AOK VERLAG

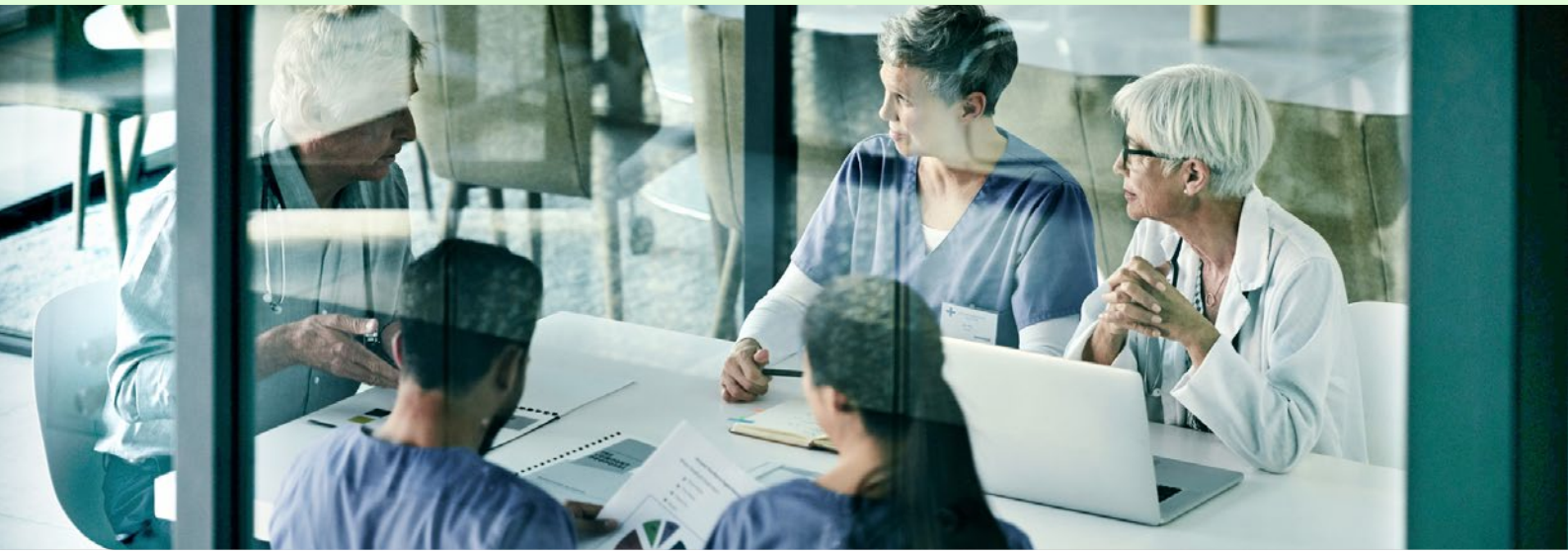
Datenschutz im Blick

Newsletter für den Datenschutz im Gesundheitswesen

www.aok-verlag.info/ds-im-blick

Ausgabe Juli/August 2021 | **Seite 1**

Inhalt



Das Betriebsrätemodernisierungsgesetz

Ende Mai dieses Jahres wurde das Betriebsrätemodernisierungsgesetz verabschiedet. Dieses regelt unter anderem in einem neuen § 79a Betriebsverfassungsgesetz (BetrVG) das datenschutzrechtliche Verhältnis zwischen Betriebsrat und Arbeitgeber. Dies ist deshalb so spannend, da lange Zeit umstritten war, ob der Betriebsrat Teil des Arbeitgebers als Verantwortlichem ist oder datenschutzrechtlich eine eigene verantwortliche Stelle darstellt.

Sven Venzke-Caprarese

Was regelt § 79a BetrVG?

§ 79a BetrVG regelt, dass der Betriebsrat bei der Verarbeitung personenbezogener Daten die Vorschriften über den Datenschutz einzuhalten hat. Dies ist eigentlich eine Selbstverständlichkeit und hätte nicht zwingend einer eigenen Regelung bedurft. Allerdings wird auch klargestellt, dass, soweit der Betriebsrat zur Erfüllung der in seiner Zuständigkeit liegenden Aufgaben personenbezogene Daten verarbeitet, der Arbeitgeber der für die Verarbeitung Verantwortliche im Sinne der datenschutzrechtlichen Vorschriften ist. An dieser Stelle wird es interessant, denn durch diese Regelung wird ein jahrelanger juristischer Streit beigelegt. Der Arbeitgeber ist für das, was der Betriebsrat im Rahmen seiner Aufgaben tut, datenschutzrechtlich verantwortlich. Hieraus ergeben sich eine Reihe von Pflichten, denen der Arbeitgeber nachkommen muss.

Unter anderem muss dieser die Verarbeitungstätigkeiten des Betriebsrats im Verzeichnis der Verarbeitungstätigkeiten (VVT) dokumentieren. Dies stellt auch die Gesetzesbegründung klar, wonach der Betriebsrat zwar keine Pflicht habe, ein eigenes Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DS-GVO zu führen, allerdings müsse das Verzeichnis des Arbeitgebers auch die Verarbeitungstätigkeiten des Betriebsrats enthalten.

Arbeitgeber und Betriebsrat sind nach dem Gesetzeswortlaut zudem verpflichtet, sich gegenseitig bei der Einhaltung der datenschutzrechtlichen Vorschriften zu unterstützen. Die Gesetzesbegründung stellt hierzu fest: „Die beiderseitige Unterstützungspflicht von Arbeitgeber und Betriebsrat bei der Einhaltung der datenschutzrechtlichen Vorschriften beruht auf der datenschutzrechtlichen Verantwortlichkeit des Arbeitgebers einerseits und der innerorganisatorischen Selbstständigkeit und Weisungsfreiheit des Betriebsrats andererseits." An dieser Stelle zeigt sich bereits, dass die Umsetzung in der Praxis in dem einen oder anderen Fall ggf. nicht ganz einfach sein wird.

Die Gesetzesbegründung geht ferner auf eine Unterstützungspflicht bei Auskunftsersuchen ein, was sinnvoll erscheint.

Ein etwaiger Widerspruch zur gesetzlichen Regelung ergibt sich aus der Gesetzesbegründung aber auch. Denn demnach habe „der Betriebsrat innerhalb seines Zuständigkeitsbereichs eigenverantwortlich die Umsetzung technischer und organisatorischer Maßnahmen zur Gewährleistung der Datensicherheit im Sinne der Artikel 24 und 32 der Datenschutz-Grundverordnung sicherzustellen." Hier kann ggf. schnell die Frage aufkommen, was dies im Hinblick auf die Pflichten des Arbeitgebers nach der DS-GVO bedeuten mag, der ja durch § 79a BetrVG nun eigentlich für die Datenverarbeitung verantwortlich ist und damit auch für die technischen und organisatorischen Maßnahmen.

Im Hinblick auf die Stellung und die Aufgaben des Datenschutzbeauftragten stellt die Gesetzesbegründung hingegen klar, dass sich diese nach Art. 38 und 39 DS-GVO richten und die Aufgaben des bzw. der Datenschutzbeauftragten somit auch gegenüber dem Betriebsrat als Teil der verantwortlichen Stelle bestehen. Soweit erforderlich, sollte der Betriebsrat nach dem Wortlaut der Gesetzesbegründung die Beratung durch den Datenschutzbeauftragten in Anspruch nehmen.

Ein etwaiges Konfliktfeld wird durch eine zusätzliche Regelung entschärft: Datenschutzbeauftragte sind gegenüber dem Arbeitgeber zur Verschwiegenheit verpflichtet über Informationen, die Rückschlüsse auf den Meinungsbildungsprozess des Betriebsrats zulassen.

Konfliktpotenzial entschärfen und die Umsetzung des Datenschutzes auf Augenhöhe regeln

Die neue Regelung trägt durchaus Konfliktpotenzial in sich. Dies wird schon dadurch deutlich, dass selbst die Gesetzbegründung auf die innerorganisatorische Selbstständigkeit und Weisungsfreiheit des Betriebsrats einerseits hinweist und andererseits der Arbeitgeber für die Datenverarbeitung verantwortlich und somit rechenschaftspflichtig ist.

Zudem wird der Betriebsrat gelegentlich auch Daten verarbeiten, von denen der Arbeitgeber eigentlich keine Kenntnis nehmen dürfte. Und dies geht über die Prozesse der Meinungsbildung des Betriebsrats, die das Gesetz ausdrücklich anspricht, hinaus. Denn wie ist z.B. mit Daten umzugehen, die dem Betriebsrat von Beschäftigten

vertraulich mitgeteilt wurden und die im Rahmen etwaiger Betroffenenanfragen aber vom Arbeitgeber als verantwortliche Stelle beauskunftet werden müssten?

Sowohl Betriebsrat als auch Arbeitgeber sollten daher jeweils ein hohes Interesse haben, die künftigen Rahmenbedingungen der Zusammenarbeit zu regeln.

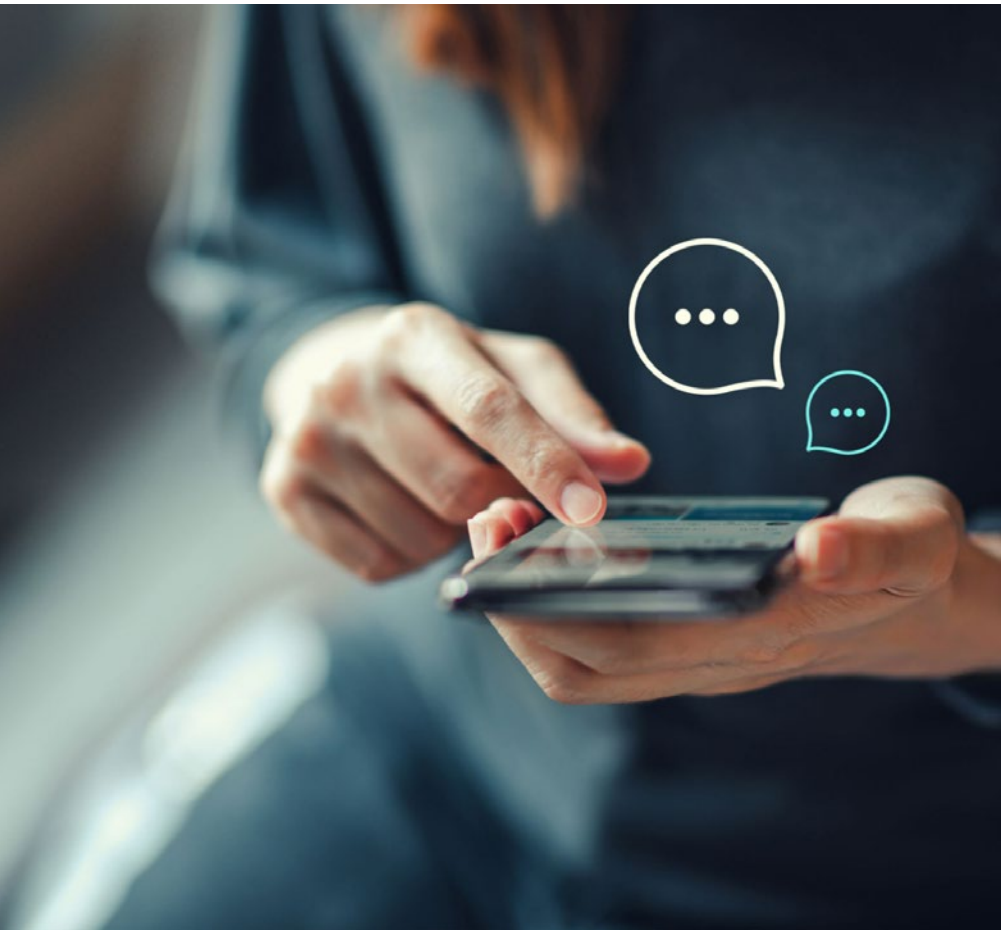
Hierbei kann es konkret um folgende Fragen gehen:

- Wer stellt in welcher Form die Informationen zur Verfügung, die zur Erstellung eines VVT nach Art. 30 DS-GVO in Bezug auf die Verarbeitungstätigkeiten des Betriebsrats erforderlich sind? Hier gibt es ggf. zahlreiche Verarbeitungstätigkeiten, die dokumentiert werden können – z.B. in Bezug auf die Verarbeitung von vom Arbeitgeber zur Verfügung gestellten Unterlagen (etwa Bruttogehaltslisten), zur Organisation der internen Betriebsratskommunikation, zur Teilnahme einzelner Mitglieder an z.B. BEM-Gesprächen, zur Anfertigung von Protokollen etc. An dieser Stelle erscheint es durchaus möglich, dass der Arbeitgeber die Erstellung des Verzeichnisses – sofern eine entsprechende Bereitschaft des Betriebsrats besteht – auch in großen Teilen dem Betriebsrat erlaubt und sich die Dokumentation zu eigen macht. Eine Pflicht des Betriebsrats, ein eigenes Verzeichnis zu führen besteht jedoch nach der Gesetzesbegründung ausdrücklich nicht.

- Auch im Hinblick auf die Umsetzung von Informationspflichten nach Art. 13 DS-GVO können sich Fragen ergeben: Wie informiert der Betriebsrat z.B. Beschäftigte, die sich mit Fragen an ihn wenden, und die eine weitere (erstmalige) Datenerhebung nach sich ziehen? Eine weitere Frage: Wie werden neue Betriebsratsmitglieder über eine etwaige Verarbeitung ihrer Daten innerhalb des Betriebsrats informiert?

- Zudem muss geklärt werden, wie der Betriebsrat in die Lage versetzt wird, die erforderlichen Datenschutzkenntnisse zu erlangen, um seinen Aufgaben datenschutzkonform nachgehen zu können. Hier kann es sinnvoll ein, dass sich Arbeitgeber und Betriebsrat über ein Schulungs- und Sensibilisierungskonzept abstimmen, zumal neue Betriebsratsmitglieder ggf. das erste Mal mit sensiblen Beschäftigtendaten in Berührung kommen. Auch auf die besondere Verschwiegenheit, den sorgsamen Umgang mit Dokumenten und das Planen von Gesprächssituationen sollte hier eingegangen werden. Zudem stellen sich in der Praxis immer wieder Herausforderungen bei der Frage, ob Verschwiegenheitspflichten auch innerhalb des Betriebsrats gelten, z.B. wenn ein Mitglied mit Einwilligung an dem BEM-Gespräch eines Beschäftigten teilnimmt.

- Die technischen und organisatorischen Maßnahmen müssen vom Betriebsrat nach der Gesetzesbegründung teilweise eigenverantwortlich umgesetzt werden. Andererseits ist der Arbeitgeber für alle nach Art. 32 DS-GVO getroffenen Maßnahmen in der Rechenschaftspflicht. Hier macht es Sinn, sich noch einmal über die Dokumentation der technischen und organisatorischen Maßnahmen Gedanken zu machen. Häufige Fragen betreffen in der Praxis in diesem Zusammenhang die Absicherung des Betriebsratsbüros, die Nutzung



der IT-Infrastruktur des Arbeitgebers und teilweise sogar der eigenen, separaten Infrastruktur des Betriebsrats – sofern vorhanden. Es sollte zudem dokumentiert werden, wie Unterlagen und Datenträger des Betriebsrats vernichtet werden. Immer wieder spannend ist auch, welche E-Mail-Adressen den Mitgliedern des Betriebsrats für ihre Tätigkeit zur Verfügung stehen. Denn in der Regel existiert für den Betriebsrat u. a. ein Postfach, auf das alle Mitglieder Zugang haben. Hier gibt es ganz unterschiedliche Gestaltungsmöglichkeiten. Vermieden werden sollte, dass auf das Gruppenpostfach über einen Gruppenaccount zugegriffen wird und sich Mitglieder die Zugangsdaten teilen. Der Zugang sollte grundsätzlich über personalisierte Accounts gewährleistet werden.

- Die Nutzung von Messenger Apps wie WhatsApp, Austauschplattformen wie Dropbox oder Online-Services wie doodle sollten auch angesprochen werden. In der Praxis stehen innerhalb von Unternehmen gelegentlich nur wenig Anwendungen zur Verfügung, die ein gemeinsames Arbeiten mit mehreren Personen unterstützen. Hier muss aber sichergestellt werden, dass nicht auf unzulässige Dienste zurückgegriffen wird. Stattdessen muss die Bereitstellung datenschutzkonformer Alternativen besprochen werden.

- Besonders relevant ist auch, wie mit Auskunftsanfragen von betroffenen Personen umgegangen wird. Wer gibt Auskunft, wenn eine betroffene Person vom Betriebsrat Auskunft über gespeicherte Daten haben möchte? Hier wäre es ggf. problematisch, wenn eine solche Auskunft über den Tisch des Arbeitgebers laufen müsste. Auf der anderen Seite muss auch der Fall betrachtet werden, wie damit umgegangen wird, wenn Beschäftigte gegenüber dem Arbeitgeber als verantwortliche Stelle die Beauskunftung und Kopien all ihrer personenbezogenen Daten fordern. Konkret stellt sich in diesen Situationen die Frage, wie an dieser Stelle mit etwaigen Daten umgegangen wird, die der Betriebsrat auch gegenüber dem Arbeitgeber vertraulich speichert. An dieser Stelle müssen die entsprechenden Prozesse definiert, geregelt und ggf. im Einvernehmen organisatorisch übertragen werden.

- Besprochen werden sollte auch die Frage, wie Datenpannen in der Sphäre des Betriebsrats aufgearbeitet und ggf. gemeldet werden. Hier sollte vorab eine klare Regelung getroffen werden. Denn wer sich hierüber erst im Fall der Datenpanne Gedanken macht, verliert im Zweifel wertvolle Zeit.

- Auch die zukünftige Zusammenarbeit mit dem Datenschutzbeauftragten sollte gemeinsam mit Arbeitgeber, Betriebsrat und Datenschutzbeauftragtem besprochen werden. Dabei sind auch die Regelungen der Gesetzesbegründung zu berücksichtigen.

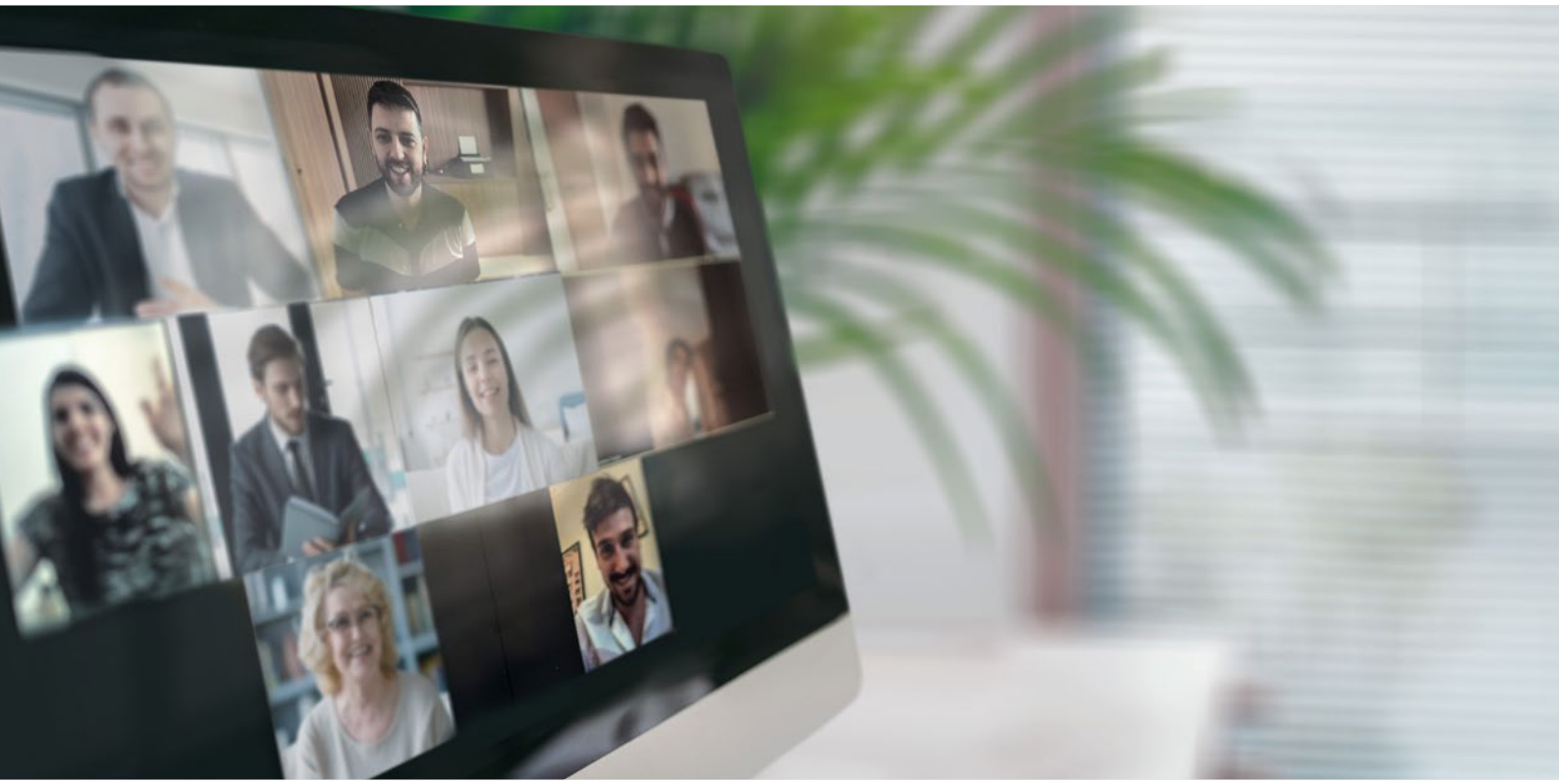
Weitere Themen, die geklärt werden sollten, sind

- der Umgang mit etwaig vom Betriebsrat eigenständig gewünschter Hard- und Software sowie der Umgang mit ausschließlich vom Betriebsrat eingesetzten Dienstleistern
- Fragen rund um etwaig erforderliche Datenschutzfolgenabschätzungen, sofern diese durch eine Tätigkeit des Betriebsrats ausgelöst würden
- die Definition von Löschfristen und deren Umsetzung.

Grundsätzlich kann es sinnvoll sein, die Konkretisierung der gegenseitigen Unterstützung sowie etwaige im Einvernehmen getroffene Aufgabendelegationen bzw. -übernahmen und Prozesse in einer Betriebsvereinbarung zu regeln. Das Ziel sollte es sein, dass zwischen Arbeitgeber und Betriebsrat unter Beteiligung des Datenschutzbeauftragten ein Konsens im Hinblick auf die künftige Organisation des Datenschutzes im Betriebsrat hergestellt wird.

Fazit

Gesundheitseinrichtungen sollten das neue Betriebsrätemodernisierungsgesetz und die Änderungen des § 79a BetrVG intern prüfen. Sofern bislang die Ansicht vertreten wurde, der Betriebsrat sei eine eigene verantwortliche Stelle oder sofern der Betriebsrat in der Vergangenheit aus Unsicherheit datenschutzrechtlich gar nicht näher betrachtet wurde, können nun zahlreiche Aufgaben anstehen. Diese sollten mit allen Beteiligten besprochen und auf Augenhöhe unter Zugrundelegung des gegenseitigen Unterstützungsprinzips geregelt werden.



Videokonferenzen mit Zoom

Die Corona-Pandemie hat unser Leben nachhaltig verändert. Insbesondere im Bereich der zwischenmenschlichen Kommunikation gab es einen elementaren Wechsel von persönlichen Terminen zu Videokonferenzen. Diese Entwicklung wird auch nach einem Ende der Pandemie in vielen Bereichen Bestand haben und das Arbeitsleben neben den dann endlich wieder stattfindenden persönlichen Kontakten massiv erleichtern.

Dr. Sebastian Ertel

Eine Umfrage in den USA im Sommer 2020 ergab einen Marktanteil von 23 Prozent für Zoom. Dieses Jahr dürfte er ungleich höher liegen, zumal der Anbieter, die Zoom Inc., das Tool weiterentwickelt und den Datenschutz erhöht hat.

Relativ unbemerkt wurde eine Zoom-Variante für den Gesundheitsbereich auf den Markt gebracht. (https://t1p.de/jdkc)

Zoom im Gesundheitswesen

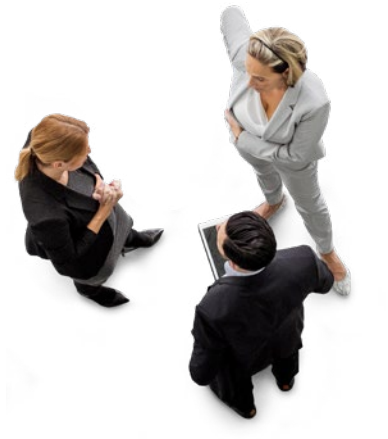
Was unterscheidet die beiden Zoom-Varianten voneinander? Das Zoom für das Gesundheitswesen (nachfolgend Zoom Gesundheit) wurde anhand der Vorgaben des HIPAA entwickelt. HIPAA steht für Health Insurance Portability and Accountability Act. Hierbei handelt es sich um ein US-amerikanisches Gesetz, welches für Gesundheitseinrichtungen gilt. Dieses definiert die Anforderungen für die Verarbeitung von Gesundheitsdaten. Derzeit gibt es keine offizielle Zertifizierung, sodass jedes Unternehmen eine eigene Konformitätsroutine definiert und entscheiden kann, ob die HIPAA-Anforderungen erfüllt sind. Im Falle von Zoom wurde die Prüfung durch eine dritte Partei, konkret durch das American Institute of Certified Public Accountants (AICPA) durchgeführt. Die AICPA hat laut Zoom festgestellt, dass Zoom die erforderlichen Kontrollen implementiert hat, um Gesundheitsdaten gemäß den HIPAA-Anforderungen zu schützen. Das Attest ist auf der Seite von Zoom leider nicht abrufbar.

Verschlüsselung

Standardmäßig verschlüsselt Zoom den Inhalt von Videositzungen auf Anwendungsebene mit TLS 1.2 mit 256-Bit Advanced Encryption Standard (AES) 256-Bit-Algorithmus. Hierbei handelt es sich allerdings nur um eine Transportverschlüsselung. Zusätzlicher Schutz kann durch die

Aktivierung der Ende-zu-Ende-Verschlüsselung erreicht werden. Nachteil der Ende-zu-Ende-Verschlüsselung ist, dass bestimmte Funktionen nicht genutzt werden können, u. a.:

- Beitreten vor dem Gastgeber
- Cloud-Aufzeichnung
- Live-Streaming
- Live-Transkription
- Breakout-Räume
- Umfragen
- Teilnahme per Telefon
- Private Chats zwischen einzelnen Teilnehmern



Standort der Server

Der Standort der Server kann frei gewählt werden. Standardmäßig werden die Server ausgewählt, die sich in der Region befinden, in der das Nutzerkonto angelegt wurde.

Die Wahl der Rechenzentrumsregionen bezieht sich jedoch ausschließlich auf aktiv genutzte Datensätze. Für ruhende Daten kann eine solche Einstellung nicht getroffen werden.

Es gibt eine europäische Region, sodass europäische Kommunikationsdaten innerhalb Europas verbleiben.

Schrems II-Urteil

Aufgrund des Schrems II-Urteils des EuGH besteht immer eine Datenschutzproblematik, wenn personenbezogene Daten in Drittstaaten verarbeitet werden oder der Dienstleister seinen Sitz in einem Drittstaat hat.

Unverschlüsselt werden in jedem Fall die Metadaten der Kommunikation übertragen. Hierbei handelt es sich um die Begleitdaten der Kommunikation, insbesondere, wer (welche IP-Adressen) wann und wie lange mit wem bei welchem Datenvolumen kommuniziert hat. Diese Daten müssen zwangsnotwendig unverschlüsselt verarbeitet werden, da andernfalls die Kommunikation nicht aufgebaut werden kann.

Dieser Umstand, aber in jedem Fall die Tatsache, dass sich der Sitz der Zoom Video Communications, Inc. in den USA, einem Drittstaat befindet, hat zur Folge, dass eine datenschutzkonforme Nutzung von Zoom nicht ohne weiteres möglich ist:

Das Schrems II-Urteil bedeutete das Aus für das sogenannte privacy shield. Hierbei handelte es sich um ein Abkommen, dass die Grundlage für einen datenschutzkonformen Datentransfer zwischen der EU und den USA ermöglichte. Auch die sogenannten EU-Standardvertragsklauseln, als Alternative zum weggefallenen privacy shield, können nur dann noch als Grundlage herangezogen werden, wenn zusätzliche Schutzmaßnahmen für die Schaffung eines adäquaten Schutzniveaus getroffen wurden.

Von Zoom gibt es hierzu leider keine entsprechenden Informationen. Auf dem Unternehmensblog wird lediglich mitgeteilt:

„Das Urteil ändert nichts am Datenfluss für unsere Services. Klarstellend betonen wir, dass Sie die Zoom-Services in Übereinstimmung mit dem EU-Recht auch weiterhin nutzen können.“ (https://t1p.de/e220)

Eine solche adäquate Schutzmaßnahme ist jedoch in jedem Fall die Ende-zu-Ende-Verschlüsselung

der Kommunikation. Durch diese kann ein unvermittelter Zugriff auf die Kommunikationsdaten ausgeschlossen werden. Da diese nicht standardmäßig aktiviert ist, muss sie vom Administrator eingerichtet werden. Dies sollte so erfolgen, dass eine Deaktivierung durch die Nutzer ausgeschlossen ist.

Die entsprechende Konfiguration muss vom Datenschutzbeauftragten geprüft und im Rahmen der zu erstellenden Datenschutz-Folgenabschätzung bei der Bewertung mitberücksichtigt werden.

Ob die Ende-zu-Ende-Verschlüsselung als alleinige zusätzliche Schutzmaßnahmen ausreichend ist, um die vom EuGH angesprochenen Anforderungen zu erfüllen, kann noch nicht belastbar beantwortet werden. Hier sind die Positionierung der Datenschutzaufsichtsbehörden und etwaige Gerichtsentscheidungen abzuwarten.

Möglicherweise werden sich im Hinblick auf die Standardvertragsklauseln kurzfristig Änderungen ergeben. Die EU-Kommission hat am 4. Juni neue Vertragstexte veröffentlicht. Diese können zukünftig gegebenenfalls dazu führen, dass mit deren Abschluss ein angemessenes Datenschutzniveau wieder angenommen werden kann. An dieser Stelle lohnt sich also die weitere Beobachtung.

Fazit

Zoom kann für den Einsatz im Gesundheitsbereich grundsätzlich in Betracht kommen, wenn mit Blick auf das Schrems-II-Urteil zusätzliche Maßnahmen zum Schutz der Daten getroffen wurden. Hierzu zählt zwingend die Aktivierung der Ende-zu-Ende-Verschlüsselung.

Kurznotiz

Standards für Messenger im Gesundheitswesen werden definiert

Sich einmal schnell mit Kolleg*innen über den Dienstplan oder die Behandlung von Patient*innen austauschen, ist sicher ein Wunsch von vielen Mitarbeitenden im Gesundheitswesen. Zwar steht mit dem Kommunikationsdienst KIM eine Funktionalität in den Startlöchern (Arztpraxen sind ab 01.10.2021 verpflichtet, KIM zu nutzen), die einen sicheren E-Mail-Austausch von Gesundheitsdaten ermöglicht. KIM ist jedoch nicht unbedingt für die kurzfristige Kommunikation, wie sie Messenger-Dienste bieten, geeignet.

Die gematik GmbH hat angekündigt, bis Oktober 2021 die Standards für einen Messenger im Gesundheitsbereich, einen Telematik-Infrastruktur-Messenger (TI-Messenger) zu definieren. Anhand dieser Kriterien sollen Unternehmen in der Lage sein, eigene Messengerlösungen zu entwickeln. Diese werden nach einer erfolgreichen Prüfung durch die gematik GmbH von dieser zugelassen und können sich dann auf dem Markt positionieren.

© AOK-Verlag GmbH | Lilienthalstraße 1-3 | 53424 Remagen | Tel 02642 931-333 | Fax 02642 931-215
Mail: fachinfo@aok-verlag.de | Web: http://www.aok-verlag.info | Herausgeber: AOK-Verlag GmbH, Remagen
Geschäftsführung: Frank Schmidt | Redaktion: Prof. Dr. Benedikt Buchner, Dr. Sebastian Ertel, Sven Venzke-Caprarese
Der Inhalt des vorliegenden Newsletters ist mit größter Sorgfalt zusammengestellt worden.
Eine Haftung für die Angaben übernimmt der Verlag jedoch nicht. | Bildnachweise: GettyImages, AOK-Verlag