datenschutz cert

18.10.2021

Auslegungshilfen für den Nachweis von Videosprechstunden gemäß Anlage 31 b zum BMV-Ä

1. Anforderungen an Videosprechstunden

Für das Betreiben von Videosprechstunden, bei denen ärztliches Personal, Pflegekräfte oder Psychotherapeuten*innen mit Patienten*innen per Videoverbindung kommunizieren, muss in Deutschland die Vereinbarung über die Anforderungen an die technischen Verfahren zur Videosprechstunde gemäß Anlage 31b zum Bundesmantelvertrag-Ärzte (BMV-Ä) i.V.m. § 365 Abs. 1 SGB V (kurz: Anlage 31b zum BMV-Ä oder „Vereinbarung“) beachtet und eingehalten werden.

Die folgende Auflistung skizziert relevante Anforderungen für Videosprechstunden gemäß der Anlage 31 zum BMV-Ä und dient für Sie als Hilfestellung im Rahmen der Vorbereitung für eine Evaluierung Ihrer Videosprechstunde.

Bitte beachten Sie, dieses Dokument stellt keine abschließende Auflistung dar – auch besteht kein Anspruch auf Vollständigkeit. Dieses Dokument wird ferner von Zeit zu Zeit angepasst, z.B. aufgrund neuer Anforderungen der Datenschutz-Aufsichtsbehörden, der Rechtsprechung oder aufgrund Gesetzesänderungen.

2. Anforderungen zum Datenschutz

2.1. Zulässigkeit der Datenverarbeitung (DV)

Der*Die Videodienstanbieter*in ist verantwortliche Stelle für die Datenverarbeitung im Zusammenhang mit der Videosprechstunde (§ 2a Abs. 2 Anlage 31 Anlage 31 b zum BMV-Ä). Etwaige vertragliche Gestaltungen, die eine Auftragsverarbeitung der Anbieter*innen von Videosprechstunden für ärztliches Personal/ Kliniken etc. nach Art. 28 DSGVO / § 80 SGB X beinhalten, sind nicht mehr zulässig. Eine gemeinsame Verantwortung gemäß Art. 26 DSGVO zwischen den* Videodienstanbietern*innen und ärztlichem Personal kann ebenfalls grundsätzlich nicht vorliegen.

Für jede Datenverarbeitung von personenbezogenen Daten im Zusammenhang mit der Videosprechstunde muss eine Rechtsgrundlage nachweisbar (dokumentiert) vorliegen gemäß Art. 6 DSGVO. Darüber hinaus ist ggf. auch Art. 9 DSGVO bei besonderen Kategorien personenbezogener Daten (z. B. Gesundheitsdaten, auch Termindaten) zu beachten.

Als Dokumentation eignet sich z.B. ein Verzeichnis der Verarbeitungstätigkeit (VVT) gemäß Art. 30 DSGVO bzw. ein entsprechender Auszug, der die Videosprechstunde beschreibt.

2.1.1. Rechtsgrundlage Vertrag

Liegt ein Vertrag mit den betroffenen Personen, i.d.R. ärztliches Personal oder Patienten*innen, vor, so ist der Vertrag die richtige Rechtsgrundlage. Dazu gehören alle Datenverarbeitungen, die zur Erfüllung der vertraglichen Pflichten oder vorvertraglichen Maßnahmen erforderlich sind.

Kommt z. B. mit der für die Nutzung der Videosprechstunde erforderlichen Registrierung der* Vertragsärzte*innen ein Vertrag zu Stande oder wird dieser außerhalb der Registrierung zwischen Anbieter*in und ärztlichen Nutzer*innen abgeschlossen, ist die Datenverarbeitung über Art. 6 Abs. 1 lit. b DSGVO legitimiert. Dazu gehört, sofern erforderlich, auch die Erfassung von Zahlungsdaten im Rahmen des Kundendatenmanagements sowie die Speicherung der Metadaten der Videosprechstunde.

Dabei gilt, dass nur Daten verarbeitet werden dürfen, die für die vertraglichen Maßnahmen erforderlich sind. Kann der Vertrag ebenso ohne die Datenverarbeitung durchgeführt werden, ist die Datenverarbeitung über die Rechtsgrundlage Vertrag rechtswidrig.

Die Vertragswerke zum Gesamtangebot der Videosprechstunde werden vom Evaluations-Team einbezogen in die datenschutzrechtliche Prüfung. Dazu gehören neben den Musterverträgen die Allgemeinen Geschäftsbedingungen (AGB) sowie anderweitige vertragliche Dokumentationen für die Nutzung der Videosprechstunde zwischen Ihnen als Videodienstanbieter*in und den Nutzern*innen der Videosprechstunde.

2.1.2. Rechtsgrundlage berechtigtes Interesse

Ebenfalls in Betracht kommt die Rechtsgrundlage des berechtigten Interesses. Demnach können einzelne Verarbeitungsvorgänge, sofern die Interessen oder die Grundrechte und Grundfreiheiten der betroffenen Person nicht überwiegen, gemäß Art. 6 Abs. 1 lit. f DSGVO auf ein berechtigtes Interesse des*der Videodienstanbieters*in gestützt werden.

Der*Die Videodienstanbieter*in muss eine sorgfältige Interessenabwägung durchführen. So ist z. B. zu berücksichtigen, ob die betroffene Person aufgrund der konkreten Situation mit einer Datenverarbeitung vernünftigerweise rechnen kann.

Das Schalten von Werbung im Rahmen der Videosprechstunde ist verboten. Diese Datenverarbeitung kann somit nicht auf das berechtigte Interesse gestützt werden.

Die Erhebung von bestimmten Daten bei einem Webseitenbesuch kann z. B. zu Sicherheitszwecken und zur Verfügungstellung des Dienstes erforderlich sein. Dies stellt regelmäßig ein berichtigtes Interesse i.S.d. Art. 6 Abs. 1 lit. f DSGVO dar, sofern die Speicherung temporär notwendiger Daten (z.B. IP-Adressen) nicht länger als erforderlich, max. aber nur für 7 Tage, erfolgt.

Auch hier werden die Vertragswerke sowie die Videosprechstunde, Webseiten und der Umgang mit Nutzer*innen-Daten in die Evaluation einbezogen.

2.1.3. Rechtsgrundlage Einwilligung

Für einige Datenverarbeitungen ist eine Einwilligung notwendig. Z. B. kann die Datenverarbeitung im Rahmen der Registrierung von Patienten*innen oder die Anmeldung zum Newsletter durch eine Einwilligung gem. 6 Abs. 1 lit. a DSGVO legitimiert werden. Auch für zusätzliche freiwillige Angaben in Webformularen ist eine Einwilligung erforderlich.

Die Datenverarbeitung aufgrund der Einwilligung ist nur zulässig, wenn keine andere Rechtsgrundlage in Betracht kommt.

Die Einwilligung muss freiwillig und ausdrücklich, durch ein aktives bestätigendes Handeln erfolgen und dokumentiert werden (nachweisbar). Einwilligungen durch z. B. Schweigen oder vorangekreuzte Kästchen stellen keine wirksame Einwilligung dar.

Es muss sichergestellt werden, dass die Einwilligung vor der Datenverarbeitung eingeholt wird.

Die betroffene Person muss jederzeit die Möglichkeit haben, die Einwilligung zu widerrufen, z. B. über ein Kontaktformular, das der*die Videodienstanbieter*in zur Verfügung stellt. Die betroffene Person ist vor Erteilung der Einwilligung über ihr Widerrufsrecht zu informieren. Das Widerrufsrecht sollte von der betroffenen Person simpel ausgeübt werden können.

Bei Gesundheitsdaten ist immer auch Art. 9 Abs. 2 lit. a DSGVO zu beachten (s. 2.1.4.).

Achtung: Unabhängig von dem*der Videodienstanbieter*in muss das ärztliche Personal für die Einladung von Patient*innen zur Videosprechstunde gemäß § 4 Abs. 2 Anlage 31b zum BMV-Ä ebenfalls eine Einwilligung einholen, etwa bei Erstkontakt

zwischen ärztlichem Personal und Patient*innen außerhalb der Videosprechstunde. Der*Die Videodienstanbieter*in muss dabei unterstützen, z. B. indem Behandelnde in den AGB entsprechend dazu verpflichtet werden, die Einwilligung einzuholen. Eigene Datenverarbeitungen des*der Videodienstanbieters*in als verantwortliche Stelle sind von dieser Einwilligung nicht gedeckt. Diese Verarbeitungen des*der Videodienstanbieters*in müssen, durch eigene Rechtsgrundlagen (Einwilligung, Vertrag, berechtigtes Interesse...) legitimiert sein.

Etwaige Einwilligungsprozesse bei der Videosprechstunde werden entsprechend evaluiert. Dies umfasst z. B. Art, Umfang und Ausgestaltung der Erklärung, durch die die betroffenen Personen in eine Datenverarbeitung einwilligen (Einwilligungserklärung), etwa, ob die betroffene Person durch ein aktives bestätigendes Handeln in die Datenverarbeitung eingewilligt hat (z. B. durch das Anklicken eines Kästchens, um der Datenverarbeitung vor dem Absenden eines Kontaktformulars zuzustimmen, durch Einwilligung zum Erhalt eines Newsletters mittels sog. Double-Opt-In-Verfahren).

Beim Einsatz von z. B. nicht technisch notwendigen Cookies, die einer Einwilligung bedürfen, müssen Nutzer*innen vor der Datenverarbeitung aktiv in die Datenverarbeitung einwilligen (sog. Opt-In-Verfahren) z. B. mittels eines Consent-Tools mit entsprechender Einwilligungserklärung. Im Consent-Tool können Cookies übersichtlich in: Notwendig, Präferenzen und Statistik klassifiziert werden. Bzgl. des Einsatzes von Marketing-Cookies ist zu beachten, dass das Schalten von Werbung im Rahmen der Videosprechstunde und damit auch das Erfassen von Daten zu werblichen Maßnahmen unzulässig ist.

Als Dokumentation werden etwa gefordert: PDF Versionen von Webformularen (z. B. Registrierung, Kontaktformular, Newsletter) mit denen die Einwilligung zur Datenverarbeitung eingeholt wird (Einwilligungsprozess) mit entsprechenden Informationen für die Nachvollziehbarkeit der Einholung einer informierten und freiwilligen Einwilligung (Einwilligungserklärung), ggf. Datenschutzerklärung, Logs.

2.1.4. Rechtsgrundlage bei besonderen Kategorien personenbezogener

Da besondere Kategorien personenbezogener Daten (z. B. Gesundheitsdaten) besonders schutzwürdig sind, gelten besondere Anforderungen. Im Rahmen von Videosprechstunden ist regelmäßig für die Verarbeitung besonderer Kategorien personenbezogener Daten, z. B. Termindaten, eine Einwilligung gemäß Art. 9 Abs. 2 lit. a DSGVO erforderlich. Nach der Anlage 31b zum BMV-Ä ist die Aufzeichnung der Videosprechstunde nur auf Basis einer Einwilligung auf Patienten*innen-Seite gemäß Art. 9 Abs. 2 lit. a DSGVO gestattet.

Eine Verarbeitung auf Grundlage eines Vertrages oder vorvertraglicher Maßnahmen ist nicht möglich.

2.1.5. Weitere Rechtsgrundlagen

Bitte beachten Sie, dass neben den oben genannten Rechtsgrundlagen noch weitere Rechtsgrundlagen gemäß Art. 6 DSGVO in Betracht kommen können. Diese sind allerdings regelmäßig nicht für die Videosprechstunde einschlägig.

2.2. Grundsätze

Die Datenverarbeitung im Rahmen der Videosprechstunde muss im Einklang mit den Grundsätzen der DSGVO (aus Art. 5 DSGVO) erfolgen. Der*Die Videodienstanbieter*in muss die Umsetzung der folgenden Grundsätze nachweisen können („Rechenschaftspflicht“).

Als Nachweis dienen z. B. Richtlinien für Mitarbeiter*innen, Prozessbeschreibungen, Löschkonzepte, Berechtigungskonzepte, Dokumentation von Auditierungen/Kontrollen, PDF Versionen von Webformularen (z. B. Registrierung, Kontaktformular), Datenschutzerklärung, etc.

2.2.1. Zweckbindung

Daten dürfen nur für festgelegte, eindeutige und legitime Zwecke erhoben, und nicht zu fremden Zwecken weiterverarbeitet werden. Der*Die Videodienstanbieter*in muss dies gemäß Art. 5 Abs. 1 lit. b DSGVO sicherzustellen.

Werden z. B. die für den Registrierungsprozess im Rahmen der Videosprechstunde Daten für die Vertragsabwicklung verarbeitet, so dürfen darüber hinaus keine Daten verarbeitet werden, die für diesen Zweck nicht notwendig sind. Eine Datenerhebung darüber hinaus wäre z. B. auf Basis einer Einwilligung mit entsprechender Zweckangabe zulässig.

Werden innerhalb eines Tools z. B. eines Online-Formulars personenbezogene Daten zu verschiedenen Zwecken verarbeitet, ist dies für die Betroffenen transparent darzulegen, z. B. durch Kennzeichnung der Formularfelder mit Symbolen o. ä., ggf. auch durch einen Verweis auf die entsprechende Stelle in der Datenschutzerklärung.

Zum Nachweis dienen insb. PDF-Versionen der entsprechenden Webformulare (z. B. Registrierung, Kontaktformular) sowie die Datenschutzerklärung.

2.2.2. Datenminimierung

Die Datenverarbeitung ist gemäß Art. 5 Abs. 1 lit. c DSGVO auf das erforderliche Maß zu beschränken.

Hier ist zu beachten, dass gemäß § 2 Abs. 4 Anlage 31b zum BMV-Ä sämtliche Inhalte der Videosprechstunde durch den*die Videodienstanbieter*in weder eingesehen noch gespeichert werden dürfen. Die personenbezogenen Metadaten/technischen Verbindungsdaten sind nach spätestens 3 Monaten zu löschen und dürfen nur für die zur Abwicklung der Videosprechstunde notwendigen Abläufe genutzt werden.

Ist die Verarbeitung der personenbezogenen Daten für den jeweiligen Zweck nicht erforderlich, sollte den Betroffenen verständlich dargelegt werden, dass Daten darüber hinaus freiwillig abgegeben werden können.

Als Nachweis der Datenminimierung dienen insb. PDF-Versionen der entsprechenden Webformulare (z. B. Registrierung, Kontaktformular), die Datenschutzerklärung als auch entsprechende Prozessbeschreibungen.

2.2.3. Richtigkeit

Die Daten der Nutzer*innen müssen gemäß Art. 5 Abs. 1 lit. d DSGVO sachlich richtig sein. Dies müssen Sie als Videodienstanbieter*in sicherstellen, indem Sie die Daten entsprechend dem Zwecke löschen oder berichtigen.

Dies kann dies z. B. auch durch die Möglichkeit der Profilbearbeitung durch die Nutzer*innen umgesetzt werden.

Als Nachweis dienen insbesondere Berechtigungskonzepte und Löschkonzepte, ggf. PDF-Versionen der entsprechenden Webformulare mit Möglichkeiten der Profilbearbeitung (z. B. Nutzerprofil), die Datenschutzerklärung oder auch entsprechende Prozessbeschreibungen.

2.2.4. Speicherbegrenzung

Der*Die Videodienstanbieter*in muss gemäß Art. 5 Abs. 1 lit. e DSGVO sicherstellen, dass die Daten nicht länger als für den jeweiligen erforderlichen Zweck, für den die Daten verarbeitet werden, gespeichert werden.

Personenbezogene Metadaten/technische Verbindungsdaten sind nach spätestens 3 Monaten zu löschen und dürfen nur für die zur Abwicklung der Videosprechstunde notwendigen Abläufe genutzt werden, § 2 Abs. 4 Anlage 31 b zum BMV-Ä. Die Inhalte der Videosprechstunde dürfen durch den*die Videodienstanbieter*in weder eingesehen, noch gespeichert werden.

Videodienstanbieter*innen können Speicherbegrenzungen bzw. Löschfristen im Verzeichnis der Verarbeitungstätigkeiten, in Löschkonzepten und in Verträgen zur Auftragsverarbeitung nachweisen.

2.2.5. Privacy-by-Design/ Privacy-by-Default

Es müssen Datenverarbeitungsvorgänge so gestaltet sein, dass die Grundsätze Privacy-by-Design/ Privacy-by-Default entsprechend umgesetzt werden.

Die Videosprechstunde sollte durch Maßnahmen zur Technikgestaltung und durch datenschutzfreundliche Voreinstellungen ein hohes Datenschutzniveau aufweisen. Dies kann z. B. durch Datensparsamkeit, Anonymisierung und Pseudonymisierung erreicht werden. Bei Auswahlmöglichkeiten sollte die datensparsamste Option voreingestellt sein.

Bei Webtracking-Tools wäre der Verzicht auf Tracking die datenschutzfreundlichste Voreinstellung. Sollte ein Web-Tracking-Tool genutzt werden, so ist im Cookie-Banner die Option voreinzustellen, dass nur technisch notwendige Cookies verarbeitet werden. Einwilligungsbegehren müssen im Einklang mit den Anforderungen an eine Einwilligung gemäß Art. 7 DSGVO, s. auch Kapitel 2.1.3, eingeholt werden und möglichst datenschutzfreundlich gestaltet werden.

Die Umsetzung des Kriteriums Datenschutz durch Technikgestaltung kann z. B. durch den Einsatz ISO 27001-zertifizierter Rechenzentren unterstützt werden.

Als Nachweis dienen insb. PDF-Versionen der entsprechenden Webformulare (z. B. Registrierung, Kontaktformular), die Datenschutzerklärung oder auch entsprechende Prozessbeschreibungen sowie, soweit vorhanden, Zertifikate zur IT-Sicherheit des Rechenzentrums, z. B. gemäß ISO 27001.

2.2.6. Informationspflichten

Es muss sichergestellt werden, dass Nutzer*innen kostenlos und in transparenter Form über die Datenverarbeitung sowie den Nutzungsbedingungen im Rahmen der Videosprechstunde informiert werden. Die Nutzungsbedingungen müssen vollständig in deutscher Sprache im Vorfeld ohne vorherige Anmeldung online abrufbar sein.

Die Datenschutzerklärung muss den*der Nutzer*in ermöglichen, sich bereits vor Beginn der Datenerhebung zu informieren. Diese muss folgende Inhalte umfassen:

Auflistung jeglicher Datenverarbeitungsvorgänge im Zusammenhang mit der Videosprechstunde, wie z. B.:

- Besuch der Webseite,
- Registrierung,
- Kontaktformular,
- Newsletter,
- Durchführung der Videosprechstunde,
- vertragsbedingte Kundendatenerfassung,
- etc.

sowie in diesem Zusammenhang für jeden Verarbeitungsvorgang folgende Informationen zum Zeitpunkt der Erhebung der Daten, sofern die Erhebung bei der betroffenen Person erfolgt:

- Art der Daten,
- Rechtsgrundlage der Datenverarbeitung,
- im Fall von Art. 6 Abs. 1 lit. f DSGVO (berechtigtes Interesse) die berechtigten Interessen des*der Videodienstanbietern*in/Dritten,
- Zweck der Datenverarbeitung,
- Speicherdauer, sofern nicht bestimmbar die entsprechenden Kriterien für die Festlegung der Dauer,
- Empfänger*in der Daten,
- die Verantwortliche Stelle,
- Betroffenenrechte des Art. 12 (Auskunftsrecht sowie das Recht auf Berichtigung, Löschung, Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung und das Recht auf Datenübertragbarkeit),
- Bestehen eines Beschwerderechts bei der zuständigen Aufsichtsbehörde,
- sofern eine Einwilligung eingeholt wurde, die Möglichkeiten zur Ausübung des Widerspruchsrechts,

- Name und Kontaktdaten des*der Videodienstanbieter*in sowie. ggf. des*der Vertreters*in/Datenschutzbeauftragten,
- bei automatisierter Entscheidungsfindung einschließlich Profiling, aussagekräftige Informationen zur involvierten Logik, Tragweite und angestrebten Auswirkungen,
- ggf. die Absicht einer Drittstaatenübermittlung/Übermittlung an internationale Organisationen sowie in diesem Zusammenhang die einschlägigen Informationen gemäß Art. 45ff. DSGVO bzw. ein Verweis gemäß Art. 46 DSGVO auf geeignete oder angemessene Garantien sowie die Möglichkeit des Erhalts einer Kopie zu den Garantien und
- ob die Bereitstellung der personenbezogenen Daten vertraglich oder gesetzlich verpflichtend/für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die Daten bereitzustellen sowie mögliche Folgen der Nichtbereitstellung.

Die Datenschutzerklärung sollte jederzeit leicht abrufbar sein. Sie kann z. B. auf der Webseite im Frame eingebunden werden – sofern vorhanden trifft dies auch auf die Cookie-Richtlinie zu. Dadurch kann der*die Nutzer*in jederzeit direkt auf die Datenschutzerklärung bzw. Cookie-Richtlinie zugreifen.

Bei der Erteilung einer Einwilligung für das Setzen technisch nicht notwendiger Cookies ist insbesondere darauf zu achten, dass entweder über die Datenschutzerklärung oder ein entsprechendes Consent-Tool über die Möglichkeiten eines Opt-Out in transparenter Weise informiert wird.

Als Nachweis eignen sich z. B. die Datenschutzerklärung und, sofern vorhanden, die Cookie-Richtlinie.

2.2.7. Auftragsverarbeitung

Werden Daten im Zusammenhang mit der Videosprechstunde im Auftrag verarbeitet, muss mit den jeweiligen Dienstleistern*innen ein Vertrag zur Auftragsverarbeitung (AV-Vertrag) konform zu Art. 28 DSVGO schriftlich oder in elektronischer Form geschlossen werden. Ein AV-Vertrag muss die Regelungen aus Art. 28 Abs. 3 S. 2 DSGVO aufweisen, insbesondere folgende Inhalte:

- ein zu dokumentierendes Weisungsrecht des*der Verantwortlichen,
- Verpflichtung zur Vertraulichkeit,
- das Ergreifen erforderlicher technisch und organisatorischer Maßnahmen gemäß Art. 32 DSGVO,
- Bedingungen für die Inanspruchnahme der Dienste eines*einer weiteren Auftragsverarbeiters*in,
- Pflicht des*der Auftragsverarbeiters*in zur Unterstützung des*der Verantwortlichen mittels geeigneter technisch und organisatorischer Maßnahmen bei der Beantwortung von Anträgen hinsichtlich Kapitel III DSGVO (Betroffenenrechte),
- den*die Verantwortlichen*Verantwortliche bei der Einhaltung der in den Art. 32 bis 36 DSGVO genannten Pflichten zu unterstützen,
- Regelung bzgl. Löschung/Rückgabe der Daten nach Vertragsbeendigung und

- Wahlrecht zur Überprüfung/Inspektion/Nachweis.

Bitte beachten Sie auch die besonderen Anforderungen der Anlage 31b zum BMV-Ä an den Einsatz von Auftragsverarbeitern in Drittstaaten, hierzu mehr in Kapitel 1.6.

Als Nachweis sind AV-Verträge gem. Art 28 DSGVO der eingesetzten Auftragsverarbeiter sowie die Dokumentation von Auditierungen/Kontrollen einzureichen.

Bei AV-Verträgen gem. Art. 28 DSGVO ist zu beachten, dass sie beidseitig unterschrieben (elektronisch ausreichend) und aktuell sind.

2.2.8. Audit

Beim Einsatz von Dienstleistern*innen zur Auftragsverarbeitung gemäß Art. 28 DSGVO muss u. a. sichergestellt werden, dass jeder dieser Dienstleister*innen vor Beginn der Datenverarbeitung und sodann regelmäßig kontrolliert werden. Dazu müssen Auditplanungen und Lieferantenkontrollen vorliegen.

Für jeden*jede Dienstleister*in sollte die übernommene Zuständigkeit sowie die damit verbundene Aufgabe dargelegt werden. In regelmäßigen Kontrollen sollte z. B. durch Überprüfung, Bewertung und Evaluierung die Wirksamkeit von Maßnahmen gemäß Art. 32 Abs. 3 lit. d DSGVO bei eingesetzten Auftragsverarbeitern sichergestellt werden. Die Kontrollen der Auftragsverarbeiter*innen (z. B. auch auf Dokumentenbasis) sollten dokumentiert werden.

Als Nachweis dienen z. B. Dokumentationen von durchgeführten Kontrollen bei Dienstleistern, auch auf Dokumentenbasis sowie Auditberichte und Zertifikate zur IT-Sicherheit der Rechenzentren, z.B. gemäß ISO 27001.

2.3. Technisch-organisatorische Maßnahmen (TOM)

Gemäß § 2 Abs. 1 der Anlage 31b zum BMV-Ä haben die Vertragsärzte*innen im Hinblick auf die Sicherheit der Verarbeitung der Daten in ihren Räumlichkeiten und IT-Systemen zu gewährleisten, dass die erforderlichen technischen und organisatorischen Maßnahmen eingehalten werden. Videodienstanbieter*innen müssen Behandelnden bei der rechtskonformen Nutzung des Dienstes bestmöglich unterstützen, z. B. indem Behandelnde in den AGB entsprechend dazu verpflichtet werden.

Daneben muss der*die Videodienstanbieter*in selbst geeignete technisch-organisatorische Maßnahmen ergreifen.

Zur Festlegung der geeigneten Maßnahmen ist im Vorfeld eine Analyse durchzuführen, zu dokumentieren sowie in regelmäßigen Abständen zu aktualisieren.

Die technischen und organisatorischen Maßnahmen müssen sich aus der o. g. Analyse ergeben sowie dokumentiert und nach dem Stand der Technik aktualisiert werden.

Der aktuelle Stand der Technik bei der Verschlüsselung ergibt sich vor allem aus der Technischen Richtlinie 02102 des Bundesamtes für Sicherheit in der

Informationstechnik in der jeweils aktuell gültigen Fassung.[1] So entspricht z. B. eine Verschlüsselung nach TLS 1.1 oder 1.2 dem alten Stand der Technik und TLS 1.3 dem aktuellen Stand der Technik. Das bedeutet eine Verschlüsselung nach TLS 1.1. muss auf TLS 1.3. aufgebessert werden.

Im Rahmen der Evaluierung sind als Nachweis die Dokumentation aller technischen und organisatorischen Sicherheitsmaßnahmen (TOMs) für die Webseite und die Videosprechstunde nach Art. 32 DSGVO - differenziert nach Standorten und Zugriffen sowie die im Vorfeld durchgeführte Risikoanalyse einzureichen.

2.3.1. Zutrittskontrolle

Es sind geeignete Maßnahmen zur Zutrittskontrolle zu implementieren. Das sind Maßnahmen, die den Zutritt unberechtigter Personen zur physischen Infrastruktur (Räumlichkeiten und Standorte), in denen die Verarbeitung personenbezogener Daten stattfindet, unterbindet.

Geeignete Maßnahmen können physische Hindernisse sein wie z. B. Zäune, Sicherheitsschlösser- und Schließsysteme, Pförtner*in, Besucherbücher, etc. Das Bürogebäude sollte z. B. mit modernsten Sicherheits- und Zugangskontrollsystemen ausgestattet sein und Systeme in zertifizierten Hochsicherheits-Datenzentren genutzt werden. Eine Zertifizierung von genutzten Rechenzentren nach ISO 27001 27017, 27018 und/oder 9001 kann die Einhaltung dieser Anforderung unterstützen.

2.3.2. Zugangskontrolle

Es sind geeignete Maßnahmen zur Zugangskontrolle zu implementieren. Das sind Maßnahmen, die vor einer unbefugten Nutzung von Datenverarbeitungsanlagen und vor möglichen Schäden schützen. Dies kann z. B. mittels eines Passwortverfahrens oder einer Verschlüsselung umgesetzt werden.

Um die Anforderungen des § 2 Abs. 2, 3 und 4 der Anlage 31b zum BMV-Ä umzusetzen, soll die Übertragung der Videosprechstunde mittels einer Peer-to-Peer-Verbindung zwischen Vertragsärzte*innen und Patienten*innen ohne Nutzung eines zentralen Servers, erfolgen. Beim Abweichen von einem Peer-to-Peer-Verfahren müssen geeignete technische und organisatorische Maßnahmen getroffen werden, sodass ein angemessenes Schutzniveau für die personenbezogenen Daten besteht.

Der*Die Videodienstanbieter*in muss zudem gewährleisten, dass sämtliche Inhalte der Videosprechstunde während des gesamten Übertragungsprozesses nach dem Stand der Technik Ende-zu-Ende verschlüsselt sind. Der Stand der Technik ergibt sich insb. aus der Technischen Richtlinie 02102 des Bundesamtes für Sicherheit in der Informationstechnik in der jeweils aktuell gültigen Fassung., vgl. des § 2 Abs. 3 der Anlage 31b zum BMV-Ä.

[1] Die Richtlinien BSI TR- 02102-1 – BSI-TR-02102-4 finden Sie unter: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr-02102.html (Abrufbar April 2021).

2.3.3. Zugriffskontrolle

Es sind geeignete Maßnahmen zur Zugriffskontrolle zu implementieren. Das sind Maßnahmen, die gewährleisten, dass keine unberechtigten Personen auf Daten zugreifen und so die Daten unbefugt lesen, verändern, kopieren oder entfernen können.

Geeignete Maßnahmen können Berechtigungskonzepte, Protokollierung oder. eine Passwort-Richtlinie (mindestens 8 Zeichen, einschließlich Zahlen, Symbole, Buchstaben, Großbuchstaben. Offensichtliche Passwörter sind unzulässig) sein.

Gemäß § 2 Abs. 4 der Anlage 31b zum BMV-Ä dürfen sämtliche Inhalte der Videosprechstunde durch den*die Videodienstanbieter*in weder eingesehen noch gespeichert werden können. Die Metadaten/technischen Verbindungsdaten müssen nach spätestens drei Monaten gelöscht werden und dürfen nur für die zur Abwicklung der Videosprechstunde notwendigen Abläufe genutzt werden. Die Weitergabe der Daten ist untersagt.

Gemäß § 2 Abs. 5 der Anlage 31b zum BMV-Ä darf der Videodienst keine schwerwiegenden Sicherheitsrisiken aufweisen. Als schwerwiegende Risiken gelten insb. alle Risiken des Videodienstes, die im Open Web Application Security Project (OWASP) TOP 10 Katalog in der Fassung von 2017[2] beschrieben sind.

Zur Erfüllung dieses Kriteriums ist ein Penetrationstest eines beim Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifizierte Pentester*innen erforderlich. Der Test muss gängige Angriffsszenarien berücksichtigen, u.a. OWASP Top 10, Cross-Site Request Forgery, Clickjacking.[3] Der vorgelegte Penetrationstestbericht darf zum Evaluierungszeitpunkt nicht älter als 6 Monate sein. Ergeben sich im Bericht Abweichungen, muss der*die Videodienstanbieter*in nachweisen können, dass diese abschließend behoben wurden.

2.3.4. Transport- und Weitergabekontrolle

Es sind geeignete Maßnahmen zur Transport- und Weitergabekontrolle zu implementieren. Das sind Maßnahmen, die gewährleisten, dass bei einer elektronischen Übertragung kein unbefugter Zugriff, z. B. zum Kopieren der Daten, möglich ist.

Geeignete Maßnahmen können z. B. sein: VPN, IPSec oder Verschlüsselung der Datenträger und Kommunikation.

Die Konten der Patienten*innen und Ärzte*innen sollten gegen unbefugten Zugriff geschützt werden, z. B. über eine begrenzte Anzahl an Fehl-Login-Versuchen oder durch automatischen Zeitablauf offener Sitzungen ohne Interaktion nach einer definierten Zeit. Das Unterlassen personenbezogenen Daten auf Endgeräten zu speichern trägt zur Transport- und Weitergabekontrolle bei.

---

2 Dokument abrufbar unter: https://owasp.org/www-project-top-ten/2017/de/ (abrufbar April 2021).

3 Eine Liste der beim BSI zugelassenen Personen finden Sie hier: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/zertifizierung-und-anerkennung_node.html 8abrufbar April 2021).

2.3.5. Trennungskontrolle

Es sind geeignete Maßnahmen zur Trennungskontrolle zu implementieren. Das sind Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten nicht zusammen verarbeitet werden.

Geeignete Maßnahmen können getrennte Systeme sein (z. B. durch die Verwendung unterschiedlicher Datenbanken kann eine Verquickung von getrennt zu verarbeitenden Daten ausgeschlossen werden).

2.3.6. Eingabekontrolle

Es sind geeignete Maßnahmen zur Eingabekontrolle zu implementieren. Das sind Maßnahmen, die sicherstellen, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen verändert, entfernt oder eingegeben worden sind.

Geeignete Maßnahmen können z. B. sein: Protokollierung in manueller oder in automatisierter Form. Findet die Protokollierung mittels Software statt, so ist zu überprüfen, inwiefern die Protokolldaten personenbezogene Daten enthalten und sicherzustellen, dass die Löschfristen bei Vorliegen eines Personenbezugs eingehalten werden.

Folgende Informationen können z. B. protokolliert werden:

- Änderungen an Daten, Anwendungen und Systemen mit Zeitpunkt,
- verwendeter Benutzer*innen-Account,
- Aktivitäten von Administratoren*innen,
- Dokumentation der Eingabeprogramme oder
- Erfassung gescheiterter Zugriffsversuche

2.3.7. Verfügbarkeitskontrolle

Es sind geeignete Maßnahmen zur Verfügbarkeitskontrolle zu implementieren. Das sind Maßnahmen, die gewährleisten, dass die Daten gegen zufälligen Verlust oder Zerstörung geschützt sind.

Geeignete Maßnahmen können sein: Einsatz einer Firewall, Datensicherung, Serverraumsicherheit (Klima & Brandschutz), unterbrechungsfreie Stromversorgung (USV) oder redundante Netzanbindung.

Es sollte eine Backup- und Wiederherstellungsrichtlinie implementiert sein.

2.3.8. Pseudonymisierung/ Anonymisierung

Maßnahmen zur Pseudonymisierung und Anonymisierung müssen, wo erforderlich, ergriffen werden. Es ist zwischen der Anonymisierung und Pseudonymisierung zu unterscheiden.

Bei reinen Pseudonymen (z.B. IP-Adressen, ID-Nummern, Patientennummern) liegt immer noch ein Personenbezug vor, sodass es sich um personenbezogene Daten handelt. Eine "echte" Pseudonymisierung kann jedoch wie eine Art Verschlüsselung

wirken, etwa, indem ein Dritter die Pseudonyme erhält, jedoch niemals Zugriff auf die Identifizierungsmerkmale (z. B. in Form einer Regerenzdatei) haben wird, um die Daten wieder zu de-pseudonymisieren / zu identifizieren. Das bedeutet, dass die bei der Pseudonymisierung entstehenden zusätzlichen Informationen zur Re-Identifizierung der Person gesondert aufbewahrt werden müssen.

Für die Beurteilung einer hinreichenden Anonymisierung/ Pseudonymisierung sollten die konkreten Umstände und insb. der aktuelle Stand der Technik berücksichtigt werden[4].

Als Nachweis dient z. B. ein Kryptografiekonzept sowie die Konfiguration der Verschlüsselung im Hinblick auf die Speicherung aller personenbezogenen Daten (z. B. IP-Adressen, Namen).

2.3.9. Überprüfung, Bewertung und Evaluierung

Videodienstanbieter*innen müssen die Wirksamkeit der umgesetzten technischen und organisatorischen Maßnahmen regelmäßig dokumentiert überprüfen, bewerten und evaluieren. Hierzu ist ein Datenschutz-Managementsystem aufrecht zu erhalten. Abweichungen müssen analysiert und korrigiert werden.

Neben eigenen Kontrollen der Wirksamkeit eingesetzter Maßnahmen unterstützt auch der gemäß § 2 Abs. 5 Anlage 31b zum BMV-Ä geforderte Penetrationstest durch BSI-zertifizierte Pentester die Einhaltung dieses Kriteriums.

Als Nachweis dienen z. B. Auditberichte und Zertifikate zur IT-Sicherheit der Rechenzentren, z.B. gemäß ISO 27001.

2.4. Datenschutz-Management

2.4.1. Datenschutzbeauftragte(r)

Im Rahmen von Videosprechstunden muss grundsätzlich gemäß den Anforderungen der Art. 37 ff. DSGVO ein*e Datenschutzbeauftragte*r bestellt werden. Insbesondere sind die Kontaktdaten der Fachkraft für Datenschutz zu veröffentlichen sowie der Aufsichtsbehörde bekannt zu geben. Datenschutzbeauftragte müssen die erforderliche Fachkunde besitzen, ausreichend Ressourcen für Ihre Tätigkeit zur Verfügung haben und dürfen keinem Interessenkonflikten unterliegen.

Als Nachweis dient z. B. die Bestellurkunde, ein Nachweis zur Fachkunde und die Unabhängigkeit sowie die Auflistung aller Aufgaben.

2.4.2. Verpflichtung auf Vertraulichkeit/ Schulungen

Videodienstanbieter*innen müssen die Vertraulichkeit der verarbeiteten Daten gewährleisten. Daher müssen Beschäftigte auf die Vertraulichkeit und die Einhaltung

[4] Die Richtlinien BSI TR- 02102-1 – BSI-TR-02102-4 finden Sie unter: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr-02102.html (Abrufbar April 2021).

des Datenschutzes verpflichtet und belehrt werden sowie regelmäßig entsprechende Schulungen zum Datenschutz und zur Datensicherheit durchgeführt werden.

Als Nachweis dienen z. B. eine Dokumentation aller bereits durchgeführten sowie geplanten künftigen Schulungen, Schulungsplaner, Dokumente zu den Schulungsinhalten, Teilnehmerlisten und Musterdokumente zu Verschwiegenheits- und Vertraulichkeitsverpflichtungen.

2.4.3. Verzeichnis der Verarbeitungstätigkeiten

Gemäß Art. 30 DSGVO ist eine schriftliche Dokumentation und Übersicht über Verfahren zu führen, bei denen personenbezogene Daten verarbeitet werden (Verzeichnis über die Verarbeitungstätigkeiten). Im Verzeichnis der Verarbeitungstätigkeiten sind alle datenrelevanten Vorgänge der Videosprechstunde aufzuführen. Das Verzeichnis der Verarbeitungstätigkeiten muss regelmäßig aktualisiert werden.

Folgende Inhalte muss insbesondere das Verzeichnis der Verarbeitungstätigkeiten gemäß Art. 30 DSGVO des*der Videodienstanbieters*in aufweisen:

- Namen und die Kontaktdaten des*der Videodienstanbietern*in und ggf. des*der Vertreters*in des*der Videodienstanbietern*innen sowie der Fachperson für Datenschutz,
- die Verarbeitungszwecke,
- Beschreibung der Kategorien betroffener Personen sowie Kategorien der personenbezogenen Daten,
- die Kategorien von Empfängern*innen der Daten, einschließlich Empfänger*innen in Drittländern/von internationalen Organisationen,
- ggf. Übermittlungen von personenbezogenen Daten an ein Drittland/internationale Organisation sowie bei Art. 49 Abs. 1 UAbs. 2 DSGVO genannten Datenübermittlungen die Dokumentierung geeigneter Garantien,
- sofern möglich, Fristen für die Löschung der verschiedenen Datenkategorien und
- sofern möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32 Abs. 1. DSGVO.

Videodienstanbieter*innen sollten z. B. Löschfristen für alle zu verarbeitenden personenbezogenen Daten im Verzeichnis der Verarbeitungstätigkeiten festhalten. Dies betrifft z. B. die Speicherdauer der IP-Adresse auf dem Videoserver sowie der Videosprechstunde.

Als Nachweis dient das Verzeichnis der Verarbeitungstätigkeit (VVT) gemäß Art. 30 DSGVO bzw. ein entsprechender Auszug, der die Datenverarbeitungstätigkeiten im Zusammenhang mit der Videosprechstunden beschreibt.

2.4.4. Datenschutz-Folgenabschätzung (DSFA)

Der*Die Videodienstanbieter*in ist verantwortliche Stelle und da aufgrund der Verarbeitung von medizinischen Daten im Rahmen der Videosprechstunde ein hohes Risiko für die betroffenen Personen erwächst, muss regelmäßig eine DSFA

entsprechend der Vorgaben der Art. 35 f. DSGVO durchgeführt und dokumentiert werden. Hiervon abweichend muss der*die Videodienstanbieter*in darlegen können, warum eine DSFA nicht erforderlich ist.

Die DSFA muss gemäß Art. 36 Abs. 7 DSGVO insbesondere folgende Informationen umfassen:

- systematische Beschreibung der geplanten Verarbeitungsvorgänge sowie Zwecke der Verarbeitung,
- Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;
- Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen und
- Maßnahmen, Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird, insbesondere im Hinblick auf berechtigte Interessen und Rechte der betroffenen/sonstigen Personen.

Als Nachweis dient die dokumentierte DSFA.

2.5. Meldung von Datenschutzverletzungen

Der*Die Videodienstanbieter*in muss sicherstellen, dass geeignete Maßnahmen für den Fall einer Datenschutzverletzung entsprechend den Regelungen der Art. 33f. DSGVO ergriffen werden.

Die Meldung muss mindestens Informationen gemäß Art. 33 Abs. 3 DSGVO enthalten:

Der gesamte Vorgang muss dokumentiert werden.

Als Nachweis dienen z. B. Musterdokumente, Prozessbeschreibungen, Mitarbeiteranweisungen und Richtlinien zum Umgang mit Betroffenenrechten und Datenpannen

2.6. Datenverarbeitung außerhalb der EU

Gemäß § 2 a Abs. 3 ist die Verarbeitung von personenbezogenen Daten im Rahmen der Videosprechstunde außerhalb der EU/ des EWR, auch im Auftrag, nur in Staaten zulässig, zu denen die EU-Kommission einen gültigen Angemessenheitsbeschluss gemäß Art. 45 DSGVO veröffentlicht hat[5] (z. B. aktuell für die Schweiz, eventuell geplant für Großbritannien), oder in einem nach § 35 Abs. 7 des Ersten Buches Sozialgesetzbuch gleichgestellten Staat. Die Verarbeitung personenbezogener Daten in Drittstaaten auf Grundlage von EU-Standardvertragsklauseln oder Binding Corporate Rules ist hingegen nicht zulässig.

Hintergrund hierfür ist, dass sich der Wortlaut der Anlage 31b zum BMV-Ä an § 3 Abs. 3 Digitale Gesundheitsanwendungen-Verordnung – DiGAV vom 08.04.2020 orientiert, vgl. für nachfolgende Ausführungen die Handreichung des BfArM für DiGA-Anbieter „Informationen zur Zulässigkeit der Datenverarbeitung außerhalb Deutschlands im

5 Liste abrufbar unter: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (abrufbar April 2021).

Zusammenhang mit dem Prüfverfahren des BfArM gemäß § 139e Fünftes Buch Sozialgesetzbuch (SGBV)"[6].

Das bedeutet, dass der Einsatz von Dienstleister*innen mit (selbstständiger) Niederlassung oder Tochterunternehmen in der EU, aber einem Mutterkonzern in den USA (oder in anderen Drittstaaten) nur bei hinreichender Gewähr für die Unterbindung einer Übertragung personenbezogener Daten gemäß DSGVO an das Mutterunternehmen im Rahmen der Videosprechstunde eingesetzt werden dürfen.

Werden im Rahmen der Videosprechstunde Dienstleister*innen mit (selbstständiger) Niederlassung oder Tochterunternehmen in der EU, aber einem Mutterkonzern in den USA (oder anderen Drittstaaten) eingesetzt, so ist die Datenverarbeitung zulässig, sofern die personenbezogenen Daten verschlüsselt sind und die Schlüssel von den Videosprechstundenanbietern*innen in der EU selbst verwaltet oder gespeichert werden (beispielsweise Customer-Managed Encryption Keys, CMEK)[7]. Das bedeutet, dass alle der vier folgenden Voraussetzungen erfüllt sein müssen:

- Vorliegen eines Data Processing Agreements (DPA) mit dem*der Dienstleister*in, auf dessen Grundlage die Datenverarbeitung erfolgt,
- Serverstandort innerhalb der EU,
- Verwaltung oder Speicherung des Schlüssels durch den*die Videosprechstundenanbieter*in selbst und
- der Transport von Informationen als auch die Verschlüsselung selbst müssen stets nach aktuellem Stand der Technik erfolgen.

Verwenden Sie als Videosprechstundenanbieter*in den Service einer europäischen Tochtergesellschaft eines US-amerikanischen Unternehmens, die Daten ausschließlich in der EU/EWR/Schweiz oder in Drittländern mit Angemessenheitsbeschluss verarbeitet und ein Drittstaatentransfer in die USA liegt nicht vor, so ist die Datenverarbeitung zulässig, sofern der*die jeweilige Auftragnehmer*in des*der Videodienstanbieters*in zusichert, dass kein Datentransfer in die USA und auch keine Datenverarbeitungen in den USA durchgeführt werden, und bestätigt, dass auch im Fall von Herausgabeverlangen von US-Behörden keine Daten zur Verfügung gestellt und auch nicht an das Mutterunternehmen herausgegeben werden. Die jeweiligen Unternehmen müssen zusichern, dass sie in jedem Fall eines Herausgabeverlangens den Rechtsweg beschreiten und ausschöpfen. Selbst im Fall eines höchstrichterlichen Urteils, das eine Herausgabepflicht bestätigt, ist Art. 48 DSGVO zu beachten, wonach ein Datentransfer auch im Falle eines rechtskräftigen Urteils nur erfolgen darf, wenn sie auf eine in Kraft befindliche internationale Übereinkunft, wie etwa ein Rechtshilfeabkommen zwischen dem ersuchenden Drittland und der Union oder einem Mitgliedstaat, gestützt sind. In jedem Fall eines Herausgabeverlangens hat der*die Auftragnehmer*in den*der

---

6 Dokument abrufbar unter: https://www.bfarm.de/SharedDocs/Downloads/DE/Medizinprodukte/Datenverarbeitung_au%C3%9Ferhalb_Deutschlands_FAQ.pdf?__blob=publicationFile&v=3 (abrufbar April 2021).

7 Informationen zur Verschlüsselung vgl. „Technische Richtlinie TR-02102-2 Kryptographische Verfahren“ vom BSI:https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2.pdf?__blob=publicationFile&v=2 (abrufbar Mai 2021).

Videosprechstundenanbieter*in unverzüglich über das Bestehen des Verlangens sowie über die Abhilfemaßnahmen und mögliche Rechtsstreitigkeiten sowie deren Verfahrensstand und Fortschritt zu informieren. Dies muss vorab vertraglich zugesichert werden. Darüber hinaus ist ein Herausgabeverlangen ggf. auch anderen Stellen und Behörden anzuzeigen.

Werden Pseudonyme (z.B. IP-Adressen, ID-Nummern, Patientennummern) durch Subunternehmer*innen im Rahmen der Videosprechstunde verarbeitet, kann dies bei einer "echten" Pseudonymisierung, die wie eine Art Verschlüsselung wirkt, zulässig sein. Der*Die als kritisch eingestufte (Sub-)Dienstleister*in darf zwar die Pseudonyme erhalten, jedoch niemals Zugriff auf eine Referenzzuordnungsdatei oder andere Identifizierungsmerkmale haben, um die Daten wieder zu de-pseudonymisieren/zu identifizieren. Kann angenommen bzw. festgestellt werden, dass die Daten für Drittstaatenunternehmen/Behörden anonym sind, ist die Verarbeitung von pseudonymisierten Daten in Drittstaaten in diesem Fall ggf. zulässig. Ganz im Sinne des größtmöglichen Schutzes der Patienten*innen und Versicherten*innen läge die Hoheit über die Daten dann alleine bei der Stelle, die über diese Referenzdatei verfügt. Diese Stelle muss die Vorgaben des § 2a Abs. 2 der Vereinbarung erfüllen.

Die Verarbeitung von anonymisierten Daten in Drittstaaten/durch Dienstleister mit Drittstaatenbezug ist hingegen zulässig, da keine „Verarbeitung von personenbezogenen Daten“ vorliegt.

Die Anonymisierung/Pseudonymisierung der personenbezogenen Daten muss durch Sie als Videodienstanbieter*in schlüssig und plausibel geprüft (1) und im Detail nachweisbar dokumentiert (2) werden.

Als Nachweis dient je nach Anwendungsfall z. B. eine verbindliche Bestätigung der eingesetzten europäischen Tochtergesellschaft, dass auch im Fall von Herausgabeverlangen von US-Behörden keine Daten zur Verfügung gestellt und auch nicht an das Mutterunternehmen herausgegeben werden sowie eine Bestätigung darüber, dass in jedem Fall eines Herausgabeverlangens der Rechtsweg beschritten und ausschöpft wird, unter Beachtung des Art. 48 DSGVO.

Ein weiterer Nachweis wäre eine vertragliche Zusicherung, in jedem Fall eines Herausgabeverlangens den*die Videosprechstundenanbieter*in unverzüglich über das Bestehen des Verlangens sowie über die Abhilfemaßnahmen und mögliche Rechtsstreitigkeiten sowie deren Verfahrensstand und Fortschritt zu informieren.

Aktuelle SCC im Rahmen des DPA sowie einen Nachweis, dass die personenbezogenen Daten verschlüsselt und die Schlüssel vom*von der Videosprechstundenanbieter*in in der EU selbst verwaltet oder gespeichert werden. Dies kann bspw. mittels Nachweis einer echten Pseudonymisierung durch z. B. Prozessbeschreibungen, Beschreibung eingesetzter kryptografischer Verfahren (Kryptografiekonzept) sowie durch die Konfiguration der Verschlüsselung im Hinblick auf die Speicherung aller personenbezogenen Daten (z. B. IP-Adressen, Namen) oder durch Dokumentation der Prüfung für das Vorliegen von Anonymisierung/Pseudonymisierung der personenbezogenen Daten geschehen.

Als Videosprechstundenanbieter*in setzen Sie Amazon Web Service Luxembourg (AWS Europe) ein. Folgende Voraussetzungen müssen in diesem Anwendungsbeispiel konkret erfüllt sein:

- Vorliegen eines Data Processing Agreements (DPA) mit Amazon Web Service, auf dessen rechtlicher Grundlage die Datenverarbeitung erfolgt,
- Serverstandorte innerhalb der EU z.B. in Frankfurt (KEIN Einsatz von Cloudflare o.ä.),
- Verschlüsselung sämtlicher personenbezogener Daten,
- Verwaltung und Speicherung des Schlüssels durch die Anbieter*innen der Videosprechstunde (z.B. unter Verwendung des Customer-Managed Encryption Keys, CMEK); dabei sollten die Anbieter*innen z.B. selbst Schlüsselpaare (public und private Keys der asymmetrischen Kryptographie) erzeugen, verwalten sowie abspeichern,
- der Transport von Informationen als auch die Verschlüsselung selbst müssen stets nach aktuellem Stand der Technik erfolgen; z.B. Transportverschlüsselung nach TLS, Verschlüsselung nach EC2.

2.7. Betroffenenrechte

Es muss ein Konzept zum Umgang mit Betroffenenanfragen vorliegen. Der*Die Videodienstanbieter*in muss über geeignete Maßnahmen verfügen, die den betroffenen Personen die Ausübung ihrer Betroffenenrechte der Kapitel .1.7.1. bis 1.7.8. ermöglichen. Die Ausübung der Rechte darf nicht behindert werden.

Anhand der Datenschutzerklärung sollten sich z. B. Nutzer*innen der Videosprechstunde jederzeit über den Umgang mit personenbezogenen Daten informieren und ihre Rechte jederzeit unkompliziert ausüben können.

Als Dokumentation eignet sich z.B. die Datenschutzerklärung sowie der Umgang mit Nutzerdaten, FAQ, Konzepte und Richtlinien zum Umgang mit Betroffenenanfragen, Richtlinien für Mitarbeiter*innen, Prozessbeschreibungen, Löschkonzepte, Berechtigungskonzepte.

2.7.1. Auskunftspflicht

Der*Die Videodienstanbieter*in muss Datenverarbeitungsvorgänge, Prozesse sowie Applikationen so implementieren, dass sichergestellt wird, dass Betroffene eine Auskunft gemäß Art. 15 DSGVO darüber einholen können, ob eine Datenverarbeitung Ihrer Daten stattfindet und welche Daten verarbeitet werden.

Vom Auskunftsanspruch umfasst gemäß Art. 15 DSGVO sind grundsätzlich Informationen zum:

- Verarbeitungszweck,
- Art der Daten,
- Speicherdauer und
- Empfänger der Daten.

Zudem muss der*die Videodienstanbieter*in der betroffenen Person eine unentgeltliche Kopie mit diesen Informationen in einem gängigen elektronischen Format zur Verfügung stellen. Dazu ist es erforderlich, dass der*die Videodienstanbieter*in den Betroffenen eindeutig identifiziert.

2.7.2. Fristen bei Informationspflicht auf Antrag

Der*Die Videodienstanbieter*in muss Datenverarbeitungsvorgänge, Prozesse sowie Applikationen so implementieren, dass sichergestellt wird, dass Betroffene bei der Stellung eines Antrags gemäß den Art. 15 bis 22 DSGVO, die Informationen unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags, zur Verfügung gestellt werden.

Gemäß Art. 12 DSGVO muss u. a. die Informationen in leicht zugänglicher Form, präzise, transparent, verständlich sowie in klarer und einfacher Sprache übermittelt werden.

Als Nachweis eignen sich z.B. Konzepte und Richtlinien zum Umgang mit Betroffenenanfragen, Prozessbeschreibungen und entsprechende Richtlinien für Mitarbeiter.

2.7.3. Berichtigung

Der*Die Videodienstanbieter*in muss Datenverarbeitungsvorgänge, Prozesse sowie Applikationen so implementieren, dass sichergestellt wird, dass auf Verlangen betroffener Personen gemäß Art. 16 DSGVO unrichtige Daten berichtigt werden.

Dies kann z. B. der*die Videodienstanbieter*in durch ein Rechte-Management umsetzen, welches vorsieht, dass Daten im Benutzerprofil durch die Nutzer*innen selbstständig bearbeitet werden können, z. B. bei einem Wohnortwechsel.

Als Nachweis eignen sich z. B. Konzepte und Richtlinien zum Umgang mit Betroffenenanfragen und Berechtigungskonzepte.

2.7.4. Löschung

Der*Die Videodienstanbieter*in muss Datenverarbeitungsvorgänge, Prozesse sowie Applikationen so implementieren, dass sichergestellt wird, dass sofern die betroffene Person von Ihrem Recht auf Löschung Gebrauch macht, die Daten gelöscht werden, insbesondere wenn einer der folgenden Punkte gemäß Art 17 DSGVO vorliegt:

- Zweckerreichung,
- Widerruf der Einwilligung und Fehlen einer anderweitigen Rechtsgrundlage für die Verarbeitung,
- Widerspruch gemäß Art. 21 Abs. 1 DSGVO und Fehlen berechtigter Gründe für die Verarbeitung,
- personenbezogenen Daten wurden unrechtmäßig verarbeitet,
- Löschung ist zur Erfüllung einer rechtlichen Verpflichtung nach Unionsrecht/Recht der Mitgliedstaaten (dem der Videodienstanbieter unterliegt) erforderlich oder

- die Daten wurden in Bezug auf angebotene Dienste der Informationsgesellschaft gemäß Art. 8 Abs. 1 DSGVO erhoben.

Das Recht auf Löschung findet in den Fällen nach Art. 17 Abs. 3 DSGVO keine Anwendung. Insb. in den Fällen, in denen z. B. eine Verarbeitung aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit gemäß Art. 9 Abs. 2 Buchstaben h und i sowie Art. 9 Abs. 3 erforderlich ist, besteht kein Anspruch auf Löschung.

Als Nachweis eignen sich z. B. Konzepte und Richtlinien zum Umgang mit Betroffenenanfragen und Löschkonzepte und die Datenschutzerklärung.

2.7.5. Einschränkung

Der*Die Videodienstanbieter*in muss Datenverarbeitungsvorgänge, Prozesse sowie Applikationen so implementieren, dass sichergestellt wird, wenn die betroffene Person von Ihrem Recht auf Einschränkung der Verarbeitung gemäß Art. 18 DSGVO Gebrauch macht, die Verarbeitung gemäß Art. 18 DSGVO eingeschränkt wird.

Sofern die betroffene Person die Daten nicht selber einschränken kann, z. B. durch Benutzerprofilbearbeitung, müssen alternative Möglichkeiten für die betroffenen Personen bestehen.

Der*Die Videodienstanbieter*in muss bei einer Aufhebung der Einschränkung die betroffene Person zuvor unterrichten.

Als Nachweis eignen sich z. B. Konzepte und Richtlinien zum Umgang mit Betroffenenanfragen und die Datenschutzerklärung

2.7.6. Mitteilungspflicht

Der*Die Videodienstanbieter*in muss Datenverarbeitungsvorgänge, Prozesse sowie Applikationen so implementieren, dass gemäß Art. 19 DSGVO sichergestellt wird, dass Empfängern, denen Daten der betroffenen Person übermittelt oder offengelegt wurden, jede Berichtigung, Löschung oder Einschränkung mitgeteilt und die betroffene Person auf deren Verlangen über diese Empfänger unterrichtet wird.

Als Nachweis eignen sich z. B. Konzepte und Richtlinien zum Umgang mit Betroffenenanfragen und die Datenschutzerklärung

2.7.7. Datenübertragbarkeit

Der*Die Videodienstanbieter*in muss Datenverarbeitungsvorgänge, Prozesse sowie Applikationen so implementieren, dass sichergestellt wird, dass sofern die betroffene Person von Ihrem Recht auf Datenübertragbarkeit gemäß Art. 20 DSGVO Gebrauch macht, dass die Daten in einem strukturierten, gängigen und maschinenlesbaren Format zur Verfügung gestellt werden, sofern:

1. die Verarbeitung auf einer Einwilligung oder auf einem Vertrag beruht und
2. die Verarbeitung mithilfe automatisierter Verfahren erfolgt.

Als Nachweis eignen sich z. B. Konzepte und Richtlinien zum Umgang mit Betroffenenanfragen.

2.7.8. Widerspruch

Der*Die Videodienstanbieter*in muss Datenverarbeitungsvorgänge, Prozesse sowie Applikationen so implementieren, dass sichergestellt wird, dass die betroffene Person ihr Recht auf Widerspruch gemäß Art. 21 DSGVO ausüben kann.

Ein Widerspruchsrecht besteht z. B., wenn die Datenverarbeitung aufgrund von Art. 6 Abs. 1 oder lit. f DSGVO (berechtigtes Interesse) erfolgt.

Der*Die Videodienstanbieter*in muss dann sicherstellen, dass jederzeit Widerspruch gegen die Verarbeitung von Daten aufgrund eines berechtigten Interesses eingelegt werden kann. Der*Die Videodienstanbieter*in darf gemäß Art. 21 Abs. 1 S. 2 DSGVO die Daten nicht mehr verarbeiten, es sei denn:

- es liegen schutzwürdige Gründe für die Verarbeitung vor, dass die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, die zwingend vom Videodienstanbieter nachgewiesen wurden
- oder die Verarbeitung dient der Geltendmachung/Ausübung/Verteidigung von Rechtsansprüchen.

Dabei dürfen die Rechte Dritter nicht beeinträchtigt werden, vgl. Art. 15 Abs. 4 DSGVO, Art. 20 Abs. 4 DSGVO.

Ein Widerspruch sollte üblicherweise über die im Impressum genannten Kontaktdaten geltend gemacht werden können. Werden beispielsweise Cookies auf Grundlage eines berechtigten Interesses gesetzt, muss die betroffene Person Widerspruch einlegen können, etwa über ein Kontaktformular oder über die Cookie-Einstellungen.

Als Nachweis eignen sich z. B. Konzepte und Richtlinien zum Umgang mit Betroffenenanfragen und die Datenschutzerklärung

3. Anforderungen zur Informationstechniksicherheit

3.1. Verpflichtung zur Einhaltung Sicherheit bei Ärzten

Der*Die Videodienstanbieter*in muss Vertragsärzt*innen verpflichten bei der Nutzung der Videosprechstunde im Hinblick auf die Sicherheit der Verarbeitung der Daten in seinen Räumlichkeiten und IT-Systemen zu gewährleisten, dass die erforderlichen technischen und organisatorischen Maßnahmen eingehalten werden.

Als Nachweis eignen sich z. B. Vertragliche Vereinbarung, welche mit Ärzt*innen geschlossen werden.

3.2. Übertragung der Videosprechstunde

Die Übertragung der Videosprechstunde soll über eine Peer-to-Peer-Verbindung zwischen Vertragsärzt*innen und Patient*innen oder der Pflegekraft, ohne Nutzung eines zentralen Servers, erfolgen. Bei einem Abweichen von einem Peer-to-Peer-Verfahren ist der Videodienstanbieter verpflichtet, durch geeignete technische und organisatorische Maßnahmen ein angemessenes Schutzniveau zu gewährleisten.

Als Nachweis eignen sich z. B. Verfahrens-, Prozessbeschreibungen, Testzugänge zur Applikation sowie Beschreibungen zur Darlegung der Umsetzung der Anforderung (etwa Funktionsbeschreibung, Schnittstellenbeschreibungen)

3.3. Ende-zu-Ende-Verschlüsselung

Der*Die Videodienstanbieter*in muss gewährleisten, dass sämtliche Inhalte der Videosprechstunde während des gesamten Übertragungsprozesses nach dem Stand der Technik Ende-zu-Ende verschlüsselt sind. Der Stand der Technik ergibt sich insbesondere aus der Technischen Richtlinie 02102 des Bundesamtes für Sicherheit in der Informationstechnik in der jeweils aktuell gültigen Fassung.

Als Nachweis eignen sich z. B. Verfahrens-, Prozessbeschreibungen, Testzugänge zur Applikation sowie Beschreibungen zur Darlegung der Umsetzung der Anforderung (etwa Funktionsbeschreibung, Schnittstellenbeschreibungen)

3.4. Absicherung der Inhalte der Videosprechstunde & Metadaten

Sämtliche Inhalte der Videosprechstunde dürfen durch den*die Videodienstanbieter*in weder eingesehen noch gespeichert werden können. Die Metadaten/technischen Verbindungsdaten müssen nach spätestens drei Monaten gelöscht werden und dürfen nur für die zur Abwicklung der Videosprechstunde notwendigen Abläufe genutzt werden. Die Weitergabe der Daten ist untersagt.

Als Nachweis eignen sich z. B. Verfahrens-, Prozessbeschreibungen, Testzugänge zur Applikation sowie Beschreibungen zur Darlegung der Umsetzung der Anforderung (etwa Funktionsbeschreibung, Schnittstellenbeschreibungen), Löschkonzepte, das Verzeichnis der Verarbeitungstätigkeiten

3.5. Ausschluss schwerwiegender Sicherheitsrisiken

Anforderung

Der Videodienst darf keine schwerwiegenden Sicherheitsrisiken aufweisen. Als schwerwiegende Risiken gelten insbesondere alle Risiken des Videodienstes, die im Open Web Application Security Project (OWASP) TOP 10 Katalog in der Fassung von 2017 beschrieben sind.

Als Nachweis eignen sich z. B. Penetrationstestbericht eines BSI-zertifizierten Penetrationstesters sowie Maßnahmenpläne zur Umsetzung gefundener Schwachstellen.

5. Auflistung üblicher Nachweise

Zur Evaluierung der Videosprechstunde durch unsere Evaluierenden sind zahlreiche Dokumente und Nachweise erforderlich.

Im Folgenden möchten wir einige dieser Nachweise nennen, damit diese für eine Evaluierung entsprechend vorbereitet werden können. Zu beachten ist, dass diese Aufzählung nicht abschließend ist.

- Vertragliche Dokumentationen, AGB o.ä. zwischen Anbieter*in und den Nutzern der Videosprechstunde (VSS)
- Handbücher, FAQs, Bedienungsanleitungen
- bei eingesetzten Subunternehmern: Verträge konform zu Art. 28 DSGVO (Auftragsverarbeitung) (mit allen unterbeauftragten Dienstleistern*innen, z.B. Rechenzentren)
- aktueller Penetrationstest für die relevanten Server, nicht älter als 6 Monate
- Muster der eingesetzten Verpflichtungserklärung für Beschäftigte des Unternehmens
- Nachweis über die Bestellung eines/einer Datenschutzbeauftragten und dessen Fachkunde
- Dokumentation der technischen und organisatorischen Sicherheitsmaßnahmen für die Webseite und die Videosprechstunde nach Art. 32 DSGVO
- soweit vorhanden: Zertifikate zur IT-Sicherheit des Rechenzentrums, z.B. gemäß ISO 27001
- Verfahrensverzeichnis nach Art. 30 DSGVO bzw. ein entsprechender Auszug, der die Webseiten beschreibt.
- PDF-Versionen von Webformularen (z. B. Registrierung, Kontaktformular) und der Datenschutzerklärung
- Dokumente zum Datenschutzmanagement
  - Richtlinien für Mitarbeiter
  - Prozessbeschreibungen
  - Löschkonzept
  - Berechtigungskonzept
  - Dokumentation von Auditierungen/Kontrollen/Schulungen
  - Risikoanalyse zu den TOMs

6. Hinweise zu den Anforderungen des § 5 Abs. 1 Anlage 31b zum BMV-Ä

Bitte beachten Sie, dass Sie als Anbieter*in weitere inhaltliche Anforderungen gemäß § 5 Abs. 2 Buchst. c) Anlage 31b zum BMV-Ä in einer Selbstauskunft gemäß Anlage zur Anlage 31b zum BMV-Ä bestätigen müssen[8]. Diese Anforderungen werden im Rahmen

[8] Auch hierfür gibt es ein Formular auf der Seite der KBV, abrufbar unter: https://www.kbv.de/html/videosprechstunde.php (abrufbar April 2021).

der Evaluierung nicht abgedeckt. Der Vollständigkeit halber sollen Sie aber im Folgenden kurz aufgelistet werden.

Der*Die für die Videosprechstunde genutzte Videodienstanbieter*in bzw. Videodienst muss neben den Anforderungen des § 2 und § 2a die folgenden Anforderungen erfüllen:

1. Die Vertragsärzt*innen müssen sich für den Videodienst registrieren.
2. Der Videodienst darf einen Zweitzugang für das Praxispersonal vorhalten.
3. Dieser darf ausschließlich zu organisatorischen Zwecken im Zusammen-hang mit der Videosprechstunde genutzt werden. Mit dem Zweitzugang darf keine Videosprechstunde durchgeführt werden.
4. Patienten*innen und Pflegekräfte müssen den Videodienst nutzen können, ohne sich vorher registrieren zu müssen. Der Klarname des*der Patienten*in bzw. der Pflegekraft muss für Vertragsärzt*innen erkennbar sein.
5. Die eingesetzte Software muss bei Schwankungen der Verbindungsqualität bezüglich der Ton- und Bildqualität adaptiv sein.
6. Die Nutzungsbedingungen müssen vollständig in deutscher Sprache und ohne vorherige Anmeldung online abrufbar sein.
7. Das Schalten von Werbung im Rahmen der Videosprechstunde ist untersagt.
8. Der*Die Videodienstanbieter*in muss eine aktuelle Bescheinigung nach Anlage 2 beim GKV-Spitzenverband und der Kassenärztlichen Bundesvereinigung schriftlich vorgelegt haben.

Sie erhalten bei der KBV entsprechende Formulare für diese Selbstauskunft.