Anmerkungen zum Whitepaper der Datenschutzkonferenz

Technische Datenschutzanforderungen an Messenger-Dienste im Krankenhausbereich – Ein Vergleich mit Join

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder haben am 07.11.2019 das Whitepaper zu Datenschutzanforderungen klinischer Messenger veröffentlicht. Es kann über die Website der Datenschutzkonferenz heruntergeladen werden.

Nachfolgend vergleichen wir die im Whitepaper genannten Anforderungen mit den Funktionen der Kommunikations-App Join.

I. Messenger-Applikation

Erfüllt	Anforderungen der Datenschutzaufsichtsbehörde	Wie werden die Anforderungen von Join erfüllt?
✓	a) Die Applikation muss die Möglichkeit bieten, die Nutzerinnen und Nutzer entsprechend Art. 13 DS-GVO über die mit der Nutzung verbundene Datenverarbeitung zu unterrichten. Die Informationen müssen in einem klar erkennbaren Bereich (z.B. Hinweise zum Datenschutz, Datenschutzerklärung) für den jederzeitigen Zugriff hinterlegt sein.	Die App Join bietet unter Einstellungen > Nutzungsbedingungen Hinweise zur Datenverarbeitung und zum Datenschutz.
✓	b) Die Applikation muss über die Möglichkeit verfügen, die Nutzung bzw. den Zugriff auf die darüber gespeicherten Daten an eine eigene vorherige Authentifizierung (z.B. PIN, Fingerabdruck etc.) zu knüpfen. Diese kann auf bestriebssystemseitige Funktionen zurückgreifen, muss sich jedoch vom Schutz zur Entsperrung des Mobilgeräts (siehe III.1) unterscheiden.	Die App Join ist unabhängig von der Entsperrung des Mobilgeräts und lässt sich nur nach vorheriger Authentifizierung mittels PIN, Fingerabdruck oder Gesichtserkennung öffnen und nutzen.
✓	c) Die Applikation muss über die Möglichkeit verfügen, Kontaktdaten von Kommunikationsteilnehmern in einem eigenen, vom allgemeinen Adressbuch des Smartphones getrennten Speicher abzulegen.	Die App Join greift nicht auf die Kontakte zu, die auf dem mobilen Gerät gespeichert sind. Join verfügt über ein eigenes Adressbuch innerhalb der App. So wird verhindert, dass Informationen (Nachrichten und Bilder) an nicht-registrierte Nutzer gesendet werden.

d) Die Applikation muss über eine Möglichkeit verfügen, Kontakte und zugehörige Informationen aus anderen Quellen importieren zu können.	Die App Join ermöglicht es, zum Beispiel Kontakte aus Gruppen-Chats zu den Join-Kontakten hinzuzufügen.
e) Die Applikation muss über die Möglichkeit verfügen, Nachrichten sowie Dateianhänge wie Bilder, Videos, Dokumente etc. ausschließlich in einem eigenen, von den allgemeinen Speicherbereichen des Smartphones getrennten Speicher in verschlüsselter Form abzulegen.	Die App Join ist vom allgemeinen Speicherbereich abgegrenzt. Mit Join aufgenommene Bilder und Videos oder in Join geteilte Dokumente, Bilder und Videos werden nicht im allgemeinen Speicherbereich des Smartphones gespeichert.
f) Die Applikation sollte über die Möglichkeit verfügen, Nachrichten und Dateianhänge aus anderen Quellen zu importieren.	In die App Join können Nachrichten und Dateianhänge wie Bilder, Videos und Dokumente importiert werden.
g) Die Applikation sollte die Möglichkeit bieten, für die serverseitige Authentifizierung, Verschlüsselung oder digitale Signatur benötigte Daten (z.B. Zertifikate, Schlüssel) zu importieren. Eine Kommunikation sollte nur auf der Grundlage einer verlässlichen Identifizierung und Authentifizierung der Kommunikationspartner möglich sein.	In der App Join erfolgt eine serverseitige Authentifizierung und Verschlüsselung. Zudem wird eine digitale Signatur mittels VPN zur Anmeldung an der Join-Cloud importiert. Die Kommunikationspartner in Join sind verlässlich zu identifizieren und erhalten Zugang durch eine gesicherte Authentifizierung (Tenant-Code/Tenant-ID).

h) Werden elektronische Signaturen oder andere elektronischer Zertifikate genutzt, muss ein Zertifikats-management vorhanden sein. Dies beinhaltet die Sicherstellung, dass elektronische Schlüssel oder Zertifikate eindeutig einer juristischen oder natürlichen Person zugeordnet werden, aber auch die Überprüfung der Gültigkeit der elektronischen Schlüssel bzw. Zertifikate. Insbesondere müssen kompromittierte Schlüsseln bzw. Zertifikate bzw. unbrauchbar gemacht werden können. Dabei ist unerheblich, ob das Management der genutzten Public Key Infrastructure („PKI") vom Verantwortlichen selbst betrieben wird oder von einem Dritten zur Verfügung gestellt wird.

Über das Join Admin-Panel lassen sich Nutzer (Nutzer-Zertifikat) direkt zuordnen (juristische und natürliche Person). Durch aktive Steuerungsmöglichkeiten (Löschen, Hinzufügen etc.) lassen sich nicht mehr aktuelle Zertifikate identifizieren und Zugriffe verbieten. Nutzern können Rollen und Berechtigungen (DICOM Permission, Live Video Streaming Permission, Case Permission, Lese-/Schreibe-Permission) zugeteilt werden. Der jeweilige Admin (Klinik-intern oder Allm als Service-Dienstleister) erhält immer eine Notification, sobald sich ein neuer Nutzer anmeldet. Außerdem lässt sich einstellen, ob nur bestimmte E-Mail-Adressen zur Anmeldung in Join (Tenant-ID) genutzt werden darf (Bsp: Max@Musterklinik.de).

i) Die Applikation sollte über eine Schnittstelle verfügen, die es erlaubt, sie in IT-Strukturen und -Prozesse eines Krankenhauses einzubinden (z.B. Aufspielen von Sicherheitsprofilen oder Voreinstellungen, Synchronisation mit dem Krankenhausinformationssystem, Übernahmen behandlungs-relevanter Messenger-Nachrichten als Teil der Patientendokumentation).

Die App Join verfügt über Schnittstellen, die es ermöglichen, sich mit Krankenhaus- IT-Strukturen und -Prozesse (PACS, Modalitäten (CT/MRT/EKG), RIS, KIS, etc.) zu verbinden, um Join in den Krankenhausalltag zu integrieren.

j) Die Applikation muss über die Möglichkeit verfügen, die über sie verwalteten Daten gezielt oder allgemein zu löschen (Nachrichten, Dateien, Kontakte etc.). Sie sollte über die Möglichkeit verfügen, eine Frist festzulegen, nach der solche Daten automatisiert gelöscht werden.

Über den Admin lassen sich die über Join verwalteten Daten gezielt löschen. Im Fall der anonymisierten DICOM-Dateien kann der Tenant festlegen, wann diese gelöscht werden sollen. Über das Admin-Panel können die Chat-Daten der einzelnen User gelöscht werden.

k) Soweit im Rahmen der Nutzung der Applikation Dienste Dritter zur Fehleranalyse eingebunden werden (z.B. Crashlytics), muss dies offen erkennbar dargestellt und als optional gekennzeichnet werden; die für eine Übermittlung zur Fehlersuche vorgesehenen Datenkategorien müssen klar erkennbar sein. Eine entsprechende Datenübermittlung muss in der Voreinstellung deaktiviert sein. Es muss sichergestellt sein, dass Daten, die dem Arztgeheimnis unterliegen oder Daten über das Nutzungsverhalten der Messenger-Anwender, auf diese Weise nicht unbefugt offenbart werden.

Im Fall eines Abstürzens der App Join wird automatisch ein Fehlerprotokoll an das von Allm verwaltete Repository gesendet. Diese Fehlerprotokolle werden sicher gespeichert und werden nur Personen, die an Join/Allm beteiligt sind, nach vorheriger Benutzerauthentifizierung angezeigt. Auf die Daten über das Nutzungs-verhalten und auf die Daten, die dem Arztgeheimnis unterliegen, haben unbefugte Personen keinen Zugriff.

l) Mit Blick auf die Verfügbarkeit der Daten nach Art. 32 Abs. 1 lit. b DS-GVO muss die Applikation über die Möglichkeit einer Sicherung der Kontaktdaten/Inhaltsdaten/Kommunikationsvorgänge verfügen. Soweit die Speicherung unter Einhaltung von Art. 28 DS-GVO durch einen Dienstleister übernommen wird, welcher nicht die Anforderungen des Art. 9 Abs. 3 DS-GVO erfüllt, muss die Möglichkeit bestehen, die Daten nach dem Stand der Technik vor ihrer Übergabe derart zu verschlüsseln, dass eine Entschlüsselung nur mit einem Schlüssel möglich ist, der nicht an den Dienstleister offenbart und separat gesichert wird.

Die App Join verfügt über die Möglichkeit, Kontaktdaten, Inhaltsdaten und Kommunikationsvorgänge zu sichern. Die Übermittlung der Daten erfolgt verschlüsselt an die Cloud. Der Schlüssel zur Entschlüsselung ist im Besitz von Allm und kann von keinem Mitarbeiter des Cloud-Dienstleisters genutzt werden.

m) Behandlungsrelevante Inhaltsdaten, die sich auf Patienten beziehen und auf dem Endgerät erzeugt werden (z. B. durch Kameraaufnahmen), müssen in der IT-Struktur des Krankenhauses gespeichert und über die Behandlungsdokumentation auffindbar sein können, soweit dies aus berufs- oder zivilrechtlicher Sicht geboten ist. Hierzu bedarf es nicht notwendigerweise einer speziellen, an das KIS angepassten Funktion in der Messenger-Applikation, solange sich der Prozess anderweitig effizient abbilden lässt. Vorgaben des Berufs- und Zivilrechts bleiben unangetastet.

Die App Join verfügt über Schnittstellen, die es ermöglichen, sich mit Krankenhaus- IT-Strukturen und -Prozesse (PACS, Modalitäten (CT/MRT/EKG), RIS, KIS, etc.) zu verbinden, um Join in den Krankenhausalltag zu integrieren. Behandlungsrelevante Inhalte, die auf dem Endgerät erzeugt wurden, können an die IT-Strukturen des Krankenhauses zurückspielt werden.

n) Soweit über die Applikation Bildaufnahmen verschickt werden (z.B. Patientenaufnahmen, Screenshots), bei denen darin enthaltene personenbezogene Daten für den verfolgten Zweck und die Identität aus ärztlicher Sicht nicht erforderlich sind, und die Patientenidentität vor dem Hintergrund einer sorgfältigen Behandlung ausnahmsweise verzichtbar ist, soll die Möglichkeit bestehen, Teile der Aufnahmen zu schwärzen oder anderweitig in der Darstellung auszunehmen. (Datenminimierung, vgl. Art 5 Abs. 1 lit. c, Art. 25 Abs. 1 DS-GVO)

Die App Join verfügt über umfangreiche Editierfunktionen für Fotos und Bilder. So können Patientendaten oder andere schützenswerte Informationen beispielsweise geschwärzt werden.

	o) Für die Messenger-Lösung ist durch das Krankenhaus und ggf. den beauftragten Auftragsverarbeiter ein geeigneter Nachweis darüber zu führen, dass die für die Erfüllung der Datenschutz-Grundsätze und die Gewährleistung der Sicherheit der Verarbeitung nach Art. 25 Abs. 1 bzw. 32 DS-GVO enthaltenen Funktionen effektiv implementiert wurden bzw. bei den jeweiligen Verarbeitungsvorgängen die Vorgaben der DS-GVO eingehalten werden (z.B. Zertifizierung nach Art. 42 DS-GVO (soweit verfügbar), Zertifizierung nach European Privacy Seal, BSI-Grundschutz- Zertifizierung)). Seitens des Krankenhauses sollte die Messenger-Applikation zudem anhand des Prüfkatalogs zum technischen Datenschutz bei Apps5 bewertet und das Ergebnis im Rahmen der Rechenschaftspflicht (Art. 5 Abs. 2 DS-GVO) dokumentiert werden.	Allm stellt Krankenhäusern einen Auftragsdatenverarbeitungsvertrag (ADV) zur Verfügung. Darin garantiert Allm, dass bei der Auftragsdatenverarbeitung die Grundsätze des Datenschutzes nach der DS-GVO eingehalten werden. Als Nachweis für die Umsetzung technischer und organisatorischer Maßnahmen ist Join nach ISO27001 zertifiziert. Join erfüllt außerdem die Standards nach dem Health Insurance Portability and Accountability Act (HIPAA).
	p) Die Applikation muss hinsichtlich ihrer Konfigurationseinstellungen dem Grundsatz datenschutzgerechter Voreinstellungen (Art. 25 Abs. 2 DS-GVO) entsprechen.	Die App Join erfüllt diese Vorgabe. Der Umgang mit den Daten wird durch den Nutzer ausgewählt.
	q) Die Applikation soll über (halb-)automatische Update-Verfahren verfügen.	Die App Join verfügt über automatische Update-Verfahren. Allm arbeitet kontinuierlich an der Verbesserung der App. Nutzer erhalten Updates über den App Store und Google Play Store.

II. Kommunikation

Erfüllt	Anforderungen der Datenschutzaufsichtsbehörde	Wie werden die Anforderungen von Join erfüllt?
	a) Die Vertraulichkeit und Integrität der über den Messenger-Dienst geführten ärztlichen Kommunikation muss unter Berücksichtigung des Stands der Technik über eine Ende-zu-Ende-Verschlüsselung zwischen den Kommunikationsteilnehmern gewährleistet werden (Art. 32 Abs. 1 lit. a DS-GVO).	Die App Join bietet eine verschlüsselte und sichere Datenübertragung. Die Vertraulichkeit und Integrität der geführten ärztlichen Kommunikation wird gewahrt.
	b) Soweit die Integrität der über den Messenger-Dienst kommunizierten Daten für nachfolgende Maßnahmen von Bedeutung ist, sollte die Möglichkeit bestehen, diese durch kryptografische Funktionen unter Berücksichtigung des Stands der Technik nachzuweisen (Art. 32 Abs. 1 Satz 1 DS-GVO). Weiterhin muss zur Gewährleistung der Integrität der Informationen, wenn diese für nachfolgende Maßnahmen von Bedeutung ist, dafür Sorge getragen werden, dass alle kommunizierten Daten beim Empfänger ankommen. Wird eine Mitteilung seitens eines Messengers auf mehrere Nachrichten verteilt (z.B. weil der Messenger pro Nachricht nur eine bestimmte Zeichenzahl oder Dateigröße zulässt), müssen Mechanismen integriert sein, die dem Empfänger mitteilen, ob die gesendete Mitteilung vollzählig angekommen ist oder ob einzelne Nachrichten fehlen. Dies kann z.B. durch die Ergänzung einer Prüfnummer „Nachricht x von y“ geschehen, so dass der Empfänger sieht, ob alle Nachrichten bei ihm angekommen sind.	Die Struktur des Kommunikationspfads der App Join bietet geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Join bietet eine gesendet/gelesen-Funktion und Nachrichten haben eine unbegrenzte Zeichenanzahl. Eine Überprüfung der vollständigen Übermittlung der Informationen ist so gewährleistet.

	c) Verbindungsdaten zu der über den Messenger-Dienst geführten Kommunikation (z.B. Kommunikationsteilnehmer, Zeitpunkt, Geräte- und Standortdaten) dürfen nur solange und soweit gespeichert werden, wie es für die Übermittlung von Nachrichten durch einen Dienstleister oder im Rahmen einer notwendigen Dokumentation erforderlich ist. Die Kommunikations- bzw. Metadaten dürfen ausschließlich für eigene Zwecke des Krankenhauses genutzt werden, Eine Nutzung für andere Zwecke durch den Hersteller der Lösung oder den Plattformbetreiber (z.B. Werbezwecke) ist unzulässig.	Die App Join speichert Verbindungsdaten im Rahmen der gesetzlichen Vorgaben zu Dokumentationszwecken und der entsprechend vorgegebenen Dauer. Krankenhäuser können ihre jeweiligen Kommunikationsdaten im Rahmen klinischer Studien und Forschungsprojekte anfordern.
	d) Es sollte zumindest optional der Einsatz offener Kommunikationsprotokolle (z.B. XMPP6) möglich sein, um eine Kommunikation mit anderen Messenger-Diensten zu ermöglichen.	Aufgrund der hohen Vertraulichkeit medizinischer Daten/Fotos/ Nachrichten ist ein Austausch mit anderen Messengern als höchst problematisch anzusehen. Es besteht das Risiko, dass Inhalte aus der sicheren Join-Umgebung in externe, unsichere Strukturen übertragen werden. Diese Strukturen sind nicht durch Allm überprüfbar und bergen das Risiko von Datenschutzverletzungen.

III. Sicherheit und Endgeräte

Erfüllt	Anforderungen der Datenschutzaufsichtsbehörde	Wie werden die Anforderungen von Join erfüllt?
*	a) Die eingesetzten Endgeräte müssen über einen wirksamen Zugriffschutz verfügen (z.B. PIN/Passphrase, biometrische Lösungen). Der interne Speicher der Geräte muss durch Verschlüsselung so geschützt werden, dass eine Entschlüsselung die Kenntnis der Anmeldedaten voraussetzt.	Hierauf kann Allm keinen Einfluss nehmen. Der Zugriffschutz liegt in der Verantwortung des Besitzers und sollte in den Krankenhäusern klar geregelt werden, bspw. in einer Datenschutz-Folgeabschätzung.
*	b) Es dürfen lediglich Geräte zum Einsatz kommen, deren Betriebssystemversion durch den Hersteller der Betriebssystemplattform (Google bzw. Apple) aktuell mit Sicherheitspatches versorgt werden und bei denen alle derartigen Sicherheitspatches angewandt wurden. Dies setzt voraus, dass die Hersteller der Endgeräte eine ggf. erforderliche Anpassung auf den jeweiligen Gerätetyp unverzüglich vornehmen.	Join ist nur für Apple- und Android-Geräte verfügbar. Für aktuelle Sicherheitsupdates ist der Besitzer des mobilen Endgeräts verantwortlich. Die Durchführung aktueller Sicherheitsupdates durch den Besitzer sollte in den Krankenhäusern klar geregelt werden, bspw. in einer Datenschutz-Folgeabschätzung.

* Die Verantwortung für die Umsetzung dieser Anforderungen liegt bei der Besitzerin oder dem Besitzer des mobilen Endgerätes.

*

c) Die Endgeräte müssen einem Dienst für das Mobile Device Management (MDM) unterworfen werden, welches durch eine sichere Konfiguration der Geräte und Datenverbindungen das Risiko a. des Ein-schleusens von Schadcodes (u. a. über Schwachstellen der Browser, Dateibetrachter, Betriebssystemplattform und Schnittstellen des Geräts), b. des unbefugten Zugangs von Dritten auf das Gerät selbst und auf die verarbeiteten Daten minimiert, eine Verarbeitung unterbindet, wenn das Betriebssystem des Geräts nicht die unter 2 genannten Eigenschaften aufweist, die Anwendung von Sicherheitspatches und Aktualisierungen anstößt und die Installation von Apps überwacht. Der Dienst sollte ebenso eine Ortung und Sperrung oder Löschung der Geräte bei Verlust ermöglichen, wobei jedoch eine permanente Lokalisierung der Besitzer auszuschließen ist.

Über das Admin-Tool können klinik-interne Administratoren Zugriffsrechte steuern und ggf. Nutzer sperren. Bei Verlust eines Geräts kann der zugeordnete Nutzer vom Zugriff auf Join ausgeschlossen werden. Im Übrigen liegt die Installation eines MDM in der Verantwortung der Klinik.

* Die Verantwortung für die Umsetzung dieser Anforderungen liegt bei der Besitzerin oder dem Besitzer des mobilen Endgerätes.

IV. Plattform und Betrieb

Erfüllt	Anforderungen der Datenschutzaufsichtsbehörde	Wie werden die Anforderungen von Join erfüllt?
	a) Soweit es sich bei dem in Anspruch genommenen Messenger-Dienst um einen öffentlich zugänglichen Telekommunikationsdienst i.S.d. § 3 Nr. 17a Telekommunikationsgesetz (TKG) handelt, muss dieser die jeweils anwendbaren Vorgaben von DSGVO und TKG erfüllen, hierunter insbesondere § 6 und Teil 7 TKG. Er ist im Hinblick auf die Einhaltung der telekommunikations- und datenschutzrechtlichen Anforderungen sorgfältig auszuwählen. Der Abschluss eines Vertrages gemäß Art. 28 Abs. 3 DS-GVO (s. u.) ist in diesem Fall entbehrlich.	Die App Join ist nicht öffentlich zugänglich, entsprechend handelt es sich nicht um einen Telekommunikationsdienst i.S.d. § 3 Nr. 17a Telekommunikationsgesetz (TKG). Zur Nutzung der App benötigt der Nutzer die Tenant-ID und das Tenant-Passwort der Organisation, für die er arbeitet und mit der Allm einen separaten Join-Vertrag und einen Auftragsdatenverarbeitungsvertrag abgeschlossen hat.
	b) Es muss gewährleistet sein, dass nur zugelassene Nutzer an einem Nachrichtenaustausch teilnehmen können. Dies gilt sowohl für die Kommunikation einer festgelegten, geschlossenen Benutzergruppe (z.B. Krankenhaus), als auch für die Kommunikation mit sonstigen Teilnehmern des Messenger-Dienstes. Hierfür bedarf es eines geeigneten Registrierungsprozesses oder entsprechender Autorisierungs-/Authentifizierungsmechanismen, etwa durch ein zentral administriertes Identitätsmanagementsystem.	Die App Join kann nur von Personen genutzt werden, die als Mitarbeiter einer Organisation (Gesellschaft/Krankenhaus) zugeordnet sind und über Tenant-ID und Tenant-Passwort dieser Organisation verfügen.

c) Für die mit der Nutzung des Messenger-Dienstes verbundenen Verarbeitungstätigkeiten muss, sofern diese umfangreich sind, eine Datenschutz-Folgenabschätzung (DSFA) nach Art, 35 DS-GVO) durchgeführt werden. Kommt eine von mehreren Verantwortlichen genutzte nicht öffentliche Plattform zum Einsatz, genügt es, eine DSFA einmalig für die Plattform durchzuführen.

Das Erstellen einer Datenschutz-Folgeabschätzung (DSFA) liegt in der Verantwortung des Krankenhauses. Da es sich bei Join um eine nicht-öffentliche Plattform handelt, genügt eine einmalige Durchführung der DSFA. Eine entsprechende Vorlage kann von Allm zur Verfügung gestellt werden.

d) Für die Messenger-Lösung ist durch das Krankenhaus eine regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der zur Gewährleistung der Sicherheit der Verarbeitung getroffenen technischen und organisatorischen Maßnahmen vorzunehmen (Art. 32 Abs. 1 lit. d DS-GVO).

Allm unterstützt Krankenhäuser bei der Überprüfung, Bewertung und Evaluierung der Wirksamkeit der getroffenen technischen und organisatorischen Maßnahmen. Darüber hinaus schießt Allm einen Auftragsdatenverarbeitungsvertrag mit dem jeweiligen Krankenhaus.

e) Die Messenger-Lösung sollte einen Betrieb sowohl als Service eines Dienstleisters/Auftragsverarbeiters als auch in der technischen Infrastruktur des Krankenhauses erlauben (On-Premises).

Die App Join ist als mobile Lösung konzipiert und bewusst nicht On-Premise nutzbar. Join vernetzt Expertinnen und Experten, Kolleginnen und Kollegen – intersektoral und über Krankenhaus-, Stadt- und Ländergrenzen hinweg. Erst ein solches Fachnetzwerk ermöglicht den schnellen Austausch klinischer Informationen und Expertise und ist der erste Schritt hin zu einer effizienteren, sektorenübergreifenden Patientenversorgung.

f) Soweit für den Betrieb des Verfahrens auf Auftragsverarbeiter zurückgegriffen wird, muss sichergestellt sein, dass diese den Regelungen der Datenschutz-Grundverordnung unterfallen und die Anforderungen des Art. 9 Abs. 3 DS-GVO i.V.m. § 203 Abs. 3 StGB sowie weiterer ggf. relevanter Vorschriften (z.B. Krankenhausgesetze) erfüllen. Hierzu sollte auf Dienstleister in Deutschland, der Europäischen Union bzw. des europäischen Wirtschaftsraums zurückgegriffen werden.	Der Betrieb und die Auftragsdatenverarbeitung wird von Allm durchgeführt. Das umfasst die Deutschland-Niederlassung Allm EMEA GmbH mit Sitz in Erlangen und Allm Inc. mit Sitz in Tokyo. Allm EMEA unterliegt der DS-GVO, Allm Inc. unterliegt den japanischen Datenschutz-Regulierungen, die durch einen Angemessenheits-beschluss der EU-Kommission als vergleichbar angesehen wird.
g) Mit den insoweit eingebundenen Auftragsverarbeitern ist ein Vertrag nach Art. 28 Abs. 3 DS-GVO zu schließen. Mit Blick auf die hinreichenden Garantien technisch-organisatorischer Maßnahmen, der Verarbeitung im Einklang mit der DS-GVO sowie des Schutzes der Rechte der Betroffenen sollte der Dienstleister über entsprechende Nachweise verfügen (z.B. Zertifizierung nach Art. 42 DS-GVO, Zertifizierung nach European Privacy Seal, BSI-Grundschutz-Zertifizierung).	Zur Nutzung von Join schließt Allm EMEA GmbH einen Auftragsdatenverarbeitungs-vertrag nach Art. 28 Abs. 3 DS-GVO mit ihren Kunden, der die technischen und organisatorischen Maßnahmen der Verarbeitung der Personenbezogenen Daten garantiert.

☑	h) Für die bei dem Dienstleister im Rahmen der Messenger-Lösung gespeicherten Daten ist eine regelmäßige Löschung sicherzustellen (vgl. TZ. I.8). Personenbezogene Patientendaten müssen auf den Servern des verantwortlichen gespeichert werden. Die temporäre Speicherfrist auf den Endgeräten soll daher so kurz wie möglich gehalten und in kurzen zyklischen Abständen vom Endgerät auf die vorgesehenen Server verlagert werden. Das gilt auch für eine etwaige Containerlösung in der Mobile-Messenger-App.	Die App Join bedient sich einer Streaming-Technologie, die es ermöglicht, keine personenbezogenen Daten auf dem jeweiligen Endgeräten speichern zu müssen. Personenbezogene Informationen werden sofort auf die vorgesehenen Server verlagert. Die Löschung von Daten (z.B. DICOM-Dateien) erfolgt nach Wunsch des jeweiligen Krankenhauses.
☑	i) Sobald verfügbar, sind insbesondere sicherheitsrelevante Updates der App zeitnah auf allen eingesetzten Geräten durchzuführen.	Allm informiert Nutzer über sicherheitsrelevante Updates und stellt diese im App Store und im Google Play Store zum Download bereit.

Sie wollen mehr über Join erfahren?

Kontaktieren Sie uns gerne über info_de@allm.net

Allm SHAPING HEALTHCARE