„Whitepaper“ der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder – 07.11.2019

Stand: 07.11.2019

Technische Datenschutzanforderungen an Messenger-Dienste im Krankenhausbereich

Messenger-Dienste haben parallel zur Verbreitung von Smartphones in den letzten Jahren zentrale Bedeutung für den Austausch von Nachrichten erlangt, andere Kommunikationsdienste wie E-Mail oder SMS vielfach ersetzt und zählen im privaten Alltag zu den beliebtesten Kommunikationsformen.

Gründe hierfür sind neben der jederzeitigen Nutzbarkeit über Smartphone und der leichten Bedienbarkeit der Funktionsumfang, der es erlaubt, neben Textnachrichten auch Bilder, Videos oder Sprachnachrichten auszutauschen, Sprach- und Videoanrufe durchzuführen und wahlweise mit einzelnen Teilnehmern oder in der Gruppe zu kommunizieren. Hinzu kommt, dass es sich vielfach um unentgeltlich nutzbare Angebote handelt.

Aufgrund der im privaten Bereich weitverbreiteten und etablierten Nutzung wird auf diese Messenger-Dienste zunehmend auch im Gesundheitsbereich zurückgegriffen, häufig verbunden mit der Nutzung eines privaten Endgeräts[1,2,3].

Der berufliche oder gewerbliche Einsatz von Messenger-Diensten unterliegt gesetzlichen Datenschutz-Vorgaben, denen gängige Messenger-Dienste bislang nicht oder nur bedingt entsprechen. Insbesondere der verbreitet genutzte Dienst WhatsApp führt bei einer geschäftliche Nutzung zu einer Reihe von Problemen[4], die einen Einsatz im Krankenhaus weitgehend ausschließen. Ähnliches gilt für andere im privaten Bereich häufig genutzte Dienste.

Mit Blick auf die Sensibilität der im Gesundheitsbereich betroffenen Daten und den besonderen Schutz, den diese nach Artikel 9 Datenschutz-Grundverordnung (DS-GVO) genießen, sind daher bei der Auswahl geeigneter Messenger-Dienste für die Übermittlung von Patientendaten im Krankenhausbereich vom Verantwortlichen die nachfolgenden Datenschutzanforderungen zu berücksichtigen. Die daraus ableitbaren

---

[1] https://www.aerztezeitung.de/praxis_wirtschaft/datenschutz/article/902262/klinik-jeder-dritte-arzt-verschickt-patientendaten-via-apps.html

[2] https://www.kardiologie.org/kardiologie/whatsapp-und-co--wissen-aerzte--was-sie-tun-/15742284

[3] https://deutsches-datenschutz-institut.de/wp-content/uploads/2018/05/FAZ_Messenger-2018.pdf

[4] https://www.datenschutz.rlp.de/de/themenfelder-themen/whatsapp/

Vorgaben dienen gleichzeitig als Orientierung für den Einsatz von Messenger-Diensten im niedergelassenen Bereich.

Ein Einsatz von Messenger-Diensten im Krankenhausbereich kann in unterschiedlichen Szenarien erfolgen (zum Beispiel krankenhausinterne Nutzung, Konsil, Kommunikation mit Rettungsdiensten, Kommunikation mit Arztpraxen, Kommunikation mit anderen Leistungserbringern, Kommunikation mit Patienten). Je nach Szenario können sich dabei unterschiedliche Anforderungen ergeben.

Die nachfolgenden Anforderungen beziehen sich vorrangig auf die eigentliche Messenger-Applikation, die Kommunikation zwischen den Teilnehmern, die genutzte Plattform sowie die eingesetzten Endgeräte. Der eigentliche Betrieb von Messenger-Diensten im Krankenhaus findet nur insoweit Berücksichtigung, als es sich um allgemeine Anforderungen handelt. Nicht betrachtet werden in diesem Papier aufgrund der Heterogenität der Einsatzbedingungen funktionale Anforderungen des Krankenhausbetriebs einschließlich gebotener technischer und organisatorischer Vorkehrungen.

"Erhebliche Risiken", wie es die DS-GVO formuliert, sind bei der Verarbeitung von in Artikel 9 DS-GVO genannten Datenkategorien wie Gesundheitsdaten oder genetische Daten immer anzunehmen. Dabei liegt der Schutzbedarf in den personenbezogenen Daten selbst. Wenn in diesem Papier die Verarbeitung in einem Krankenhaus angesprochen wird, dann deshalb, weil die datenschutzrechtlichen Anforderungen sich grundsätzlich an "den" Verantwortlichen (im Sinne von Artikel 4 Ziffer 7 DS-GVO) richten und in Krankenhäusern in der Regel immer auch eine umfangreiche Verarbeitung personenbezogener Daten erfolgt.

Soweit der nachfolgende Text Muss-Anforderungen formuliert, sind diese datenschutzrechtlich geboten und müssen deshalb zwingend umgesetzt werden. Soll-Anforderungen können dagegen verschiedene Ausprägungen haben: Sofern es zur Sicherstellung des Datenschutzes gleichwertige Handlungsalternativen gibt, reicht es aus, wenn eine dieser davon realisiert wird. Dabei bleibt es dem Verantwortlichen im Rahmen der durch Artikel 24 Absatz 1, Artikel 32 Absatz 1 DS-GVO eröffneten Spielräume überlassen, welcher der Möglichkeiten er tatsächlich auswählt. Darüber hinaus können Sollte-Anforderungen einen aus der Sicht des Datenschutzes zwar wünschenswerten, rechtlich aber nicht zwingend gebotenen Umstand beschreiben. Hier entscheidet der Verantwortliche selbst, ob er der Anforderung nachkommt.

I. Messenger-Applikation

1. Die Applikation muss die Möglichkeit bieten, die Nutzerinnen und Nutzer entsprechend Artikel 13 DS-GVO über die mit der Nutzung verbundene Datenverarbeitung zu unterrichten. Die Informationen müssen in einem klar erkennbaren Bereich (zum Beispiel Hinweise zum Datenschutz, Datenschutzerklärung) für den jederzeitigen Zugriff hinterlegt sein.
2. Die Applikation muss über die Möglichkeit verfügen, die Nutzung beziehungswese den Zugriff auf die darüber gespeicherten Daten an eine eigene vorherige Authentifizierung (zum Beispiel PIN, Fingerabdruck etc.) zu knüpfen. Diese kann auf betriebssystemseitige Funktionen zurückgreifen, muss sich jedoch vom Schutz zur Entsperrung des Mobilgeräts (siehe III.1) unterscheiden.
3. Die Applikation muss über die Möglichkeit verfügen, Kontaktdaten von Kommunikationsteilnehmern in einem eigenen, vom allgemeinen Adressbuch des Smartphones getrennten Speicher abzulegen. Sie sollte in diesem Zusammenhang über eine Möglichkeit verfügen, Kontakte und zugehörige Informationen aus anderen Quellen importieren zu können. Sie muss weiterhin 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. Dabei kann auf betriebssystemseitig vorhandene kryptografische Funktionen zurückgegriffen werden. Die Applikation sollte über die Möglichkeit verfügen, Nachrichten und Dateianhänge aus anderen Quellen zu importieren.
4. Die Applikation sollte die Möglichkeit bieten, für die serverseitige Authentifizierung, Verschlüsselung oder digitale Signatur benötigte Daten (zum Beispiel Zertifikate, Schlüssel) zu importieren. Eine Kommunikation über die Messenger-Applikation sollte nur auf der Grundlage einer verlässlichen Identifizierung und Authentifizierung der Kommunikationspartner möglich sein.
5. Werden elektronische Signaturen oder andere elektronischer Zertifikate genutzt, muss ein Zertifikatsmanagement 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 beziehungsweise Zertifikate. Insbesondere müssen kompromittierte Schlüsseln beziehungsweise Zertifikate beziehungsweise. 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.
6. Die Applikation sollte über eine Schnittstelle verfügen, die es erlaubt, sie in IT-Strukturen und -Prozesse eines Krankenhauses einzubinden (zum Beispiel Aufspielen von Sicherheitsprofilen oder Voreinstellungen, Synchronisation mit dem Krankenhausinformationssystem, Übernahmen behandlungsrelevanter Messenger-Nachrichten als Teil der Patientendokumentation).

7. 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.

8. Soweit im Rahmen der Nutzung der Applikation Dienste Dritter zur Fehleranalyse eingebunden werden (zum Beispiel 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.

9. Mit Blick auf die Verfügbarkeit der Daten nach Artikel 32 Absatz 1 Buchstabe b DS-GVO muss die Applikation über die Möglichkeit einer Sicherung der Kontaktdaten/Inhaltsdaten/Kommunikationsvorgänge verfügen. Soweit die Speicherung unter Einhaltung von Artikel 28 DS-GVO durch einen Dienstleister übernommen wird, welcher nicht die Anforderungen des Artikel 9 Absatz 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.

   Dabei ist eine Sicherung zur Gewährleistung der Verfügbarkeit aus datenschutzrechtlichen Gründen von der Speicherung zu Dokumentationszwecken abzugrenzen. Die aus berufsrechtlicher Sicht einschlägige ärztliche Dokumentationspflicht (vergleiche § 10 [Muster-]Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte [MBO-Ä], § 630f Bürgerliches Gesetzbuch [BGB]) bleibt davon unberührt; sie darf bei einem Einsatz von Messengern nicht vernachlässigt werden. Eine Dokumentation, die (teilweise) im Messenger erfolgt und in der Patientendokumentation nicht nachvollziehbar ist, muss unterbleiben. Behandlungsrelevante Inhaltsdaten, die sich auf Patienten beziehen und auf dem Endgerät erzeugt werden (zum Beispiel 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.

10. Soweit über die Applikation Bildaufnahmen verschickt werden (zum Beispiel 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, vergleiche Artikel 5 Absatz 1 Buchstabe c, Artikel 25 Absatz 1 DS-GVO)

11. Für die Messenger-Lösung ist durch das Krankenhaus und gegebenenfalls 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 Artikel 25 Absatz 1 beziehungsweise 32 DS-GVO enthaltenen Funktionen effektiv implementiert wurden beziehungsweise bei den jeweiligen Verarbeitungsvorgängen die Vorgaben der DS-GVO eingehalten werden (zum Beispiel Zertifizierung nach Artikel 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 Apps[5] bewertet und das Ergebnis im Rahmen der Rechenschaftspflicht (Artikel 5 Absatz 2 DS-GVO) dokumentiert werden.
12. Die Applikation muss hinsichtlich ihrer Konfigurationseinstellungen dem Grundsatz datenschutzgerechter Voreinstellungen (Artikel 25 Absatz 2 DS-GVO) entsprechen.
13. Die Applikation soll über (halb-) automatische Update-Verfahren verfügen.

II. Kommunikation

1. 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 (Artikel 32 Absatz 1 Buchstabe a DS-GVO).
2. 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 (Artikel 32 Absatz 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 (zum Beispiel, 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 zum Beispiel durch die Ergänzung einer Prüfnummer "Nachricht x von y" geschehen, sodass der Empfänger sieht, ob alle Nachrichten bei ihm angekommen sind.

[5] https://www.lda.bayern.de/media/baylda_pruefkatalog_apps.pdf

3. Verbindungsdaten zu der über den Messenger-Dienst geführten Kommunikation (zum Beispiel 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- beziehungsweise Metadaten dürfen ausschließlich für eigene Zwecke des Krankenhauses genutzt werden, Eine Nutzung für andere Zwecke durch den Hersteller der Lösung oder den Plattformbetreiber (zum Beispiel Werbezwecke) ist unzulässig.

4. Es sollte zumindest optional der Einsatz offener Kommunikationsprotokolle (zum Beispiel XMPP[6]) möglich sein, um eine Kommunikation mit anderen Messenger-Diensten zu ermöglichen.

III. Sicherheit der Endgeräte

1. Die eingesetzten Endgeräte müssen über einen wirksamen Zugriffschutz verfügen (zum Beispiel PIN/Passphrase, biometrische Lösungen). Der interne Speicher der Geräte muss durch Verschlüsselung so geschützt werden, dass eine Entschlüsselung die Kenntnis der Anmeldedaten voraussetzt.

2. 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 gegebenenfalls erforderliche Anpassung auf den jeweiligen Gerätetyp unverzüglich vornehmen.

3. 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 Einschleusens von Schadcodes (unter anderem 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.

[6] Extensible Messaging and Presence Protocol (XMPP) der IETF, als Protokollstandard RFC 6120, 6121 und 6122 veröffentlicht: https://tools.ietf.org/html/rfc6122

IV. Plattform/Betrieb

1. Soweit es sich bei dem in Anspruch genommenen Messenger-Dienst um einen öffentlich zugänglichen Telekommunikationsdienst im Sinne des § 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 Artikel 28 Absatz 3 DS-GVO (siehe unten) ist in diesem Fall entbehrlich.
2. Es muss gewährleistet sein, dass nur zugelassene Nutzer an einem Nachrichtenaustausch teilnehmen können. Dies gilt sowohl für die Kommunikation einer festgelegten, geschlossenen Benutzergruppe (zum Beispiel 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.
3. Für die mit der Nutzung des Messenger-Dienstes verbundenen Verarbeitungstätigkeiten muss, sofern diese umfangreich sind, eine Datenschutz-Folgenabschätzung (DSFA) nach Artikel 35 DS-GVO) durchgeführt werden. Kommt eine von mehreren Verantwortlichen genutzte nichtöffentliche Plattform zum Einsatz, genügt es, eine DSFA einmalig für die Plattform durchzuführen.
4. 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 (Artikel 32 Absatz 1 Buchstabe d DS-GVO).
5. Die Messenger-Lösung sollte einen Betrieb sowohl als Service eines Dienstleisters/Auftragsverarbeiters als auch in der technischen Infrastruktur des Krankenhauses erlauben (On-Premises).
6. 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 Artikels 9 Absatz 3 DS-GVO in Verbindung mit § 203 Absatz 3 StGB sowie weiterer gegebenenfalls relevanter Vorschriften (zum Beispiel Krankenhausgesetze) erfüllen. Hierzu sollte auf Dienstleister in Deutschland, der Europäischen Union beziehungsweise des europäischen Wirtschaftsraums zurückgegriffen werden.
7. Mit den insoweit eingebundenen Auftragsverarbeitern ist ein Vertrag nach Artikel 28 Absatz 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 (zum Beispiel Zertifizierung nach Artikel 42 DS-GVO, Zertifizierung nach European Privacy Seal, BSI-Grundschutz-Zertifizierung).

8. Für die bei dem Dienstleister im Rahmen der Messenger-Lösung gespeicherten Daten ist eine regelmäßige Löschung sicherzustellen (vergleiche Textziffer I.7). 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.
9. Sobald verfügbar, sind insbesondere sicherheitsrelevante Updates der App zeitnah auf allen eingesetzten Geräten durchzuführen.