Checkliste Datenschutz in Videokonferenzsystemen

Stand 11.11.2020

Bezogen auf die Orientierungshilfe Videokonferenzsysteme, Stand 23.10.2020

Kapitel in der Orientierungshilfe	Anforderung erfüllt? [ja/nein/nicht zutreffend]	Referenz
3 Rechtliche Anforderungen Rollen und Verantwortlichkeiten der Beteiligten sind klar verteilt und eindeutig festgelegt (Art. 4 Nr. 7 DS-GVO i.V.m. Art. 28 Abs. 3 und/oder Art. 26 DS-GVO). **3.1 Selbst betriebener Dienst** Der Betreiber des Videokonferenzsystems ist sich seiner Verantwortlichkeit im Sinne der DS-GVO bewusst, da er oder sie im Rahmen des Einsatzes dieses Systems über die Zwecke und Mittel der Verarbeitung bestimmt. Es bestehen jeweils die erforderlichen Rechtsgrundlagen für die unterschiedlichen Verarbeitungen personenbezogener Daten durch den selbst betriebenen Dienst. Der Verantwortliche setzt für Betrieb und Wartung ausreichende technische und personelle Kapazitäten ein. Der Verantwortliche ergreift geeignete technische und organisatorische Maßnahmen zum Schutz der Daten. **3.2 Betrieb durch einen externen IT-Dienstleister** Der Verantwortliche (im Folgenden auch: der Veranstalter) hat einen wirksamen Vertrag zur Auftragsverarbeitung nach Art. 28 DS-GVO mit dem IT-Dienstleister abgeschlossen. Der Auftragsverarbeiter (im Folgenden auch: der Anbieter) bietet hinreichende Garantien zu den erforderlichen technischen und organisatorischen Maßnahmen (Art. 28 Abs. 1 DS-GVO). Die eingesetzte oder Teilnehmenden angebotene Software wurde auf Datenabflüsse überprüft. Dies schließt Diagnose- und Telemetriedaten oder sonstige Datenabflüsse z.B. an Hersteller ein. Entsprechende Datenabflüsse wurden unterbunden, soweit nicht eine Rechtsgrundlage hierfür besteht. **3.3 Online-Dienst** Im Falle einer Verarbeitung zu eigenen Zwecken durch den Anbieter verfügt der Veranstalter für jede Offenlegung personenbezogener Daten an den Anbieter über eine Rechtsgrundlage.		

Der Anbieter verfügt für jede Verarbeitung personenbezogener Daten in eigener Verantwortlichkeit über eine Rechtsgrundlage. Die Notwendigkeit einer Vereinbarung zur gemeinsamen Verantwortlichkeit von Anbieter und Verantwortlichem nach Art. 26 Abs. 1 DS-GVO wurde geprüft. Der Verantwortliche hat die vom Auftragsverarbeiter vorgelegten Auftragsverarbeitungsverträge, Nutzungsbedingungen und Sicherheitsnachweise sowie dessen Datenschutzerklärung geprüft. Der Verantwortliche hat bei der Auswahlentscheidung für einen Anbieter darauf geachtet, 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 Konfigurationsoptionen des eingesetzten Dienstes wurden hinsichtlich datenschutzrechtlicher Aspekte geprüft und bei Bedarf angepasst. Gegenüber den betroffenen Personen wird transparent gemacht, wer in welcher Rolle personenbezogene Daten verarbeitet. Die Kontaktdaten des Verantwortlichen und – falls im jeweiligen Nutzungsszenario anwendbar – des Anbieters sind klar für den Nutzer auffindbar. **3.4 Rechtsgrundlage und Zweckbindung** Für die Veranstaltung einer Videokonferenz liegt eine Rechtsgrundlage des Veranstalters und, soweit er Daten nicht alleine im Rahmen der Auftragsverarbeitung empfängt, des Anbieters gemäß Art. 6 DS-GVO vor. **3.4.1 Zur Struktur der Rechtsgrundlagen** Eine einschlägige Befugnisnorm nach Art. 6 Abs. 1 lit a, b, e, f DS-GVO, gegebenenfalls auch in Verbindung mit dem nationalen Recht, ist vorhanden. **3.4.2 Einwilligung** Sollte die Verarbeitung personenbezogener Daten in einer Videokonferenz auf Basis von Einwilligungen legitimiert werden, so sind diese in informierter Weise und freiwillig abgegeben worden (Art. 4 Nr. 11 DS-GVO und Art. 6 Abs. 1 lit. a i.V.m. Art. 7 DS-GVO). Ausreichende Datenschutzinformationen wurden erteilt, damit die Einwilligung informiert abgegeben werden kann. Es besteht eine echte Wahlmöglichkeit hinsichtlich der Teilnahme an der Videokonferenz. **3.4.3 Arbeitgeber als Verantwortliche** Die Erforderlichkeit der Übertragung auch von Bilddaten wurde überprüft, insbesondere, wenn die Rechtsgrundlage für die Datenverarbeitung auf § 26 Abs. 1 Satz 1 BDSG oder entsprechenden landesrechtlichen Vorschriften im öffentlichen Bereich beruht. **3.4.4 Verarbeitung besonderer Kategorien personenbezogener Daten** Sofern bei der Videokonferenz besondere Kategorien personenbezogener Daten thematisiert werden, ist diese Datenverarbeitung auch nach Art. 9 Abs. 2 DS-GVO, ggf. in Verbindung mit einem nationalen Gesetz, zulässig. 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. Diese Einwilligung wurde ausdrücklich, informiert, freiwillig, vorherig, aktiv, für den konkreten Einzelfall und separat erklärt und ist jederzeit zumutbar widerruflich.

3.4.5 Teilnahme aus Privatwohnungen

Soweit Beschäftigte aus ihrem Home-Office teilnehmen, hat der Arbeitgeber durch technische und organisatorische Maßnahmen sichergestellt, dass Einblicke in deren Privatsphäre durch Bild und Ton nicht möglich sind.

Unter Sicherstellung der Freiwilligkeit ist eine gesonderte Einwilligung in diese Einblicke denkbar. Die Freiwilligkeit wird in diesem Falle zugesichert und die betroffenen Beschäftigten wurden vom Verantwortlichen über die diesbezüglichen Risiken informiert.

3.4.6 Verarbeitungen durch Anbieter zu eigenen Zwecken

Sofern ein Anbieter personenbezogene Daten zu eigenen Zwecken verarbeitet hat dieser selbst – als Verantwortlicher im datenschutzrechtlichen Sinne (Art. 4 Nr. 7 DS-GVO) – eine Rechtsgrundlage.

Gegenüber einem Auftragsverarbeiter wird im Auftragsverarbeitungsvertrag sichergestellt, dass dieser die personenbezogenen Daten der teilnehmenden Personen nur auf Weisung des Verantwortlichen und nicht für eigene Zwecke verarbeitet (Art. 28 Abs. 3 DS-GVO).

3.4.7 Verarbeitung von Daten Dritter

Für die Verarbeitung personenbezogener Daten Dritter, die nicht an der Videokonferenz teilnehmen, werden die allgemeinen Rechtsgrundlagen herangezogen.

3.4.8 Transparenz, Aufzeichnungen von Videokonferenzen

Art und Zweck der Verarbeitung personenbezogener Daten sind klar definiert.

Die Verarbeitung ist auf den Zweck der Videokonferenz beschränkt.

Die Rechtsgrundlage für Aufzeichnungen wurde erfolgreich geprüft.

Wirksame Einwilligungen in die Aufzeichnung und die weitere Verarbeitung liegen vor.

Aufzeichnungsmöglichkeiten werden bei der Erfüllung der Informationspflichten erwähnt.

Bestehende Aufzeichnungsfunktionen wurden in der Voreinstellung deaktiviert.

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

Audio- und Videodaten werden nur solange und soweit verarbeitet, wie es für die Übermittlung der Nachrichten durch einen Dienstleister oder im Rahmen einer notwendigen Dokumentation erforderlich ist.

3.5 Pflichten des Verantwortlichen

3.5.1 Informationspflichten und Betroffenenrechte

Den an der Konferenz teilnehmenden Personen werden klare und eindeutige Informationen über die mit der Nutzung des Dienstes verbundene Datenverarbeitung zur Verfügung gestellt (Art. 13 und 14 DS-GVO).

Die Informationen werden so dargestellt, dass sie für einen durchschnittlichen Nutzer des Dienstes ohne übermäßigen Aufwand verständlich sind (Art. 12 und Art. 5 Abs. 1 lit. a DS-GVO).

Werden die Daten auf Grund eines berechtigten Interesses (Art. 6 Abs. 1 lit. f DS-GVO) verarbeitet, so werden diese Interessen konkret benannt und die wesentlichen Gesichtspunkte der Abwägung mit den Interessen und Grundrechten der Betroffenen dargestellt.

Die teilnehmenden Personen werden über die Zwecke und die Rechtsgrundlagen der einzelnen Verarbeitungsvorgänge informiert (Art. 13, 14 DS-GVO).

Die teilnehmenden Personen werden ggf. auf ihr Widerspruchsrecht hingewiesen (Art. 21 Abs. 4 DS-GVO).

Der Veranstalter der Videokonferenz informiert die teilnehmenden Personen über Verarbeitungstätigkeiten des Anbieters des Dienstes, die dieser – soweit das überhaupt zulässig ist – zu eigenen Zwecken vornimmt.

Der Veranstalter informiert die teilnehmenden Personen darüber, welche Möglichkeiten für sie bestehen, im Rahmen der Privatsphäre-Einstellungen des Dienstes selbst auf den Schutz ihrer personenbezogenen Daten hinzuwirken (z. B. Nutzung eines Synonyms, Einstellen eines künstlichen Hintergrunds).

Die Betroffenenrechte aus Art. 15 bis 21 DS-GVO sind gewährleistet.

Die Löschung der Inhalts- und Rahmendaten der beendeten Konferenz erfolgt auch unabhängig von einem Antrag der betroffenen Personen nach Art. 17 DS-GVO regelmäßig unverzüglich nach dem Abschluss der Videokonferenz.

3.5.2 Auftragsverarbeitungsvertrag

Wenn das Videokonferenzsystem durch den Anbieter betrieben wird oder dieser die Möglichkeit hat, auf personenbezogene Daten zuzugreifen, wurde mit ihm ein gültiger Auftragsverarbeitungsvertrag abgeschlossen (Art. 28 DS-GVO).

3.5.3 Verarbeitungsverzeichnis

Die Veranstaltung der Videokonferenz(en) wurde in das Verzeichnis der Verarbeitungstätigkeiten gemäß Art. 30 DS-GVO aufgenommen.

3.5.4 Meldepflichten bei Datenpannen

Im Fall einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit der Videokonferenz werden die Pflichten aus Art. 33 und 34 DS-GVO eingehalten.

3.5.5 Datenschutz-Folgenabschätzung

Der Verantwortliche hat überprüft, ob eine Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO durchzuführen ist und diese bei Bedarf durchgeführt.

3.5.6 Besonderheiten bei Übermittlungen an Drittländer

Werden Videokonferenzsysteme von Anbietern ausgewählt, die zu Datenübermittlungen in Drittländer führen, so hält die Übermittlung besondere Bedingungen (vgl. Kapitel V, Art. 44 ff. DS-GVO, siehe dazu auch Kurzpapier Nr. 4 der Datenschutzkonferenz sowie Veröffentlichungen des EDSA) ein.

4 Technische und organisatorische Anforderungen

4.1 Sicherheit der Übertragung

Für die Übertragung der Videokonferenzdaten werden mindestens Transportverschlüsselungen nach dem Stand der Technik, entsprechend den einschlägigen Technischen Richtlinien des BSI, genutzt.

Sollte ein hohes Risiko bestehen, werden geeignete technische und organisatorische Maßnahmen zur Sicherstellung der Vertraulichkeit der Inhaltsdaten ergriffen (bspw. über Ende-zu-Ende-Verschlüsselung oder über TLS-Verbindungen mit zusätzlichen technischen und organisatorischen Maßnahmen).

Die einzelnen Funktionalitäten des eingesetzten Videokonferenzsystems wurden separat betrachtet, insbesondere hinsichtlich der Risiken ihres Einsatzes für Rechte und Freiheiten der betroffenen Personen.

Es wurden Funktionalitäten des Dienstes unterbunden, für die ein unbefugter Abfluss personenbezogener Daten zu befürchten ist.

Über die Protokollierung der Inanspruchnahme von Funktionalitäten wird für die teilnehmenden Personen Transparenz gewahrt.

Es wird sichergestellt, dass der Hersteller und andere Dritte keinen Zugriff auf die verarbeiteten Daten, wie bspw. Nutzungsdaten, erhalten.

4.2 Nutzerauthentifizierung

Es wird sichergestellt, dass nur berechtigte Personen auf eine Videokonferenzsitzung und deren Daten zugreifen können.

4.2.1 Normale Risiken

Die Nutzer werden mittels Nutzername und Passwort authentisiert oder mittels eines stärkeren Verfahrens, beispielsweise Zwei-Faktor-Authentisierung.

Die Authentisierung mittels Nutzername und geeignetem Passwort ist so ausgestaltet, 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 verwendet werden können.

4.2.2 Hohe Risiken

Bei hohem Risiko wird eine Zwei-Faktor-Authentisierung nach dem Stand der Technik eingesetzt. Dafür kommen je nach Höhe des Risikos insbesondere Softwaretoken bzw. Hardwaretoken in Frage.

4.2.3 Authentifizierungsdienst

Die Nutzerauthentifizierung wird nach erfolgter Risikoabwägung auf ein Verfahren gestützt, das bereits für andere Verfahren genutzt wird. Der Identity Provider gewährleistet die Integrität des Authentifizierungsvorgangs und die Nichtverkettung verschiedener Nutzungsvorgänge.

Bei Anwendungsfällen, die eine vorherige Identifikation der Nutzer erfordern, werden geeignete Verfahren implementiert, um die Authentizität der Nutzer im Nachhinein nachvollziehen zu können.

4.2.4 Gastteilnahme

Der Gastzugang ist für den Anwendungsfall erforderlich.

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.

Die Empfänger eines Einladungslinks werden auf die Folgen einer nicht autorisierten Weitergabe des Links hingewiesen.

Die Übergabe des Links wahrt die Vertraulichkeit auf angemessenem Niveau.

4.3 Installation und Softwareaktualisierung

Technische Schwachstellen und sonstige Sicherheitslücken in Videokonferenzsystemen werden in einem angemessenen Zeitraum behoben.

Alle Komponenten, die für die Teilnahme an einer Videokonferenz auf einem Client installiert werden, können einfach und vollständig deinstalliert werden. Auch bei einer nur einmaligen Nutzung eines nativen Clients ist sichergestellt, dass keine ungewartete Software auf dem System verbleibt.

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

4.4 Rollentrennung

Das Videokonferenzsystem ermöglicht die Einrichtung administrierender, moderierender, präsentierender und teilnehmenden Personen bzw. andere Zuschnitte, soweit die Verantwortung für die Steuerung der implizit vorgenommenen Verarbeitung von personenbezogenen Daten klar zugewiesen bleibt.

Die teilnehmenden Personen können ihr Mikrofon und ihre Kamera jederzeit deaktivieren. Ohne die Zustimmung der teilnehmenden Person kann deren Mikrofon und deren Kamera nicht aktiviert werden.

Bei Anwendungen mit hohem Risiko ist eine Nutzerverwaltung vorgesehen, die die Autorisierung der teilnehmenden Personen zur Übernahme einer der o.g. Rollen sicherstellt.

4.5 Datensparsamkeit

Es werden für die Bereitstellung des Dienstes nur die zwingend erforderlichen technischen und sonstigen Informationen verarbeitet.

Die Protokolldaten werden nur für den Zweck der Konferenz verarbeitet.

Das Videokonferenzsystem erfüllt die Grundsätze Datenschutz durch Technikgestaltung sowie datenschutzfreundlicher Voreinstellungen.

Vor Eintritt in die Konferenz sind Funktionen von Kamera, Mikrofon und das Teilen des Bildschirms deaktiviert und müssen erst von der teilnehmenden Person aktiviert werden.

4.6 Transparenz Der Hersteller des Videokonferenzsystems stellt, zusätzlich zu den rechtlich gebotenen Hinweisen in den Datenschutzbestimmungen, Informationen zur technischen Implementierung, den eingesetzten Standards, genutzten Software-Bibliotheken und Lizenzen bereit. Es ist teilnehmenden Personen leicht möglich und an prominenter Stelle erkennbar, ob und ggf. welche Datenverarbeitungsvorgänge über den eigentlichen Anwendungszweck der Videokonferenz hinaus erfolgen. Berichte zu Sicherheitsprüfungen werden frei zugänglich veröffentlicht. **4.7 Aufzeichnungen** Aufzeichnungen werden technisch unterbunden, sofern diese nicht aus sonstigen Gründen zulässig sind. Die notwendige Konfigurationseinstellung kann nur von einem Administrator zurückgenommen werden. Die an der Videokonferenz teilnehmenden Personen werden darauf hingewiesen, dass eine Aufzeichnung unzulässig ist. Im Falle einer zulässigen Aufzeichnung können ausschließlich besonders privilegierte Nutzer diese Funktion aktivieren. Alle teilnehmenden Personen werden durch einen expliziten und durch einen durch die teilnehmende Person zu bestätigenden Hinweis oder durch Kennzeichnung innerhalb der Benutzerschnittstelle darauf hingewiesen, dass die Videokonferenz ganz oder in Teilen aufgezeichnet wird. Aufzeichnungen von Videokonferenzen werden wenn möglich verschlüsselt gespeichert. Bei hohem Risiko ist dies zwingend vorgesehen. **4.8 Intervenierbarkeit** Die teilnehmenden Personen haben die technische Möglichkeit, zumindest zeitweise an Konferenzen lediglich passiv (empfangend), aber nicht aktiv (sendend) teilzunehmen. Dies beinhaltet auch das separate Abschalten von jeweils der Kamera und des Mikrofons durch die teilnehmende Person.		

Anwendungshinweis

Die vorliegende Checkliste stellt die wesentlichen Anforderungen an Videokonferenzsysteme der „Orientierungshilfe Videokonferenzsysteme“ der DSK in verkürzter Form dar. Sie soll den Verantwortlichen bei der Überprüfung, ob ein Videokonferenzsystem datenschutzkonform ist sowie bei der Erfüllung seiner Transparenz- und Dokumentationspflichten unterstützen. Aus der Erfüllung sämtlicher bzw. Nicht-Erfüllung einzelner Anforderungen kann nicht unmittelbar auf die Zulässigkeit oder Nichtzulässigkeit geschlossen werden.