eine angemessene Sicherheit gewährleistet. Das schließt den Schutz durch geeignete technische und organisatorische Maßnahmen vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust genauso ein wie den vor unbeabsichtigter Zerstörung oder Schädigung.

Der Verantwortliche ist verpflichtet, technisch-organisatorische Maßnahmen (TOM) zu implementieren oder implementieren zu lassen, durch welche die Rechte und Freiheiten natürlicher Personen angemessen geschützt werden. Dies ist Aufgabe des Verantwortlichen, nicht die des Herstellers der Systeme. Die TOM trifft der Verantwortliche sowohl, wenn er die Mittel für die Verarbeitung festlegt als auch zum Zeitpunkt der eigentlichen Verarbeitung (**Datenschutz durch Technikgestaltung**, data protection by design, Art. 25, Abs. 1 DS-GVO). Zudem trifft er geeignete TOM, die sicherstellen, dass durch Voreinstellung nur personenbezogene Daten verarbeitet werden, die für den jeweiligen Verarbeitungszweck erforderlich sind (**Datenschutz durch datenschutzfreundliche Voreinstellungen**, data protection by default, Art. 25, Abs. 2 DS-GVO).

Im Sinne des EG 78 sollten die Hersteller von "Produkten, Diensten und -Anwendungen **ermutigt** werden, das Recht auf Datenschutz bei der Entwicklung und Gestaltung der Produkte, Dienste und Anwendungen zu berücksichtigen und unter gebührender Berücksichtigung des Stands der Technik sicherzutellen, dass die Verantwortlichen und die Verarbeiter in der Lage sind, ihren Datenschutzpflichten nachzukommen“. Eine rechtliche Durchsetzbarkeit seitens des Verantwortlichen oder der Datenschutzaufsichtsbehörden gegen die Hersteller gibt es nicht. Die faktische Durchsetzbarkeit hängt derzeit vielmehr von Angebot und Nachfrage ab. Deshalb sollten Verantwortliche den Systemen und Diensten der Vorzug geben, bei denen der Hersteller Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen bereits berücksichtigt.

14. Wie ermittele ich, welche technischen und organisatorischen Maßnahmen ausreichend sind, um eine datenschutzkonforme Lösung zu erhalten und zu betreiben?

Im Wesentlichen kommt es hierbei auf die Einhaltung einiger Schrittfolgen an, um alle wichtigen Einflussfaktoren zu berücksichtigen.

Jeder Verantwortliche muss zunächst alle beteiligten Personen, räumlichen, organisatorischen und technologische Aspekte erheben und betrachten. Im Kern geht es um die Betroffenenrechte und die Gewährleistungsziele, die sich insbesondere auch aus Art. 5 DS-GVO ergeben. Betroffene sind zunächst die an der Videokonferenz beteiligten Personen. Aber es gibt je nach Kontext oft auch Betroffene, die in den Konferenzinhalten als Subjekte oder Objekte auftreten, also ggf. Personen, über die gesprochen wird und deren personenbezogenen Daten zu schützen sind, z. B. vor einer Verletzung der Vertraulichkeit oder Integrität. Die Gewährleistungsziele des Datenschutzrechtes

- Datenminimierung (übergreifende Anforderung)
- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Transparenz und
- Nichtverkettung (unzulässige Verkettung von Daten verhindern)
- Intervenierbarkeit.

sind also für beide Betroffenengruppen zu erreichen.

Um die Verarbeitung der personenbezogenen Daten beurteilen zu können, müssen diese analysiert und beschrieben werden. Der Verantwortliche muss also den Zweck der Verarbeitung bestimmen und beschreiben, Art und Umfang sowie den Ablauf der Verarbeitungstätigkeit darstellen, die genutzten und erzeugten Daten benennen, das Verzeichnis der Verarbeitungstätigkeiten heranziehen, abgrenzen, was kein Bestandteil der Prüfung ist und Schnittstellen zu anderen Verarbeitungstätigkeiten (falls vorhanden) darstellen.

In den weiteren Schritten muss der Verantwortliche

- eine Strukturanalyse aller beteiligter Komponenten durchführen,
- eine Risikoanalyse für die Rechte und Freiheiten der Betroffenen erarbeiten: dies erfolgt unter Berücksichtigung der zuvor festgestellten Umstände der Verarbeitung, der Feststellung der Gefährdungen und deren Relevanz für die Risiken, die durch Untersuchung der Eintrittswahrscheinlichkeit und der einzuschätzenden Schadensschwere ermittelt wird und im Ergebnis den Risikowert (gering, normal oder hoch) ergeben
- sowie geeignete Schutzmaßnahmen auswählen; die Auswahl erfolgt unter Berücksichtigung des genannten Risikowertes, des Standes der Technik und der Implementierungskosten. Die Maßnahmen müssen wirksam und je nach den Abwägungsergebnissen angemessen sein. Dieser Schritt dient dazu, sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß den datenschutzrechtlichen Bestimmungen erfolgt.
- Schließlich müssen nach der Bestimmung der Maßnahmen das Restrisiko bewertet und die Maßnahmen ggf. konsolidiert werden.

15. Gibt es typische Gefährdungen für Rechte von Betroffenen?

Ja. Allerdings haben diese je nach Betriebsmodell (siehe Frage 1) und je nach Videokonferenzsystem teilweise unterschiedliche Relevanz. Ob die typischen Gefährdungen für das Risiko tatsächlich relevant sind, muss individuell nach dem Risiko basierten Ansatz (siehe Frage 14) geprüft werden.
Es sollten folgende Gefährdungen immer auf Relevanz geprüft werden:

- **Elementare Gefährdungen** nach IT-Grundschutzkompendium des BSI[1], die für alle IT-Systeme gelten (nicht abschließend):

[1] Gefährdungskatalog G0 Elementare Gefährdungen des BSI von 2011, abrufbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/Gefaehrdungskatalog-G0-ElementareGefaehrdungen.html bzw. die modernisierte Version Elementare Gefährdungen des BSI-Grundschutzkompendiums 2020, abrufbar unter

- G 0.9 Ausfall oder Störung von Kommunikationsnetzen
- G 0.11 Ausfall oder Störung von Dienstleistern
- G 0.14 Ausspähen von Informationen (Spionage)
- G 0.15 Abhören
- G 0.19 Offenlegung schützenswerter Informationen
- G 0.23 Unbefugtes Eindringen in IT-Systeme
- G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen
- G 0.32 Missbrauch von Berechtigungen
- G 0.38 Missbrauch personenbezogener Daten
- G 0.46 Integritätsverlust schützenswerter Informationen

- **Gefährdungen nach dem BSI-Kompendium für VK-Systeme[2]**

  - **Missbrauch von Administrations- und Wartungszugängen**: Dieses Risiko ist besonders hoch bei von Externen verwalteten Serverumgebungen. Daher bedarf es sorgfältig ausgewählter Gegenmaßnahmen (TOM), die im Vertrag zur Auftragsverarbeitung festgehalten werden müssen.

  - **Aufzeichnung, Protokollierung und Dateiablage**: Viele Systeme bieten den Anwendern die Möglichkeit der teilweise unkontrollierten Aufzeichnung der Bild- und Tondaten. Bei unbefugter Aufzeichnung kann eine Straftat nach § 201 StGB vorliegen. Protokoll- und Metadaten bieten die Gefahr der automatisierten unrechtmäßigen Weiterverarbeitung; dieses Risiko stellt insbesondere eine Verletzung der Gewährleistungsziele Vertraulichkeit und Datenminimierung dar.

  - **Zusätzliche Funktionen** in VK-Systemen, die z. B. über Schnittstellen oder Plugins insbesondere aus dem Umfeld von Büroanwendungsprogrammen, Kalendern und E-Mail-Clients bereitgestellt werden, oder die teils auch kleinteilige Anwesenheitskontrolle von Beschäftigten ermöglichen würden, bergen die Gefahr unzulässiger Überwachung. Gleiches gilt für Funktionen, die eine Aufmerksamkeitskontrolle ermöglichen, für die die Erforderlichkeit allerdings explizit begründet sein muss.

  - **Auswirkungen von VK-Systemen auf vorhandene Verfahren und auf die Netzsicherheit:**
    Gefährdungen durch zusätzlich nach außen offene Ports, eingesetzte Netzwerk-Protokolle, fehlende oder unsachgemäße Implementierung von Transportverschlüsselung und Ende-zu-Ende-Verschlüsselung (E2EE); hier ist

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/elementare_gefaehrdungen/elementare_Gefaehrungen_Uebersicht_node.html

[2] „IT-Grundschutz-Kompendium - Edition 2019“, Februar 2009, abrufbar unter:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Kompendium-Videokonferenzsysteme.pdf bzw.
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/itgrundschutzKompendium_node.html

eine individuelle kritische Risikobewertung der gesamten Netzarchitektur erforderlich, um angemessene TOM zu bestimmen

- **Kollaboration/Dokumentensharing:** Die Möglichkeiten zu Präsentation und Dateiaustausch und gemeinsamer Bearbeitung bergen die Gefahr, dass Daten nicht gelöscht werden oder in eine (unzulässige) Archivierung nach dem Ende der Konferenz transferiert werden. Hierbei kommt dem automatischen Löschen von temporär entstehenden Daten besondere Bedeutung zu. Sofern eine Archivierung zulässig oder verpflichtend ist (z. B. Videoaufzeichnung eines Authentifizierungsprozesses per Video-Identverfahren), sind dafür explizite Archivierungs- und Löschkonzepte notwendig.

- Bei der Auswahl des Videokonferenzsystems kommen nur die Produkte in Frage, die die allgemein festgestellten Anforderungen erfüllen. **Proprietäre Videokonferenzsysteme** weisen aber eigene, nicht quelloffene Entwicklungs-Standards (closed source) und Protokolle auf, zu denen Informationen über die spezifischen Risiken fehlen oder unvollständig zugänglich sind. Daher können Maßnahmen nicht explizit empfohlen werden, solange dafür keine belastbaren Tests von unabhängiger Seite vorliegen. Verantwortliche werden regelmäßig mit der gleichen Problematik konfrontiert sein. Solange die Risiken im Einzelfall nicht valide eingeschätzt werden können, ist vor dem Hintergrund des Art. 25 DS-GVO ausdrücklich vom Einsatz der jeweiligen proprietären (Closed Source) Systeme abzuraten. Etwas anderes gilt, wenn der Hersteller **umfassende belastbare Unterlagen** bereitstellt, die eine wirksame Umsetzung der Vorgaben des Art. 25 DS-GVO durch den Verantwortlichen ermöglichen.

- Zentrale Frage des Videokonferenzsystems ist die Auswahl der eingesetzten **Netzprotokolle mit unterschiedlichen Vorteilen und Gefährdungen**: Wer den Einsatz von Systemen erwägt, die auf den zwar offenen, aber älteren Telekommunikations-Protokollen (z. B. das Session Initiation Protocol (SIP)3 oder das H.323-Protokoll4 und andere) aufsetzen, sollte die entsprechende Anwendbarkeit der vorliegenden Hinweise auf solche Lösungen prüfen und ggf. sinngemäß angepasst bei der Risikobewertung berücksichtigen.
  Der Einsatz von Plattformen mit dem WebRTC-Standard5 und entsprechender Programmierschnittstelle (API) hat dagegen den Vorteil, dass diese aus dem Webumfeld stammen und von Seiten des Clients am einfachsten einsetzbar sind, da sie von aktuellen Browsern ohne die Installation weiterer Software unterstützt werden.

- Insbesondere klassische Videokonferenzsysteme beinhalten typische Funktionen von Telefonkonferenzanlagen. Die Gefährdungslage vererbt sich daher aus dem Baustein NET.4.1 TK-Anlagen des IT-Grundschutz-Kompendiums (siehe [BSI

[3] Das Session Initiation Protocol (SIP) ist ein Netzprotokoll zum Aufbau, zur Steuerung und zum Abbau einer Kommunikationssitzung zwischen zwei und mehr Teilnehmern, insb. genutzt bei IP-Telefonie, spezifiziert im RFC 3261 der IETF, abrufbar unter https://tools.ietf.org/html/rfc3261.
[4] Der H.323-Protokoll-Standard ist eine Empfehlung der Internationalen Fernmeldeunion (UN-Sonderorganisation) ITU-T, abrufbar unter https://www.itu.int/rec/T-REC-H.323/en; er basiert auf dem ISDN-Protokoll Q.931 und wird mit sog. Gatekeeper-Geräten zwischen IP-Netz und Telefonnetz umgesetzt.
[5] WebRTC (Web Real-Time Communication) ist ein offener Standard des W3C (https://w3c.dfki.de/), abrufbar unter https://webrtc.org/ und definiert eine Sammlung von Kommunikationsprotokollen und Programmierschnittstellen (API), die Echtzeitkommunikation über Rechner-Rechner-Verbindungen (peer to peer) und damit auch Videokonferenzen und andere Kollaboration von Browser zu Browser ermöglichen.

GSK-2019][6])

- Da moderne Videokonferenzsysteme die Signalisierung und die Medienströme mit ähnlichen Mitteln übertragen, wie es bei Voice over IP (VoIP) der Fall ist, vererbt sich auch hier die Gefährdungslage des Bausteins NET.4.1 TK-Anlagen für Telekommunikationsanlagen).

- Die Gefährdungen für mit dem Internet verbundene Komponenten eines Videokonferenzsystems, z. B. eine evtl. gekoppelte Sprachsteuerung, finden sich im relevanten Baustein SYS.4.4 Allgemeines IoT-Gerät (Internet of Things).

- Gefährdungen beim Einsatz privater Endgeräte (BYOD): siehe Frage 18

16. Gibt es typische oder generelle technische und organisatorische Maßnahmen, für ein datenschutzkonformes Videokonferenzsystem?

Ja, aber diese sind für sich allein genommen nicht ausreichend, sondern müssen angepasst und ergänzt werden.

Diese angepasste Betrachtung, welche Maßnahmen wirksam, geeignet und angemessen sind, schreibt die DS-GVO durch Art. 5, 24 Abs. 1, 25 Abs. 1 und 32 DS-GVO vor. (Vgl. hierzu die methodische Vorgehensweise in Frage 14)

Im Einzelnen spielen bei der Eignung von TOM folgende Kriterien bei der Auswahl eines Dienstleisters oder eines lizenzierten Produktes eine Rolle:

- Verschlüsselte Übertragung (vgl. Fragen 5 und 15)
- Auswahloptionen für datenschutzfreundliche Voreinstellungen
- Freigaben nur mit Zustimmung
- Keine Datennutzung des Anbieters für eigene Zwecke; kein Profiling der Konferenzteilnehmer
- Löschung von Protokollen und Aufzeichnungen, sobald sie nicht mehr erforderlich sind
- Blurr Möglichkeiten (um den Hintergrund unkenntlich zu machen)
- Zugangsbeschränkungen durch Log-in oder durch Erfordernis einer Einladung durch den Organisator, damit nicht jeder beliebige Nutzer an der Konferenz teilnehmen kann
- Informationspflichten und Gewährleistung von Betroffenenrechten

Generische TOM für Videokonferenzsysteme (nicht abschließend):

- Zu betrachten sind der Client des Senders, der Transportweg zum Server, der Server und der Transportweg zum Empfänger sowohl hinsichtlich der Verkehrsdaten als auch der Inhaltsdaten. Ein Risiko geht zwar auch vom Client des Empfängers aus, jedoch entzieht sich dieser dem Verantwortungsbereich des Verantwortlichen. Ggf. muss jedoch der Verantwortliche berücksichtigen, ob die

[6] [BSI GSK-2019] „IT-Grundschutz-Kompendium - Edition 2019“, Februar 2009, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/itgrundschutzKompendium_node.html

Risiken eines fremden Clients Vorkehrungen erfordern, diese wahlweise durch Einhalten bestimmter technischer Spezifikationen (z. B. Softwareversion mit Mindeststand, Schutzmaßnahmen in Form von Malwareabwehr etc.) oder Verweigerung der Verbindung zu behandeln.

- **Zugriff auf die Kommunikationsdaten** auf dem Transportweg oder auf dem Server:
  Bei besonders schutzwürdigen Daten, insbesondere bei Vorliegen eines hohen Risikos der Verarbeitung, müssen geeignete technische Implementierungen des jeweiligen Dienstes sicherstellen, dass zentrale Server oder anderweitig beteiligte Instanzen keine Einsicht in die übermittelten Verbindungsdaten erlangen können. Zur **Transportverschlüsselung** und sicheren **Ende-zu-Ende-Verschlüsselung** (End-to-End-Encryption, E2EE) der Inhaltsdaten siehe Frage 5.
- Für die **Endanwendungen** der Videokonferenzsysteme und der Plattformen, auf denen sie betrieben werden, gilt es insbesondere den Baustein "SYS: IT-Systeme" des IT-Grundschutzes[7] und die dort beschriebenen Gefährdungen bei der Wahl der Maßnahmen zu beachten. Resultat ist ein zusätzlich zu berücksichtigendes Maßnahmenbündel aus dem Grundschutz für IT-Systeme

- **Verzicht auf nicht erforderliche Funktionalitäten**: Die Verpflichtung zum Abschalten entbehrlicher Zusatzfunktionen ergibt sich bereits aus dem Gewährleistungsziel der Datenminimierung und Zweckbindung. Weitere Hinweise finden sich im IT-Grundschutz unter "SYS 1.1.A6".[8]
  Maßnahme: Ggf. deklarativer (dokumentierter) und wirksamer Ausschluss von Funktionen, die nicht dem Verarbeitungszweck dienen durch Implementierung oder Konfigurierung

- Es ist ein auf das verwendete Videokonferenzsystem zugeschnittenes **Datensicherungs**-[9] und **Archivierungskonzept**[10] zu erstellen bzw. ein bestehendes Konzept zu ergänzen. So muss im Datensicherungs- bzw. Archivierungskonzept festgelegt werden, welche Daten (wie beispielsweise Chatprotokolle, Videoaufzeichnungen oder Konfigurationsdaten) zur Sicherung bzw. Archivierung wie, wann und wie lange gespeichert werden sollen. Außerdem muss ein technischer bzw. organisatorischer Prozess existieren, der eine rasche Reintegration der Daten ermöglicht. Insbesondere ist die rechtliche Grundlage für die Verarbeitung der personenbezogenen Daten zu nennen, hieraus resultiert auch die Notwendigkeit zur Erstellung eines **Löschkonzepts**

- **Transparenz zum Produkt:** Eine Grundlage sind bei Videokonferenzsystemen dokumentierte Aussagen über die technischen Implementierungen, die eingesetzten Standards, Software-Bibliotheken und Lizenzen vom Hersteller und Dienstleister. Zu den Informationspflichten ggü. den Nutzenden vgl. Frage 6.

---

[7] BSI-IT-Grundschutz-.Kompendium Baustein „SYS: IT-Systeme“:
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/SYS/SYS_Uebersicht_node.html

[8] BSI a.a.O. Baustein SYS.1.1.A6:
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/SYS/SYS_1_1_Allgemeiner_Server.html

[9] CON.3: Datensicherungskonzept, in: BSI, IT-Grundschutz-Kompendium, 2. Edition 2019.

[10] OPS.1.2.2. Archivierung, in: BSI, IT-Grundschutz-Kompendium, 2. Edition 2019.

- **Sichere Nutzerverwaltung und Konfiguration**: Bei Lösungen für eine größere Nutzerzahl wird die Berechtigungsverwaltung regelmäßig über einen unternehmensweiten Verzeichnisdienst realisiert. Der Zugang zu Konferenzräumen ist durch zusätzliches Wissen (Kennwort, PIN) zu beschränken. Werden Konferenzen über Terminverwaltungssysteme geplant, ist sicherzustellen, dass Kennworte oder PINs möglichst nicht im Klartext darüber verteilt werden. Außerdem sollte der Konferenzleiter die Möglichkeit haben, die Teilnehmenden zur Teilnahme zuzulassen.

- **Rollen und Rechte**: Für die Sicherheit beim Zugriff auf verarbeitete personenbezogene Daten muss ein Rollen- und Berechtigungskonzept erstellt werden. Soweit dies bereits besteht, ist es um die Anwendung „Videokonferenzsystem“ zu ergänzen. Neben den Rollen des Administrators (technisch) und dem Teilnehmenden sollte in Videokonferenzsystemen für größere Teilnehmerzahlen ein Moderator/Organisator definiert und besetzt werden, der Berechtigungen für die Gesprächsleitung und unterstützende technische Funktionen für die Gesprächsdurchführung erhält. Der Moderator sollte anderen Teilnehmenden den Zutritt in die Konferenz gestatten sowie sie stummschalten und entfernen können.

- **Nutzerauthentisierung:** An einer Videokonferenzsitzung dürfen nur Berechtigte teilnehmen und auf die Ressourcen zugreifen können. Bei speziellen Anwendungsfällen, die eine vorherige Identifikation der Nutzerinnen und Nutzer erfordern, müssen geeignete Verfahren implementiert sein, um deren Authentizität nachvollziehen zu können. Grundsätzlich sollten Videokonferenzsysteme Administratoren/Gruppenleitern die Möglichkeit bieten, (passwort-) geschützte Konferenzen zu erstellen

- **Automatisierte Auswertung v**on Konferenzinhalten: Funktionen wie das Einblenden von Namen auf der Grundlage von Gesichtserkennung, Aufmerksamkeitsanalysen o. ä. (hierunter fallen nicht Funktionen, die lediglich bei Erkennung des Sprechers mittels Mikrofon- und Audio-Zuordnung den Fenster-Fokus auf den Sprecher legen) sind ohne ausdrückliche Einwilligung des Betroffenen bzw. Betriebs- oder Dienstvereinbarung bei abhängig Beschäftigten zu unterbinden. Gleiches gilt für Zusatzfunktionen wie Übersetzungsdienste, Diktiersysteme, Sprachsteuerung etc.

- **Absicherung der Endgeräteanwendungen**: In der Vergangenheit hat es wiederholt Probleme mit einzelnen Produkten gegeben, die auf dem Endgerät zusammen mit dem Konferenzclient einen Webserver installiert haben, der unzureichend abgesichert wurde und von außen angreifbar war. Daher muss eine Webserver-Freigabe unterbunden werden. Es muss zudem sichergestellt sein, dass solche zusätzlichen Komponenten abgeschaltet sind, wenn der Konferenzclient nicht in Betrieb ist.

- **Die automatische Annahme von Konferenzanfragen** ist durch Konfiguration (ggf. entsprechende Produktauswahl) zu unterbinden, da die Gefahr einer unbefugten akustischen und visuellen Überwachung besteht.

- Sofern interne **Kameras** von Geräten genutzt werden, sollte bei der Standardkonfiguration durch den Administrator von den mechanischen oder BIOS-basierten Möglichkeiten, Kamera und Mikrofon außerhalb von Konferenzen zu deaktivieren, Gebrauch gemacht werden und durch Anpassung der Security-Policy

manifestiert werden. Die Inbetriebnahme von Mikrofon und Kamera sollte optisch am Gerät, zumindest aber in der Anwendung deutlich sichtbar signalisiert werden.

- **Administrationsanforderungen**, Installation und Softwareaktualisierung:
  Das Videokonferenzsystem ist in regelmäßigen Abständen auf Schwachstellen und bereitliegende Patches zu überprüfen. Die Patches sollten auch bezüglich ihrer Authentizität und Vertraulichkeit überprüft werden und zeitnah installiert werden. Vor dem Start der Produktivphase des Systems mit den installierten Patches sollten die Patches innerhalb einer Test-Umgebung getestet werden. Technische Schwachstellen und sonstige Sicherheitslücken in Videokonferenzsystemen müssen in einem angemessenen Zeitraum behoben werden. Dies kann entweder direkt durch den Hersteller oder den Betreiber des Dienstes oder den Verantwortlichen erfolgen.
  Sofern webbasierte Videokonferenzsysteme genutzt werden, muss für einen sicheren Betrieb stets eine aktuelle Webbrowser-Version eingesetzt werden.
  Der Einsatz gehärteter oder teilgehärteter Systeme sollte erwogen werden, etwa durch Reduzierung der Apps und Funktionen auf das Nötige. Zudem kann dies durch das Prinzip des application containment erfolgen, bei dem Anwendungen wie der Browser in einem isolierten Kontext, also in einer micro-virtuellen Maschine (Micro-VM) und damit im Fall von Angriffen vom Betriebssystem abgekapselt laufen. Ein Schaden durch ein evtl. eingenistetes Schadprogramm beim Browsen oder durch andere Kommunikationsverbindungen - z. B. beim Video-Conferencing - bleibt dadurch immer auf die jeweilige Micro-VM beschränkt und befällt nicht das gesamte System.

- **Penetrationstest**: Ein Videokonferenzsystem muss bei der Einrichtung und im laufenden Betrieb auf Schwachstellen untersucht werden. Hierbei müssen auch Risiken der künstlichen Intelligenz (z. B. digitale Assistenten, smarte Lautsprecher im Homeoffice, die auf Schlüsselworte reagieren) beachtet werden.

Ergänzende TOM lassen sich zusätzlich aus folgenden Quellen ableiten:

- Standard-Datenschutzmodell (SDM) - generische Maßnahmen im SDM Kapitel 7[11] sowie SDM –Maßnahmenkatalog (erste Bausteine von einzelnen Aufsichtsbehörden in Erprobung) BSI - IT-Grundschutz-Kompendium und ggf. BSI-Grundschutzmaßnahmen (alt)
- ISO 27001 generische Maßnahmen[12]
- IT-Grundschutz-Profile[13]

[11] Das Standard-Datenschutzmodell - Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele, Version 2.0b, von der 99. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder am 17. April 2020 beschlossen, abrufbar unter: https://lfd.niedersachsen.de/startseite/themen/technik_und_organisation/orientierungshilfen_und_handlungsempfehlungen/standard_datenschutzmodell/standard-datenschutzmodell-139069.html

[12] Standard ISO 27001 “Information technology — Security techniques — Information security management systems — Requirements” von der International Organization for Standardization, abrufbar: https://www.iso.org/standard/54534.html

[13] IT-Grundschutz-Profile gemäß den BSI-Spezifikationen, vgl. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Profile/Strukturbeschreibung.pdf?__blob=publicationFile&v=6 und https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzProfile/Profile/itgrundschutzProfile_Profile.html

Zusätzlich kommen Ergänzungen durch **individuelle eigene TOM zur jeweiligen Anwendung** in Betracht.

Im Ergebnis der Prüfung, welche technischen und organisatorischen Maßnahmen (TOM) wirksam, geeignet und angemessen sind, wird deutlich, dass es zwar typische TOM gibt, diese jedoch in den allermeisten Fällen durch individuelle TOM ergänzt werden müssen. Der Verantwortlichen muss einen **Katalog der TOM für die individuelle Videokonferenzlösung erstellen**, die er verantwortet. Dieser enthält detaillierte Beschreibungen aller zu treffenden technischen Maßnahmen sowie die für die Umsetzung und die Kontrolle verantwortliche Rolle (und Personen). Zudem beschreibt er, welche organisatorischen Regelungen für die sichere Einführung bzw. den weiteren Betrieb der betrachteten Verarbeitungstätigkeit erforderlich sind.

Beschäftigtendatenschutz

17. Kann mein Arbeitgeber/meine Arbeitgeberin/meine Dienststelle mich zwingen, Videokonferenzsysteme zu beruflichen/dienstlichen Zwecken zu nutzen?

Ja, der Arbeitgeber/die Arbeitgeberin hat ein „Weisungsrecht“ und die Dienststelle ein „Direktionsrecht“.

Grundsätzlich darf der Arbeitgeber/die Arbeitgeberin Inhalt, Durchführung, Zeit und Ort der Tätigkeit bestimmen: Somit auch, dass Beschäftigte im Rahmen ihrer Tätigkeit ein Videokonferenzsystem nutzen. Etwas anderes kann sich aber aus einem individuellen Arbeitsvertrag, Betriebsbestimmungen, einem Tarifvertrag oder gesetzlichen Bestimmungen ergeben.

Der Arbeitgeber/die Arbeitgeberin hat bei seinem/ihrem Weisungsrecht auch Ermessen. Dabei muss er/sie zum Beispiel auch auf Behinderungen der Beschäftigten Rücksicht nehmen (siehe hierzu zum Beispiel § 315 BGB). So kann gegebenenfalls je nach Behinderung die Anweisung unzulässig sein, ein Videokonferenzsystem zu nutzen.

Beamtinnen und Beamte haben eine Folgepflicht und müssen auf Weisung ihres/ihrer Vorgesetzten ein Videokonferenzsystem nutzen (§ 35 Beamtenstatusgesetz). Für Angestellte des öffentlichen Dienstes gelten dieselben Bedingungen wie für Beschäftigte.

18. Kann mein Arbeitgeber/meine Arbeitgeberin/meine Dienststelle mich zwingen, meine privaten Endgeräte zu nutzen, um Videokonferenzen durchzuführen?

Nein.

Private Endgeräte, wie zum Beispiel Smartphones, Tablets, Notebooks oder Desktop-PC, gehören zur Privatsphäre der Beschäftigten. Der Arbeitgeber/die Arbeitgeberin beziehungsweise die Dienststelle hat gegenüber den Beschäftigten keinen Anspruch darauf, dass diese ihre privaten Geräte für die Erfüllung der Arbeitsleistung oder für dienstliche Zwecke nutzen. Jedoch können die Beschäftigten diese freiwillig zur Verfügung stellen (Prinzip des „Bring your own device“, BYOD).

Sofern sich Arbeitgeber/Arbeitgeberin/Dienststelle und Beschäftigte darauf verständigen, private Endgeräte zu beruflichen/dienstlichen Zwecken zu nutzen, ist dies aus datenschutzrechtlicher Sicht nur möglich, wenn sichergestellt ist, dass auf dem Gerät der Beschäftigten die jeweils geltenden datenschutzrechtlichen Erfordernisse gewährleistet sind und bleiben.

So muss beispielsweise durch entsprechende Maßnahmen eine Verantwortlichkeit der Beschäftigten im Sinne von Art. 4 Nummer 7 der DS-GVO für die entsprechenden Datenverarbeitungen ausgeschlossen sein. Auch ist eine unzulässige Verhaltens- und Leistungskontrolle der Beschäftigten oder ein rechtwidriger Zugriff auf nicht-dienstliche personenbezogenen Daten auszuschließen.

Im Hinblick auf die dafür vorzusehenden technischen und organisatorischen Maßnahmen ist besonders auf Folgendes zu achten:

Gefährdungen können von privaten Endgeräten selbst ausgehen. Dazu gehören insbesondere folgende Faktoren:

- Betriebssysteme, die keine Updates und Patches erhalten, weil Hersteller diese für alte Geräte nicht mehr anbieten oder Nutzer die verfügbaren Updates und Patches nicht installieren;
- Geräte, auf denen keine oder kein aktueller Schutz gegen Malware (z. B. Viren, Trojaner, Keylogger, Spyware, Adware, Ransomware) installiert ist sowie
- Geräte mit nicht den Risiken der Videokonferenz angemessenen Voreinstellungen (z. B. wenn in den Default-Einstellung Optionen zu Ungunsten von Betroffenen vorweggenommen worden sind, die auch nicht überprüft und bewusst an die Risiken angepasst wurden).

Als weitere Gefährdung gilt der mögliche Zugriff durch Dritte: Hier muss geprüft werden, welche Konflikte im Rahmen einer Datenschutzkontrolle oder der Bekämpfung eines Sicherheitsvorfalles beim Zugriff auf private Geräte auftreten können, wenn die Geräte nicht nur von den Beschäftigten, sondern auch von deren Haushaltsangehörigen und sonstigen Dritten genutzt werden können. Zusätzlich können Gefährdungen aufgrund des Zuganges durch Unbefugte in unterschiedlicher Ausprägung ausgehen, die auf Umstände in der Raumanordnung (z. B. leichter Zugang innerhalb der Wohnung) und im baulichen Zustand (z. B. einbruchsgefährdete Fenster und Türen) begründet liegen. Diese Gefährdungen können sich insbesondere gegen die Vertraulichkeit und Integrität der personenbezogenen Daten richten. Es liegt in der Entscheidungshoheit des Arbeitnehmers, seine (private) Hard- und Software sowie die auf den Geräten verarbeiteten personenbezogenen Daten zu schützen.

Allen Gefährdungen sind geeignete und unter Berücksichtigung von Art, Umfang und Zweck der Verarbeitung, des Standes der Technik, der Implementierungskosten sowie der Risiken (abhängig von Schadenshöhe und Eintrittswahrscheinlichkeit) entsprechend angemessene **technische und organisatorische Maßnahmen** entgegenzusetzen, also je nach Risikowert (gering, normal oder hoch) mindestens (nicht abschließend):

- Betriebssysteme auf dem aktuellen Update- und Patchstand halten, keine veralteten Geräte nutzen.
- Aktuellen Malwareschutz installieren und auf dem aktuellen Stand halten.
- Voreinstellungen wählen, die eine strikte Trennung zwischen der Videokonferenzsoftware und anderen Anwendungen sowie privaten Daten sicherstellen.
- Nicht mit einem Nutzerkonto mit Administrationsrechten in die Konferenz einwählen.
- Räume nutzen, die vor Fremdeinfluss anderer Personen geschützt sind (z. B. abschließbares Arbeitszimmer oder Büro).

19. Kann mein Arbeitgeber/meine Arbeitgeberin/meine Dienststelle mich zwingen, mein Profilbild im Videokonferenzsystem einzustellen?

Nein. Der Arbeitgeber/die Arbeitgeberin oder Dienststelle sollte es den Beschäftigten stets freistellen, ihr Profilbild im Konferenzsystem hochzuladen und zu entscheiden, ob dieses für alle Konferenzteilnehmenden sichtbar ist.

Denn die Veröffentlichung von Personenfotografien (personenbezogene Daten im Sinne von Art. 4 Nummer 1 DS-GVO) kann nur auf eine freiwillig abgegebene Einwilligung der abgebildeten Person (Betroffener) gestützt werden (siehe Art. 6 Abs. 1 lit. a DS-GVO).

An die Rechtmäßigkeit der Einwilligung von Beschäftigten sind dabei besondere Anforderungen zu stellen, weil zwischen dem Arbeitgeber/der Arbeitgeberin und den Beschäftigten ein Über-/ Unterordnungsverhältnis besteht (siehe Erwägungsgrund 43 zur DS-GVO). Freiwilligkeit kann insbesondere dann vorliegen, wenn für die Beschäftigten ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber/Arbeitgeberin und Beschäftigte gleichgelagerte Interessen verfolgen (siehe hierzu § 26 Abs. 2 Bundesdatenschutzgesetz – BDSG). Freiwillig ist die Einwilligung vor allem dann, wenn die Betroffenen sie verweigern können, ohne Nachteile zu erleiden (z. B. ohne von der Videokonferenz ausgeschlossen zu werden).

Arbeitgeber/Arbeitgeberin/Dienststelle müssen ihre Beschäftigten über die Verarbeitung ihrer personenbezogenen Daten informieren (Art. 12f. DS-GVO). Dazu zählt natürlich auch, dass die Verarbeitung der personenbezogenen Daten mittels eines Videokonferenzsystems erfolgt und gegebenenfalls, inwieweit die personenbezogenen Daten an Dritte und/oder Drittländer übermittelt werden.

20. Kann mein Arbeitgeber/meine Arbeitgeberin/meine Dienststelle mich zwingen, zusätzlich zum Mikrofon die Kamera im Videokonferenzsystem zu starten?

Nein, siehe dazu auch die Ausführungen unter Frage 4 zur Einwilligung.

Grundsätzlich dürfen Bilder/Videos von Beschäftigten im Rahmen von Videokonferenzsystemen nur dann verarbeitet werden, wenn dies für die Arbeitsleistung erforderlich ist (§ 26 Abs. 1 BDSG, § 88 Abs. 1 Satz 2 NBG in Verbindung mit Art. 5 Abs. 1 Buchstabe c DS-GVO). Für eine Konferenz ist es meistens nicht notwendig, dass die teilnehmende Person im Bild zu sehen ist. Maßgeblich ist im Allgemeinen das gesprochene Wort. In bestimmten Situationen kann es aber auch erforderlich sein, Mimik und Gestik der agierenden Personen zu erfassen, zum Beispiel im Rahmen eines Personalauswahlverfahrens oder in Sicherheitsbereichen.

In fast allen Videokonferenzsystemen, die auf dem Markt sind, kann die oder der Betroffene selbst einstellen, ob die Kameraaufnahme für alle Konferenzteilnehmenden freigegeben wird. Es wird empfohlen, dass der Arbeitgeber/die Arbeitgeberin /Dienststelle festlegt, dass jede oder jeder Beschäftigte durch Start der Kamera selbst bestimmen kann, ob Aufnahmen an die anderen Konferenzteilnehmenden übermittelt werden.

21. Kann mein Arbeitgeber/meine Arbeitgeberin/meine Dienststelle mich zwingen, die Anzeige meiner Verfügbarkeit gegenüber allen Beschäftigten freizugeben?

Grundsätzlich nein, es sei denn, die Erforderlichkeit hierfür wird vom Arbeitgeber/von der Arbeitgeberin/von der Dienststelle ausreichend begründet. Das könnte etwa bei Notdiensten wegen der hohen Eilbedürftigkeit der Fall sein.

Das Bundesverfassungsgericht hat im sogenannten „Volkszählungsurteil" vom 15. Dezember 1983 ausgeführt, dass „die Datenverarbeitung auf das unbedingt notwendige Maß begrenzt werden“ muss. Demnach ist eine Datenverarbeitung nur erforderlich, „wenn die jeweilige Aufgabe ohne das konkrete Datum nicht oder nicht vollständig erfüllt werden könnte. Es reicht somit nicht aus, wenn die Datenverarbeitung für die Aufgabenwahrnehmung lediglich dienlich oder nützlich ist, zur Abrundung des Bildes beiträgt oder Hintergrundinformationen liefert.“

Der Arbeitgeber/die Arbeitgeberin/die Dienststelle ist im Rahmen der Nachweispflicht nach Art. 5 Abs. 2 DS-GVO gehalten, die Beweggründe für eine Anweisung sowie die vorgenommene Interessenabwägung schriftlich darzulegen.

Bildungsbereich

22. Welche Besonderheiten gelten beim Einsatz und bei der Durchführung von Videokonferenzen im Bildungsbereich?

Videokonferenzen werden gegenwärtig insbesondere im Bildungsbereich (Schulen, Hochschulen, sonstige Bildungseinrichtungen, wie z.B. Studienkollegs) zum mobilen Lernen eingesetzt. Sofern die Landesgesetze entsprechende Rechtsgrundlagen zum Einsatz digitaler Lehr- und Lernmittel vorsehen (so z. B. § 31 Abs. 5 Nds. SchulG für den Schulbereich) kann auch die damit unmittelbar verbundene Datenverarbeitung (insbes. die Verarbeitung der IP-Adresse) grundsätzlich hierauf gestützt werden, sofern zugleich die weiteren im Schulgesetz vorgesehenen organisationsrechtlichen Beteiligungserfordernisse, wie die Zustimmung der Schulleitung und die Einbindung des Schulelternrats bzw. der Klassenelternschaft, eingehalten werden.

Allerdings werden in der Praxis regelmäßig cloudbasierte Videokonferenzsysteme eingesetzt, bei denen sich die Verantwortlichen externer Dienstleister bedienen. Meist ist es dabei nötig, dass das Lehrpersonal, die Schülerinnen und Schüler und ggf. deren Erziehungsberechtigte bei der Installation und erstmaligen Nutzung der jeweiligen Programme auf den eigenen Endgeräten in die Nutzungsbedingungen des externen Dienstleisters einwilligen. Da es keine Rechtspflicht zur Einwilligung in solche Nutzungsbedingungen Dritter gibt, kann der Einsatz von Videokonferenzsystemen im Bildungsbereich zumindest in dieser Variante nur auf der Basis von Einwilligungen eingesetzt und nicht verpflichtend vorgegeben werden. Die Anforderungen an die Freiwilligkeit der Einwilligungen (vgl. EG 43 DS-GVO) sind dabei zu beachten. Insbesondere für Schülerinnen und Schüler, die über keine einsatzfähigen Endgeräte verfügen oder sich den Nutzungsbedingungen eines Anbieters nicht unterwerfen wollen, müssen stets Alternativen vorgehalten werden. Zudem muss die jeweilige Bildungseinrichtung als datenschutzrechtlich Verantwortlicher die Nutzungsbedingungen einer rechtlichen Prüfung unterziehen.

Gesundheitsbereich

23. Welche Besonderheiten gelten für Videokonferenzen im Gesundheitsbereich?

Die Nutzung von Videokonferenzsystemen ist zulässig, wenn Patientinnen und Patienten einen ärztlichen Kontakt auf diesem Weg wünschen. Außerdem müssen sie nach entsprechender Information über die Voraussetzungen der Teilnahme und der Datenverarbeitung ihre Einwilligung erteilt haben.

Die Nutzung telemedizinischer Anwendungen darf nicht zu einer rechtlichen oder faktischen Verschlechterung der Patientenrechte führen.

Eine Videosprechstunde im Gesundheitswesen muss mindestens folgende Punkte erfüllen:

- Die Videosprechstunde muss in Räumen stattfinden, die Privatsphäre bieten. Außerdem müssen die eingesetzte Technik und die elektronische Datenübertragung eine angemessene Kommunikation gewährleisten, wie sie auch bei einem Gespräch vor Ort möglich wäre.
- Die Videosprechstunde muss vertraulich und störungsfrei verlaufen - wie eine normale Sprechstunde auch. So darf die Videosprechstunde beispielsweise von niemandem aufgezeichnet werden, auch nicht von der Patientin oder dem Patienten.
- Zum Nachweis der Identität muss der Klarname der Patientin oder des Patienten für die Ärztin oder den Arzt erkennbar sein.
- Die Videosprechstunde muss frei von Werbung sein.

Weitere Informationen bietet die Internetseite der Kassenärztlichen Bundesvereinigung: https://www.kbv.de/html/videosprechstunde.php

Kommunaler Bereich

24. Gibt es Besonderheiten zum Einsatz von Videokonferenzsystemen im Kommunalbereich?

Der Einsatz von Videokonferenzsystemen kommt regelmäßig nur bei den freiwilligen kommunalen Angeboten, wie z.B. bei Musikschulen, auf der Basis von Einwilligungen der Betroffenen in Betracht.

Sitzungen der kommunalen Vertretungsorgane setzen grundsätzlich die körperliche Anwesenheit der Beteiligten voraus. Zur Bewältigung einer epidemischen Lage kann für Sitzungen Videokonferenztechnik eingesetzt werden, sofern die oder der Hauptverwaltungsbeamte im Benehmen mit der oder dem Vorsitzenden die Möglichkeit in der Ladung anordnet (§ 182 Abs. 2 Nr. 3 NKomVG).

Sozialbereich

25. Was gilt für Videokonferenzen im Sozialbereich?

Gegenwärtig kommen Videokonferenzen wegen der gebotenen pandemiebedingten Reduzierung physischer Kontakte im Bereich der Kinder- und Jugendhilfe zum Einsatz, um die bestehenden Beratungsangebote weiter vorhalten zu können. Voraussetzung ist, dass die ratsuchende Person bzw. deren Vertretung ihre Einwilligung in den Einsatz der Videokonferenzen erteilt hat.

Datenschutz-Folgenabschätzung

26. Muss für den Einsatz von Videokonferenzen eine Datenschutz-Folgenabschätzung durchgeführt werden?

Vor der Nutzung eines Videokonferenzsystems muss der Verantwortliche prüfen, ob es einer Datenschutz-Folgenabschätzung (DSFA) nach Art. 35 DS-GVO bedarf. Dabei sind die von den Aufsichtsbehörden veröffentlichten Listen heranzuziehen. Diese führen Verarbeitungsvorgänge auf, für die eine DSFA in jedem Fall erforderlich ist (sogenannte Muss-Listen). Außerdem sollten die Leitlinien des Europäischen Datenschutzausschusses zur Datenschutz-Folgenabschätzung mit den neun Kriterien für ein voraussichtlich hohes Risiko berücksichtigt werden. Bei der Prüfung ist immer der konkrete Einsatzzweck des Videokonferenzsystems zu berücksichtigen, da von diesem die Risikoeinschätzung maßgeblich abhängt.

Möchte ein Verantwortlicher beispielsweise Auswahlgespräche in einem Bewerbungsverfahren über ein Videokonferenzsystem durchführen, sind folgende Prüfungspunkte besonders relevant:

- Wird eine automatisierte Auswertung von Video- oder Audioaufnahmen zur Bewertung der Persönlichkeit der betroffenen Personen durchgeführt, ist hierfür eine DSFA nach Nummer 13 der Muss-Liste der Verarbeitungstätigkeiten durchzuführen.
- Ist dies nicht der Fall, sind die neun Kriterien für ein voraussichtlich hohes Risiko des Europäischen Datenschutzausschusses zu prüfen. Sind zwei dieser Kriterien erfüllt, dann ist eine DSFA in den meisten Fällen obligatorisch.

Bei Auswahlgesprächen über Videokonferenzsysteme sind zwei Kriterien erfüllt, weil Gegenstand des Gesprächs unter anderem vertrauliche oder höchstpersönliche Daten sein werden (Nr. 4) und es sich bei den Bewerberinnen und Bewerbern um besonders schutzbedürftige betroffene Personen handelt (Nr. 7).

Von einer DSFA kann bei Auswahlgesprächen dennoch abgesehen werden, wenn der Umfang der Verarbeitung so niedrig ist, dass kein voraussichtlich hohes Risiko vorliegt. Werden beispielsweise durch eine Behörde oder ein Unternehmen lediglich um die 50 Bewerbungsgespräche im Jahr über das Videokonferenzsystem durchgeführt, dann ist hierfür keine DSFA erforderlich, es sei denn, von dem beabsichtigten Verfahren werden noch weitere Kriterien des Europäischen Datenschutzausschusses erfüllt.

Die Landesbeauftragte für den Datenschutz Niedersachsen
Prinzenstraße 5
30159 Hannover

Telefon 0511 120-4500

Fax 0511 120-4599

E-Mail poststelle@lfd.niedersachsen.de