Gesellschaft für Datenschutz
und Datensicherheit e.V.

GDD-Praxishilfe DS-GVO XVI

Videokonferenzen und Datenschutz

INHALT

Videokonferenzen und Datenschutz

Mit der vorliegenden Praxishilfe möchte die GDD einen Beitrag zur Beseitigung bestehender Unsicherheit im Hinblick auf aktuelle datenschutzrechtliche Fragen rund um das Thema Videokonferenzen leisten. Mit einer Auswahl und Gegenüberstellung verschiedener Anbieter von Videokonferenzlösungen und der dazugehörigen Veranschaulichung datenschutzrechtlicher Aspekte, soll eine Hilfestellung für Datenschutzverantwortliche bei der Auswahl eines geeigneten Videokonferenzdienstleisters gegeben werden. Die Checkliste soll zudem die grundsätzlichen Anforderungen an Datenschutz und -sicherheit in diesem Zusammenhang veranschaulichen und einfaches „Abarbeiten" der Kriterien ermöglichen.

Hintergrund

Auf Grund der Maßnahmen zur Bekämpfung der Corona-Pandemie richten viele Unternehmen kurzfristig Telearbeitsplätze ein, so dass ihre Beschäftigten ihren arbeitsvertraglichen Pflichten auch von Zuhause nachkommen können. Um trotzdem die betriebsinterne Kommunikation sicherzustellen, setzen Unternehmen häufig sog. **Software as a Service Dienstleister (kurz: SaaS)** für Video- und Onlinekonferenzen, -Meetings oder Webinare ein. Hierbei die Vorgaben der DS-GVO einzuhalten, erhöht nicht nur das Datensicherheitsniveau in Organisationen, sondern hilft den ungeregelten Abfluss von solchen Unternehmensinformationen zu verhindern, die im internationalen Wettbewerb die eigene Wertschöpfung sichern sollen.

1. Allgemeine Punkte

Vorüberlegungen:

>> Handeln Sie vorausschauend bei der Auswahl eines Anbieters (ggf. gibt es gleich- oder höherwertige europäische Alternativen)

>> Beachten Sie etwaige Beteiligungsrechte des Betriebs- oder Personalrats (siehe. § 87 Abs. 1 Nr. 6 BetrVG bzw. § 75 Abs. 3 Nr. 17 BPersVG oder LandesPersVG)

>> Beziehen sie den Datenschutz- und falls vorhanden den IT-Sicherheitsbeauftragten mit in Ihre Überlegungen ein

>> Kann eine Videokonferenzlösung performant auf eigener Infrastruktur betrieben werden, (sog. On-Premise-Lösung), ist dies grundsätzlich ggü. einer Cloud-Variante vorzugswürdig

2. Anforderungskatalog an den Funktionsumfang von Videokonferenzlösungen

>> Vor einer Entscheidung für einen Anbieter muss aus unternehmerischer Sicht die Frage beantwortet werden, welche technischen Möglichkeiten ein Videokonferenz-Tool dem Unternehmen im Rahmen der Aufgabenerfüllung bieten muss und ob die vom jeweiligen Anbieter angebotenen Funktionen aus datenschutzrechtlicher Perspektive zwingend erforderlich sind.

>> Die Funktionen müssen bedarfsgerecht priorisiert werden, dies kann z.B. in Form einer sog. **MoSCoW-Priorisierung** erfolgen:

> **M - "Must-have"** (auf Deutsch: Muss): Essenzielle Funktionen, ohne diese kann eine Videokonferenzlösung nicht realisiert werden.

> **S – "Should-have"** (auf Deutsch: Sollte): Notwendige Funktionen, um Unternehmensaufgaben effektiv ausfüllen zu können, exakte Anforderung sind ausgestaltbar).

> **C - "Could-have"** (auf Deutsch: Könnte): Wünschenswerte Funktionen, aber eine Aufgabenerfüllung kann auch ohne diese erfolgen, spätestens hier muss genaueres Augenmerk auf die datenschutzrechtliche Erforderlichkeitsprüfung angewendet werden.

> **W – "Won't"** (auf Deutsch: Nicht): Anforderungen die aktuell aus unternehmerischen oder datenschutzrechtlichen Gründen nicht realisierbar sind. Diese werden ggf. in einen Ideenpool oder in zukünftige Anforderungslisten übernommen.

Praxishinweise:

Die Lösungen unterscheiden sich teilweise elementar in Bezug auf ihre Anforderungen an die technische Infrastruktur bei Unternehmen und Beschäftigten:

So existieren sogenannte Peer-to-peer-Lösungen (P2P) wie bspw. Jitsi und zentrale Lösungen wie bspw. Zoom. Während zentrale Lösungen die eigene Infrastruktur belasten, belasten P2P-Lösungen die Infrastruktur bei den Beschäftigten im Home-Office (Internetanschluss).

Bei einer P2P-Kommunikation läuft nur der Verbindungsaufbau über die zentrale Infrastruktur, die eigentliche inhaltliche Kommunikation läuft direkt zwischen den Kommunikationsteilnehmern. Eine P2P-Lösung entlastet den Internetzugang des Unternehmens, verlangt jedoch im Gegenzug mehr Bandbreite bei den Beschäftigten.

Konferenztools sollten bei der Verwendung von Clouddienstleistern nicht über die VPN-Verbindung laufen, wenn der VPN-Anschluss des Unternehmens stark ausgelastet ist. Sonst muss jede Videoverbindung zweimal über den Anschluss des Unternehmens. Vom Home-Office des Beschäftigten ins Unternehmen und aus dem Unternehmen zum Cloudanbieter. Nutzen mehrere Beschäftigte aus dem Unternehmen eine VC gleichzeitig, kann das zu ziemlichen hohen Anforderungen an die Bandbreite des Internetanschlusses führen.

3. Erforderlichkeitsprüfung im Hinblick auf Anwendungen und Funktionen

Sowohl bei der Anschaffung als auch beim Einsatz von Videokonferenzdiensten sollte darauf geachtet werden, dass im Hinblick auf datenschutzfreundliche Voreinstellungen und vor dem Hintergrund des Datenminimierungsprinzips (Art. 5 Abs. 1 lit. c DS-GVO), nur solche Datenverarbeitungsvorgänge stattfinden, die für die Zweckerfüllung erforderlich sind.

Hinweis: Die Erforderlichkeit sog. Screen-Sharing und Aufzeichnungsoptionen muss bei Videokonferenzen im Einzelfall hinterfragt werden, ebenso wie Tracking- und Beobachtungsfunktionen sowie automatisierte Protokolle und Transkripte. Die Zulässigkeit des Einsatzes technischer Lösungen kann aber nicht pauschal einheitlich bewertet werden, sondern muss in Abhängigkeit von der Schutzbedürftigkeit bzw. Sensibilität der jeweils zu verarbeitenden Daten bewertet werden. D.h. jede Datenverarbeitung muss in Bezug auf die eingesetzte Softwarefunktion und dem im Einzelfall verfolgten Zweck ihrer Nutzung beurteilt werden. Die Prüfung der Erforderlichkeit sollte daher auch im Sinne der sich aus Art. 5 Abs. 2 und 24 DS-GVO ergebenden Rechenschaftspflicht dokumentiert werden. Vor dem Einsatz von Videokonferenzlösungen und dem Beginn einzelner Konferenzen sollten nachfolgende Fragen gestellt werden.

>> Ist der Zweck der Datenerhebung zulässig?

>> Für welchen Zweck wird die Funktion benötigt? (Dokumentation von Vertragsabschlüssen und einzelner Vertragsbedingungen, Aufzeichnung als Gedächtnisstütze, Dokumentation von Organisationsentscheidungen, Diktate für Pressemitteilungen, Ermöglichung der Kommunikation mit Geschäftspartnern im Home-Office)

>> Ist die Funktion zur Zweckerfüllung geeignet, d.h. kann sie den Zweck überhaupt erfüllen?

>> Existieren datenschutzfreundlichere Wege, welche den Zweck in gleichem Maße erfüllen können und ebenso effektiv sind.

> Wahl einer Telefonkonferenz anstatt einer Videokonferenz, wenn es keinen Mehrwert hat, dass sich die Teilnehmer zusätzlich sehen können

> Handschriftliche Protokolle oder das notieren von Rückfragen anstatt Videoaufzeichnungen

>> Existieren keine datenschutzfreundlicheren Mittel, dann müssen entsprechende datenschutzrechtliche Schutzmaßnahmen vorgesehen werden.

Praxishinweis:

Die Kommunikation von zwei Personen kann in der Regel genauso gut als Telefonat abgewickelt werden. Bei einer größeren Zahl von Teilnehmern ist die Identifikation des Sprechenden nur auf Grund der Stimme schwieriger. Hier hilft die Videokonferenz, da es den Sprechenden im Bild zeigt. Bei geringen Bandbreiten würde zu dieser Funktionalität auch ein Standbild reichen.

Für die Nutzung von nicht zwingend erforderlichen Funktionen während einer Videokonferenz, kann unter Hinweis auf die Risiken für Rechte und Freiheiten der betroffenen Personen ggf. eine freiwillige und informierte Einwilligung seitens der Teilnehmenden eingeholt werden.

4. Auswahl eines geeigneten Anbieters anhand der Einhaltung von Betroffenenrechten gem. Art. 15 – 22 DS-GVO

Damit Betroffenenrechte eingehalten werden können, müssen dem Dienstleister entsprechende Verpflichtungen auferlegt werden, in der Regel durch einen Vertrag zur Regelung einer Auftragsdatenverarbeitung (ggf. einer gemeinsamen Verantwortlichkeit) mit entsprechendem Inhalt:

>> Der Videokonferenzanbieter muss den Auftraggeber bspw. unverzüglich darüber informieren, wenn Betroffene ihre Betroffenenrechte gegenüber dem Auftragnehmer geltend machen und dies unmittelbar den Auftraggeber betrifft.

>> Auftragnehmer müssen verpflichtet werden, den Auftraggeber bei seiner Pflicht, Anträge von Betroffenen nach Art. 12 - 23 DS-GVO zu bearbeiten, zu unterstützen, sofern der Auftraggeber die Ansprüche nicht ohne Mitwirkung erfüllen kann.

>> Auftragnehmer haben insbesondere Sorge dafür zu tragen, dass die insoweit erforderlichen Informationen unverzüglich an den Auftraggeber erteilt werden, damit dieser insbesondere seinen Pflichten aus Art. 12 Abs. 3 DS-GVO nachkommen kann.

Soweit eine Mitwirkung des Auftragnehmers für die Wahrung von Betroffenenrechten – insbesondere auf Auskunft, Berichtigung, Sperrung oder Löschung – durch den Auftraggeber erforderlich ist, müsste der Auftragnehmer die jeweils erforderlichen Maßnahmen nach Weisung des Auftraggebers treffen. Der Auftragnehmer wird den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nachzukommen.

5. Auswahl eines geeigneten Anbieters anhand der Grundprinzipien aus Art. 25 DS-GVO „Privacy-by-Design“ und „Privacy-by-Default“

Bei der Auswahl eines geeigneten und letztlich auch zuverlässigen Anbieters sollten Dienste mit möglichst datensparsamen Voreinstellungen bzw. Einstellungsmöglichkeiten („Privacy by Default“) und datenschutzfreundlicher Technikgestaltung („Privacy by Design“) gewählt werden. Diese in Art. 25 DS-GVO niedergelegten Ziele korrelieren letztlich auch mit dem Schutz von eigenen und fremden Geschäftsgeheimnissen oder sonstigen schutzwürdigen Informationen.

>> **Verschlüsselte Übertragung:** Ein Anbieter sollte Daten zwischen den einzelnen Teilnehmern verschlüsselt übertragen können, bestenfalls Ende-zu-Ende verschlüsselt, ggf. – d.h. bei nicht-sensiblen personenbezogenen bzw. geschäftlichen Daten - kann auch die Nutzung von SSL- und TLS-Protokollen ausreichenden Schutz bieten. Bei der Nutzung von Transportverschlüsselung (TLS) wird alleine der Transport durch das Internet, d.h. vom Client zum Server sowie zu ggf. weiteren Clients verschlüsselt. Beim Dienstleister besteht die theoretische Möglichkeit, auf die kurzzeitig unverschlüsselt vorliegende Kommunikation zuzugreifen.

>> **Auswahloptionen für datenschutzfreundliche Voreinstellungen:** Anbieter sollten Optionen vorsehen, um datenschutzfreundliche Voreinstellungen durch Unternehmen zu ermöglichen, wie z.B. eine Deaktivierung der Erhebung von Statistikdaten, Senden von Absturzberichten oder automatischer Transkriptionen.

>> **Freigaben nur mit Zustimmung:** Bildschirmübertragungen (Screen-Sharing/Desktop-Sharing) oder Aufzeichnungen sollten technisch nur möglich sein, wenn die Teilnehmer vorher aktiv zustimmen können.

>> **Keine Datennutzung des Anbieters für eigene Zwecke:** Ein Profiling von Teilnehmern sollte ausgeschlossen/abgeschaltet werden können. Gleichzeitig sollte die Erstellung nicht zwingend benötigter Logfiles (ggf. benötigt zur Fehlerbehebung durch den Dienstleister) unterbunden werden können. Ebenso wie die Erhebung von Daten, welche für die Erbringung des Dienstes nicht zwingend erforderlich sind, wie z.B. eine Verarbeitung für Marktforschungszwecke oder eine Werbeprofilbildung von Nutzern.

>> **Löschung von Protokollen und Aufzeichnungen:** Aufzeichnungen, Chatverläufe, Transkripte oder ausgetauschte Dateien sollten nach Gesprächsende gelöscht werden können bzw. nur so lange gespeichert werden, wie erforderlich, ggf. sollten entsprechende Löschfristen gesetzt werden können.

Praxistipp:

Empfehlen Sie Ihren Beschäftigten, alle Objekte aus dem Hintergrund zu entfernen, die die Kommunikationspartner nicht sehen sollen. Eine alte Dia-Stativ-Leinwand schafft als Sichtschutz einen neutralen Hintergrund.

>> **Blurr-Möglichkeiten:** Videokonferenz-Tools sollten die Möglichkeit bieten, den Hintergrund auszugrauen bzw. unkenntlich zu machen. Unternehmen können hiermit für mehr Datenschutz und Privatsphäre bei den Mitarbeitern sorgen.

>> **Zugangsbeschränkungen:** Videokonferenzen dürfen nicht für jedermann zugänglich sein, es bedarf einer Login-Funktion bzw. der Zustimmung des Organisators, damit nur Berechtigte an der Videokonferenz teilnehmen können und ein Datenabfluss verhindert wird.[1]

>> **Informationspflichten und Gewährleistung von Betroffenenrechte:** Der Anbieter sollte Funktionen bereitstellen, um betroffene Personen vor dem Beginn von Videokonferenzen die entsprechenden Informationen gem. Art. 12 ff. DS-GVO auf transparente Weise bereitstellen zu können (First- vs. Second-Level-Informationen).

1 Negativbeispiel: https://www.heise.de/ct/artikel/c-t-deckt-auf-Bayerischer-Innenminister-bespricht-Corona-Krise-in-ungeschuetzter-Videokonferenz-4680288.html

6. Datenschutzfolgenabschätzung

Vor Einführung und Einsatz von Videokonferenzsystemen könnten Verantwortliche dazu verpflichtet sein, eine Datenschutzfolgenabschätzung (DSFA) im Sinne von Art. 35 Abs. 1 DS-GVO vorzunehmen. Ob der unternehmensspezifische Einsatz der Videotechnologie ggf. unter Einsatz weiterer Funktionalitäten eine neuartige Form der Datenerfassung und -nutzung ist, die möglicherweise ein hohes Risiko für die Rechte und Freiheiten im Sinne des Kriterienkataloges des Arbeitspapieres Nr. 248[2] der Art.-29 Datenschutzgruppe mit sich bringt, ist im Einzelfall zu prüfen. Berücksichtigt werden muss auch, dass die Verarbeitung ggf. auf eigenen Endgeräten der Beschäftigten und darüber hinaus im privaten Umfeld der Beschäftigen erfolgt, was unter Umständen einen zweiten Punkt des Kriterienkataloges erfüllt, um die Erforderlichkeit zur Vornahme einer Datenschutzfolgenabschätzung zu bestimmen.

7. Vereinbarung eines Vertrags zur Auftragsverarbeitung bzw. gemeinsamen Verantwortlichkeit

Immer wenn ein Verantwortlicher Videokonferenzlösungen nicht auf eigener IT-Infrastruktur erbringt, sondern sich bei deren Einsatz eines Dritten bedient (entweder eines SaaS-Anbieters oder indem ein Dienstleister entsprechende Infrastruktur bereit stellt), muss geprüft werden, ob es eines Abschlussses eines Vertrags zur Auftragsverarbeitung gem. Art. 28 DS-GVO oder eines Vertrags zur Regelung einer gemeinsamen Verantwortlichkeit gem. Art. 26 DS-GVO bedarf.

Verarbeiten Dienstleister die Daten weisungsgebunden „im Auftrag“ und nicht für eigene Zwecke, kommt das Instrument der Auftragsverarbeitung gem. Art. 28 DS-GVO zum Einsatz. Die Verantwortung für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten trägt hier allein der Auftraggeber der Auftragsverarbeitung, nicht der Auftragsverarbeiter/Dienstleister. Aus diesem Grund werden Auftragsverarbeiter nicht mehr als „Dritte“ angesehen, sondern dem Verantwortlichen zugeordnet. Nur kraft dieser gesetzlichen Fiktion entfällt das Erfordernis einer Rechtsgrundlage für eine Offenlegung gegenüber einem Dritten und der Verantwortliche kann sich weiterhin auf die Rechtsgrundlage stützen, die ihm ursprünglich die Verarbeitung erlaubt. Nach Art. 28 Abs. 3 DS-GVO muss mit dem Auftragsverarbeiter eine Vereinbarung abgeschlossen werden. Findet eine Datenübermittlung in ein Drittland statt, bspw. weil die Server außerhalb der EU/des EWR stehen, ist zusätzlich für ein angemessenes Datenschutzniveau zu sorgen (**s. Punkt I**).

Verarbeitet der Dienstleister die personenbezogenen Daten allerdings auch für eigene Zwecke, so muss geprüft werden, ob ein Anwendungsfall des Art. 26 DS-GVO, gemeinsame Verantwortlichkeit, vorliegt. Auch hier muss eine Vereinbarung geschlossen werden, allerdings ist diese mit den wesentlichen Inhalten auch der betroffenen Person zur Verfügung zu stellen. Im Gegensatz zur Stellung als Auftragsverarbeiter bedarf es als gemeinsamer Verantwortlicher einer eigenen Rechtsgrundlage für die Verarbeitung.

Beispiel Microsoft:

Microsoft sieht sich bei seinen Produkten selbst in der Rolle eines Auftragsverarbeiters, aber auch dies ist, da Microsoft Daten auch für eigene Zwecke verwendet (für Produktaktualisierungen, zur Problembehandlung, aber auch zur Personalisierung von Produkten und zur Bereitstellung von Empfehlungen), strittig. Diesbezüglich wäre auch eine gemeinsame Verantwortlichkeit nach Art. 26 DS-GVO grundsätzlich nicht fernliegend.

2 Das Arbeitspapier Nr. 248 in der Rev. 1 ist in deutscher Sprache hier abrufbar: https://www.datenschutz-bayern.de/technik/orient/wp248.pdf

8. Technisch-organisatorische Maßnahmen, Art. 32 DS-GVO

Der Verantwortliche ist bei der Auftragsverarbeitung als auch bei der gemeinsamen Verantwortlichkeit für die Einhaltung der in der DS-GVO vorgesehenen technischen und organisatorischen Maßnahmen (TOM) verantwortlich. In der Praxis ist es üblich, dass der Dienstleister/Auftragsverarbeiter dem Verantwortlichen – ggf. nur Zug-um-Zug gegen die Unterzeichnung einer Verschwiegenheitsvereinbarung - seine TOM vorlegt. Diese sollten zumindest Angaben zu folgenden nachweislich dokumentierten Maßnahmen umfassen:

- Verschlüsselung nach dem Stand der Technik (z.B. BSI TR-02102-1)
- Anonymisierung und Pseudonymisierung
- Widerstandsfähigkeit/Resilienz der Infrastruktur (ggf. nachgewiesen durch Zertifikate)
- Verfügbarkeit von Backups (u.a. Wiederherstellbarkeit von Backups)
- Ausreichende IT-Sicherheit
- Zutritts-, Zugangs-, und Zugriffskontrollen
- Datenschutz-Schulung und Verpflichtung auf die Vertraulichkeit der mit der DV betrauten Beschäftigten
- Dokumentation über Meldepflichten bei einer Datenpanne (Meldekette)

Kurzgesagt: Es bedarf überwiegend des Abschlusses eines Auftragsverarbeitungsvertrags sowie der Kontrolle seiner Einhaltung durch den Verantwortlichen. Dementsprechend muss ein Dienstleister auch im Hinblick auf den Einsatz von Unterauftragsverarbeitern überprüft werden.

In der Praxis wird man gerade jetzt keine Vor-Ort-Kontrolle durchführen können. Ist ein Dienstleister entsprechend zertifiziert (z.B. ISO 27001, ISO 27018 oder SOC 1 Typ 2-, SOC 2 Typ 2- und SOC 3-Berichte oder ähnlich) lässt dies vermuten, dass die TOM angemessen sind.

9. Angemessenes Datenschutzniveau bei Datenverarbeitung außerhalb der EU (sog. Drittländer)

Erbringt ein Anbieter die Dienstleistung aus einem Drittland heraus und findet eine Datenübermittlung in eines statt (Länder außerhalb der EU/des EWR), dann muss der Verantwortliche sicherstellen, dass das Datenschutzniveau in diesen Ländern den Vorgaben der DS-GVO nach Art. 44 DS-GVO entspricht. Das geforderte Datenschutzniveau kann mittels folgender datenschutzrechtlicher Instrumente sichergestellt werden:

- **Angemessenheitsbeschluss der EU-Kommission:** Ein Angemessenheitsbeschluss gem. Art. 45 DS-GVO garantiert ein entsprechendes Datenschutzniveau. Angemessenheitsbeschlüsse existieren z.B. für die Schweiz, Argentinien, die Faröer Inseln, Japan und Kanada (https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en).
- Laut Adäquanzbeschluss der EU-Kommission[3] verfügen auch solche US-amerikanischen Unternehmen/Datenverarbeiter über ein der EU angemessenes Datenschutzniveau, die sich selbst nach dem **EU-US-Privacy Shield-Abkommen** zertifiziert haben (durchsuchbare Liste zertifizierter Unternehmen[4]).

3 Durchführungsbeschluss der EU-Kommission v. 12. Juli 2016, ABl EU 1.8.2016 L 207/1.

4 Die durchsuchbare Liste selbstzertifizierter Unternehmen ist auf den Webseiten des US-Wirtschaftsministeriums abrufbar: https://www.privacyshield.gov/

>> **Abschluss von europäischen Standardvertragsklauseln (engl. Standard Contractual Clauses (SCC)[5]) mit dem Anbieter:** Der Abschluss von Standarddatenschutzklauseln gem. Art. 46 Abs. 2 lit. c DS-GVO mit dem Anbieter: Der Abschluss von Standarddatenschutzklauseln gem. Art. 46 Abs. 2 lit. c DS-GVO verpflichten Anbieter das europäische Datenschutzniveau einzuhalten.

>> **Datenübermittlung ist für die Vertragserfüllung erforderlich:** Die Datenübermittlung in ein Drittland ist zur Vertragserfüllung oder auf Antrag des Betroffenen zur Durchführung vorvertraglicher Maßnahmen ohne geeignete Garantien oder Angemessenheitsbeschluss gem. Art. 49 Abs. 1 lit. b DS-GVO zulässig (bspw. Buchung von Flügen/Hotels – eine Übermittlung der personenbezogenen Daten ist hier unerlässlich und auch für die betroffene Person erwartbar). Diese Ausnahme gilt nicht für Behörden in Ausübung ihrer hoheitlichen Aufgaben (Art. 49 Abs. 3 DS-GVO).

>> **Einwilligung von Betroffenen:** Unter Aufklärung der Betroffenen über bestehende Risiken derartiger Datenübermittlungen ohne Vorliegen eines Angemessenheitsbeschlusses und ohne geeignete Garantien, bleibt als letztes Mittel die Einwilligung des Betroffenen gem. Art. 49 Abs. 1 lit. a DS-GVO. Diesbezüglich bedarf es im Zweifel eines Nachweises, dass EU-Dienste oder Dienste mit einem Privacy-Shield-Zertifikat oder Standarddatenschutzklauseln nicht in Frage kamen, da ansonsten erhebliche Zweifel an der Freiwilligkeit bestehen können. Eine weitere Herausforderung besteht außerdem darin, dass Einwilligungen jederzeit wiederrufen werden können.

10. Transparenzanforderungen gem. Art. 12 ff. DS-GVO[6]

Der Verantwortliche muss allen Teilnehmern (auch eigenen Mitarbeitern) einer Videokonferenz vorab die Informationen gem. Art. 13 DS-GVO über Zwecke, Arten sowie den Umfang einer Verarbeitung von personenbezogenen Daten im Rahmen der Konferenzen zur Verfügung stellen. Dies kann über sog. 1st-Level-Informationen[7] erreicht werden. Einige Anbieter stellen hierfür bereits entsprechende Infoflächen bereit, über welche die Unternehmen ihre Datenschutzhinweise einflechten können.

Informationen gem. Art. 13 DS-GVO sollten spätestens vor dem Betreten eines virtuellen Videokonferenz-/Chatraums über sogenannte Buttonlösungen sichtbar im Fenster der geöffneten Videokonferenz zugänglich gemacht werden oder zusätzlich auch noch vor dem Beginn einer Videokonferenz mittels im Vorfeld erfolgter E-Mail-Einladung (z.B. im Zuge mit dem entsprechenden Zugangslink) bereitgestellt werden.

11. Verzeichnis von Verarbeitungstätigkeiten (VVT)

Der Verarbeitungsprozess für die Nutzung des Konferenz-/Messengerdienstes sollte auch im Verzeichnis von Verarbeitungstätigkeiten (VVT) gem. Art. 30 DS-GVO aufgeführt werden. Beispielhalber könnte der Verarbeitungsprozess wie folgt lauten: Etablierung eines IT-gestützten Videokonferenzverfahrens - Ermöglichung der Kommunikation mit Bewerbern/Mitgliedern/Mitarbeitern/Geschäftspartnern im Homeoffice durch eigene Mitarbeiter/Geschäftsführer unter Einsatz eines Videokonferenzdienstes wie bspw.: Teams, Skype etc.

5 https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_de

6 Weiterführende Hinweise hierzu finden Sie in unserer GDD-Praxishilfe DS-GVO VII – Transparenzpflichten bei der Datenverarbeitung, kostenlos abrufbar unter https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_7.pdf

7 Zur Unterteilung der Transparenzinformationen in 1st und 2nd-Level-Informationen siehe GDD Praxishilfe DS-GVO VII, a.a.O., Seite 7 f.

12. Risikominimierung durch verbindliche Richtlinien zur Nutzung von Videokonferenzsystemen

Risiken müssen nach Art. 32, Art. 24 Abs. 1 und Art. 5 Abs. 1 lit. f DS-GVO ausgeschlossen bzw. minimiert werden, indem technische und organisatorische Maßnahmen vom Verantwortlichen getroffen werden.

Allem voran müssen die Mitarbeiter im Hinblick auf die einzusetzenden Funktionen und die Erforderlichkeit dieser sensibilisiert werden. Mitarbeiter sollten über das Wissen verfügen, welche Daten sie über Konferenztools teilen und speichern dürfen und welche nicht. Es bedarf daher organisatorischer Maßnahmen zur Sensibilisierung der Mitarbeiter und zur Festlegung von Verhaltensregeln für Videokonferenzlösungen sowie die umliegende Software-/Hardwareimplementierung. Diese Vorgaben sollten entweder in einer vorhandenen Richtlinie ergänzt (bspw. IT-Richtlinie) oder als eigenständige Richtlinie den Mitarbeitern mit an die Hand gegeben werden.

Dies betrifft unter anderem nachfolgende regelungsbedürftige Schwerpunkte:

>> **Technisch-organisatorische Maßnahmen (TOM) für die Nutzung von Endgeräten im Home Office:** Regelungen treffen welche TOM im Rahmen des Homeoffice von den Mitarbeitern eingesetzt werden sollten, Stichwort „Härtung der eingesetzten IT-Systeme“: z.B. Dateitrennung, aktueller Virenscanner, Zugangssicherungen, aktuelle Softwareupdates des Betriebssystems und des Konferenztools.

>> **Desktop-Sharing:** Sofern ein Desktop-Sharing überhaupt erforderlich ist, sollte auf dem Desktop nur das angezeigt werden, was für die Besprechung erforderlich ist. Es ist möglich bei Verwendung von mehreren Monitoren nicht den Hauptbildschirm auszuwählen oder unter Windows 10 Desktopsymbole auszublenden (Desktop > Ansicht > Desktopsymbole anzeigen).

Tipp: Schliessen Sie Mail- und Messenger-Programme, damit nicht versehentlich Einblick in Konatkdaten und/oder Nachrichten gegeben wird. So wird auch verhindert, dass immer wieder “Neu Nachricht”-Popups erscheinen.

>> **Digitale Unternehmensführungen:** Wenn auch die Unternehmensführung hauptsächlich digital erfolgt, muss unter anderem beachtet werden, dass nur die notwendigsten Informationen von den Teilnehmern gesehen und gehört werden können, z.B. keine Geschäftsunterlagen erkennbar liegen lassen.

>> **Regelungsinhalt von Black- oder Whitelists:** Wann und für welche Zwecke dürfen Anwendungsfunktionen durch den Benutzer verwendet werden – hier wäre auch auf eine mögliche Strafbarkeit eines unbefugten Abhörens oder Aufzeichnens des nicht öffentlich gesprochenen Wortes (§ 201 StGB) ggf. hinzuweisen. Welche Dateien dürfen empfangen/freigegeben werden - allem voran: Umgang mit dienstlichen Unterlagen/Daten mit erhöhtem Schutzbedarf und personenbezogene Daten.

>> **Anleitung zur Wahl des datenschutzfreundlichsten Mittels:** Mitarbeiter sollen in der Lage sein, die eingesetzten Videokonferenzlösungen datenminimal konfigurieren und einsetzen zu können. Darüber hinaus sollten Mitarbeiter Hinweise an Teilnehmer im Hinblick auf die Wahl von datenschutzfreundlichen Funktionen geben, z.B. dass diese auch ohne aktive Videokamera an einer Konferenz teilzunehmen können.

>> **Sicherheitsrichtlinie für die Nutzung von Videokonferenzsystemen und ggf. Merkblätter über die Gefahren der Videokonferenzkommunikation:** Regelungen zur Anwendung von Maßnahmen zum Einsatz der Konferenzsoftware müssen etabliert und von den Mitarbeitern eingehalten werden, ggf. unter Sanktionsandrohung bei Verstößen der Mitarbeiter.

- > Einsatz von Blurr-Möglichkeiten (Nicht Einsatz = Gefahr mangelnde Privatsphäre, ggf. ungeregelter Abfluss von Unternehmensinformationen)
- > Setzen von Zugangsbeschränkungen / Identifikation der Teilnehmer (Nicht Beachtung droht Verlust von Geschäftsgeheimnissen oder wohlmöglich Datenpannen)
- > Sensibilisierung für Social-Engineering und Social-Hacking-Angriffe (Ohne Sensibilisierung drohen Datenverluste; Kompromittierung der IT-Sicherheit; Datenpannen, Wirtschaftsspionage)
- > Anwendung von Löschrichtlinien (Ohne Regelung und Anwendung = mögliche Verstöße gegen das Datenschutzrecht)
- > Meldekette für Störungen oder Auffälligkeiten bei der EDV-Nutzung (Ohne Meldekette = Datenverluste; Kompromittierung der IT-Sicherheit; Datenpannen)

13. Dokumentation über Meldepflichten bei einer Datenpanne

Im Rahmen der Nutzung von Videokonferenzsystemen kann es zu Datenpannen i.S.v. Art. 33 DS-GVO kommen, sei es durch das versehentliche Offenbaren von personenbezogenen Daten oder IT-Notfälle auf Grund von geöffneten unbekannten Dateien. Den betroffenen Mitarbeitern muss klar sein, welche Maßnahmen sie ergreifen müssen. Bei einer Datenpanne sieht die DS-GVO eine Frist von 72 Stunden vor, innerhalb der eine Datenpanne der zuständigen Aufsichtsbehörde gemeldet werden muss.

14. Klärung der datenschutzrechtlichen Verantwortlichkeit bei Videokonferenzen zwischen Unternehmen

Bei der Nutzung von Videokonferenzdiensten ist grundsätzlich der Ersteller bzw. der Veranstalter einer Videokonferenz Session bzw. Instanz als Verantwortliche Stelle anzusehen. Arbeitnehmer, die aus dem Homeoffice heraus konferieren, fallen hierbei grundsätzlich unter die datenschutzrechtliche Verantwortlichkeit des entsprechenden Arbeitgebers, sofern Daten nicht selbst und unter Verstoß gegen die Richtlinien zur Nutzung von Videokonferenzsystemen für eigene Zwecke verarbeitet werden.

Eine gemeinsame Verantwortlichkeit zwischen selbstständig verantwortlichen Unternehmen, dürfte für die Fälle gelten, in denen die Konferenzpartner gleichwertigen Zugriff bzw. gleichwertige Kontrolle über die Videokonferenz und die entsprechenden Funktionen (Aufzeichnen, Bildschirmfoto, Transkription) haben.

15. Zusammenfassung – Datenschutz ermöglicht auch Einsatz neuer Technologien

Zusammenfassend lässt sich sagen, dass der Datenschutz auch in Krisenzeiten dem Unternehmen zahlreiche Lösungswege aufzeigt[8], sofern folgende Maßgaben beachtet werden:

Bei der Auswahl einer geeigneten Videokonferenzlösung bzw. eines Anbieters kommt es darauf an, dass die benötigten bzw. gewünschten Funktionalitäten abgebildet werden und diese entsprechend durch das Unternehmen/den Anwender in geeigneter Weise eingesetzt werden können. Dazu gehört auch, dass sich Funktionalitäten je nach Bedarf an- und abschalten lassen. Das Produkt sollte zudem in der Lage sein, die Wahrnehmung der Betroffenenrechte gewährleisten zu können. Mit dem Anbieter sollte ein **Vertrag zur Auftragsverarbeitung gem. Art. 28 DS-GVO** geschlossen werden können, sofern es sich nicht um eine gemeineinsame Verantwortlichkeit handelt. Dazu sollten geeignete und benutzerfreundliche **technische und organisatorische Maßnahmen** gem. Art. 32 DS-GVO in der Anwendung implementiert sein, um den einfachen, aber sicheren Umgang sicherzustellen. Gleichzeitig ist aber auch die innerbetriebliche Organisation von Bedeutung, da datenschutzkonformer Einsatz von Videokonferenzsystemen auch maßgeblich vom Verhalten eines jeden Mitarbeiters abhängt. **Interne Richtlinien** sind dafür ein sehr wichtiges Instrument, sie sollten nicht nur erstellt werden, sondern Beschäftigten inhaltlich durch **Mitarbeiterschulungen** vermittelt und in der täglichen Arbeit jederzeit zur Verfügung stehen. Schlussendlich sollten die Einführung und Umsetzung obiger Maßnahmen, ggf. etwaige Datenschutzfolgenabschätzungen zwecks Erfüllung der Rechenschaftspflicht dokumentiert werden (ggf. auch im Verzeichnis der Verarbeitungstätigkeiten (VVT) gem. Art. 30 DS-GVO.

Hinweis zu den Anlagen:

Als Anlagen finden Sie ein **Merkblatt für Beschäftigte (I)** zum Einsatz von Vidokonferenzsystemen und eine **Übersicht (II) über Videokonferenzsysteme, Messenger und Ferwartungssoftware** (Excel-Tabelle als Download unter: https://www.gdd.de/downloads/praxishilfen/ph_videokonferenzsysteme_aktuelle-tabelle_prelayout_04/. Zu den einzelnen Diensten erhalten Sie die datenschutzrechtlichen Kerninformationen auf einen Blick (z.T. mit klickbarem Link zur Webseite des Anbieters) sowie weitere hilfreiche Hinweise.

8 Siehe in diesem Sinne auch den Beitrag des LfDI Baden-Württemberg, abrufbar unter: https://www.baden-wuerttemberg.datenschutz.de/datenschutzfreundliche-technische-moeglichkeiten-der-kommunikation/ (8.4.2020)

Anlage I

Merkblatt für Beschäftigte

In unserem Unternehmen wird die Videokonferenzsoftware … eingesetzt. Die erforderlichen datenschutz- und lizenzrechtlichen Voraussetzungen wurden geschaffen. Sie dürfen keine andere Videokonferenzsoftware eigenmächtig in Betrieb nehmen. Werden Sie von einem Geschäftspartner zu einer Videokonferenz eingeladen, dürfen Sie an der Videokonferenz teilnehmen. Muss dazu eine Software auf Ihrem Rechner installiert werden, stimmen Sie dies mit der IT-Abteilung ab.

Die folgenden Grundsätze sollten von Ihnen beachten werden und soweit möglich als Voreinstellung in der Videokonferenzsoftware vorgenommen werden:

>> Videokonferenzsoftware nicht automatisch beim Hochfahren des Computers starten.

>> Beim Betreten eines VC-Raums das Mikrofon automatisch stumm schalten.

>> Überprüfen Sie vorab Ihr eigenes Videobild, ob es Objekte enthält, die nicht gesehen werden sollten.

>> Wählen Sie Ihre Meeting-ID bzw. Meeting-URL möglichst kryptisch und keinesfalls sprechend (z.B: Ihr Name oder Ihre Telefonnummer), damit sie nicht erraten werden kann.

>> Vergeben Sie ein Passwort zum Betreten des Meeting-Raums.

>> Geben Sie die Zugangsdaten zu dem Meeting nur an die geplanten Teilnehmer.

>> Beobachten Sie als Veranstalter des Meetings die Teilnehmer. Reagieren Sie sofort, wenn ein nicht ein geladener Teilnehmer erscheint.

>> Halten Sie die Videokonferenzsoftware (oder den Browser, mit dem Sie an der Videokonferenz teilnehmen) aktuell.

>> Für die Aufzeichnung einer Videokonferenz ist die Zustimmung aller Teilnehmer erforderlich.

>> Wenn Sie parallel zur Videokonferenz in der Software einen Chat-Kanal benutzen, sollten Sie sich nur so äußern, dass eine versehentliche Veröffentlichung des Chats keinen Schaden für Sie oder unser Unternehmen anrichtet.

>> Klären Sie vor der Einladung zu einem Meeting, ob die zu erwartenden Inhalt der Konferenz, für das Medium geeignet sind. Insbesondere bei Gesprächen aus dem Personalbereich (z.B. Vorstellungsgespräche, Mitarbeitergespräche) müssen Sie klären, ob das zulässig ist. Fragen Sie in Zweifelsfällen unseren Datenschutzbeauftragten.

Als Organisator einer Videokonferenz obliegt Ihnen auch die Verantwortung für die ordnungsgemäße Durchführung der Videokonferenz.

Anlage II

Übersicht über Videokonferenzsysteme, Messenger und Fernwartungssoftware

Die Excel-Tabelle ist abrufbar unter:
https://www.gdd.de/downloads/praxishilfen/ph_videokonferenzsysteme_aktuelle-tabelle/view
Zu den einzelnen Diensten erhalten Sie die datenschutzrechtlichen Kerninformationen auf einen Blick (z.T. mit klickbarem Link zur Webseite des Anbieters) sowie weitere hilfreiche Hinweise.

Gesellschaft für Datenschutz
und Datensicherheit e.V.

Satz: C. Wengenroth, GDD-Geschäftsstelle, Bonn

Herausgeber:
Gesellschaft für Datenschutz und Datensicherheit (GDD e.V.)
Heinrich-Böll-Ring 10
53119 Bonn
Tel.: +49 2 28 96 96 75-00
Fax: +49 2 28 96 96 75-25
www.gdd.de
info@gdd.de

Stand:
Version 1.0 (April 2020)