Whitepaper

WhatsApp Business API im Rahmen der Verarbeitung von Gesundheitsdaten

Die Datenschutzbeauftragten des Bundes und der Länder trafen sich erstmalig am 7. Dezember 1978 in Hessen zu einem gemeinsamen Informationsaustausch und zur Abstimmung nationaler datenschutzrechtlicher Empfehlungen. Seit dem treffen sie sich regelmäßig zweimal im Jahr unter dem jährlich wechselnden Vorsitz eines Datenschutzbeauftragten zu ihren Datenschutzkonferenzen. Die Ergebnisse dieser Treffen werden der Öffentlichkeit als Konferenzbeschlüsse oder -entschließungen bekannt gegeben.

Im Rahmen der 98. Datenschutzkonferenz am 6. /7. November 2019 wurde unter anderem ein Whitepaper zu den technische Anforderungen an Messenger-Dienste im Krankenhausbereich erstellt. Im Whitepaper wurde dabei Anforderungen festgelegt, den Messenger-Dienste für eine Vielzahl an Anwendungsfällen im Rahmen des Einsatzes im Krankenhaus und angelehnte Fälle gerecht werden müssen. Dabei wurde unterschieden zwischen SOLL Anforderungen und MUSS Anforderungen.

Das Whitepaper kann hier heruntergeladen werden:
https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/DSK/2019/2019-DSK-Whitepaper_Messenger-Dienste_im_Krankenhausbereich.pdf

Flexperto nutzt den Anforderungskatalog um im allgemeineren Kontext die Frage zu erörtern, ob im mit dem Messengerdienst WhatsApp Gesundheitsdaten verarbeitet werden dürfen. Einschlägige Medien und Experten haben bereits auf das DSK Whitepaper reagiert und festgestellt, dass ein Einsatz von WhatsApp nicht möglich ist.

Eine dieser Prüfungen kann bspw. hier entnommen werden:
https://www.datenschutz-notizen.de/messenger-im-gesundheitswesen-rote-karte-fuer-whatsapp-0824102/

Zunächst möchten wir festhalten, dass die die o.g. Sicht größtenteils nachvollziehen können und die Meinung in einigen Punkten teilen. Jedoch wurde aus unserer Sicht die Verwendung des privaten WhatsApp Messengers bewertet. WhatsApp bietet jedoch eine technische Schnittstelle als Unternehmenslösung an. Die sogenannte WhatsApp Business API bietet aus unserer Sicht alle rechtlich notwendigen Funktionalitäten um bestimmte Anwendungsfälle in der Arzt – Patientenkommunikation abzudecken.

Es könnte durchaus argumentiert werden, die Bewertung ließe sich nach weiterer Auslegung auch allgemein auf die Verarbeitung von Gesundheitsdaten oder, noch allgemeiner, auf die Verarbeitung besonders schützenswerter Daten erweitern, losgelöst vom Kontext des Krankenhausbereichs.

I. Messenger-Applikation

#	Anforderung	Einschätzung	Kommentar
1	Die Applikation muss die Möglichkeit bieten, die Nutzerinnen und Nutzer entsprechend Art. 13 DS-GVO über die mit der Nutzung verbundene	Erfüllt	Über WhatsApp Business lassen sich zum ersten im Unternehmensaccount stets statische Informationen hinterlegen, die jederzeit abrufbar sind. So beispielsweise der

	Datenverarbeitung zu unterrichten. Die Informationen müssen in einem klar erkennbaren Bereich (z.B. Hinweise zum Datenschutz, Datenschutzerklärung) für den jederzeitigen Zugriff hinterlegt sein.		Unternehmensname, generelle Informationen, aber auch ein Link zu Datenschutzhinweisen und anderen Informationen gem. Art. 13 DSGVO. Durch die Funktion der automatisierten Ausspielung von Nachrichten können bei einer eingehenden Nachricht, erstmals oder auch immer zunächst Erstinformationen als Antwort bereitgestellt werden.
2	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.	Erfüllt	Da aus Sicht des Unternehmens nicht die WhatsApp Applikation selbst genutzt wird, kommt es auf die genaue Umsetzung an. Mit Flexperto muss sich ein Anwender zunächst in der Web-App oder App authentifizieren.
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.	Erfüllt	Im Rahmen der WhatsApp Business API wird aus Unternehmenssicht keine WhatsApp App auf einem Smartphone installiert. Dadurch kommt es weder zu einer Ablage von Kontakten in einem allgemeinen Adressbuch, noch zu einem Austausch der Daten mit WhatsApp.
	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.	Erfüllt	Auch hier kommt es auf die Umsetzung der Webapp, App an, die die WhatsApp Business API nutzt. Da die Datenbank vom Unternehmen selbst oder von Dienstleistern gehostet wird, hat man größtmögliche Freiheit wo die Datenabgelegt werden. Durch die Hoheit und Kontrolle der Datenbank, werden diese Daten stets verschlüsselt gespeichert.
	Die Applikation sollte über die Möglichkeit verfügen, Nachrichten und Dateianhänge aus anderen Quellen zu importieren.	Erfüllt	Durch die API ist eine Vielzahl an Szenarien möglich wie sämtliche Inhaltsdaten von Drittsystemen importiert werden können.
4	Die Applikation sollte die Möglichkeit bieten, für die serverseitige Authentifizierung, Verschlüsselung oder	Irrelevant	Keine MUSS Anforderung, daher kann an dieser Stelle davon abgesehen werden.

	digitale Signatur benötigte Daten (z.B. 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 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.	Irrelevant	Elektronische Signaturen können je nach gewünschter Güteklasse (einfach, fortgeschritten oder qualifiziert) einfach über geeignete Drittanbieter eingebunden werden. Innerhalb der Flexperto Applikation kann das angebundene Signatursystem genutzt werden.
6	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 behandlungsrelevanter Messenger Nachrichten als Teil der Patientendokumentation).	Erfüllt	WhatsApp Business API ist zunächst ausschließlich eine technische Schnittstelle ohne GUI. Daher sind derartige Integrationsszenarien prädestiniert für die API.
8	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.	Erfüllt	Durch die vollständige Datenhoheit über die WhatsApp Datenbank und durch die Möglichkeit der API Nachrichten zu löschen sind vielfältige Szenarien möglich. Flexperto bietet automatisierte Löschroutinen der Nachrichten an, auch auf Basis von speziellen Merkmalen, die individuell festgelegt werden können. Dadurch, dass die Nachrichten, bzw. der Empfänger mit einem CRM – System verknüpft werden, können sehr individuelle, Löschroutinen eingestellt werden.
9	Soweit im Rahmen der Nutzung der Applikation Dienste Dritter zur	Teilw. erfüllt	WhatsApp selbst erhält nur Metadaten im Rahmen der Nutzung, niemals

	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		inhaltliche Daten in Form von Nachrichten, Dateien, Videos etc. Nach unserer Interpretation ist die Übermittlung von Metadaten im Rahmen der Auftragsverarbeitung zwischen Ihrem Unternehmen und WhatsApp sowie zwischen Ihrem Unternehmen und einem Anbieter und/oder Hoster der WhatsApp Datenbank rechtlich vollständig zulässig. Eine gänzliche Unterlassung der Übersendung des Nutzerverhaltens ist per Gesetz nicht angezeigt.
10	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.	Erfüllt	Alle Daten können vollumfänglich gesichert und in beliebige Systeme übertragen werden.
	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.	Erfüllt	WhatsApp selbst verarbeitet keine Gesundheitsdaten, da WhatsApp aufgrund der Ende-zu-Ende Verschlüsselung nicht die Möglichkeit erhält, Nachrichtendaten einzusehen. Dies trifft insofern auf die genannte Ausnahme so insodern dass der Schlüssel nicht an den Dienstleister offenbart wird. Metadaten, Telefonnummer und Name sind nicht als Gesundheitsdaten zu werten. Der Hoster der WhatsApp Datenbank sowie Flexperto erhalten Zugriff auf die Daten, da diese aus technischen Gründen den Schlüssel auf den Servern vorhalten müssen. Die vorbenannten Parteien verpflichten sich gegenüber dem Verantwortlichen in der Auftragsverarbeitungskette der Verpflichtung gem. §203 StGB und hat auch alle Mitarbeiter dementsprechend verpflichtet.
	Dabei ist eine Sicherung zur Gewährleistung der Verfügbarkeit aus datenschutzrechtlichen Gründen von der Speicherung zu Dokumentationszwecken abzugrenzen. Die aus berufsrechtlicher Sicht einschlägige ärztliche Dokumentationspflicht (vgl. § 10 MBO-Ä, § 630f BGB) bleibt davon unberührt; sie	Erfüllt	Ein derartiges Szenario ist grundsätzlich technisch abbildbar. Alle Nachrichten können mit unterschiedlichen Merkmalen anderer Systeme technisch verknüpft werden. Die Logik der Löschung ist dabei in einem zentralen Datenhaltungssystem festzulegen. Sofern das zentrale Datenhaltungssystem die Löschung der

	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 (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.		Daten erfordert, agiert die WhatsApp Nachrichtenbank als „Slave“ und wird die entsprechenden Nachrichten löschen. Auch können Nachrichten separiert werden. Dies bedeutet, dass Nachrichten in der WhatsApp Datenbank gelöscht werden, jedoch weiterhin in einem anderen System zu Dokumentationspflichten vorgehalten werden.
11	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)	Erfüllt	Dies ist wäre über zusätzliche Applikationen abbildbar, in denen das empfangene Bild in eine Bildbearbeitungssoftware oder Funktion eingeladen wird und nach erfolgtem Bearbeiten in der Datenbanküberarbeitet wird.
12	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	Erfüllt	Sowohl WhatsApp als auch Flexperto verfügen über extensive Dokumentation über getroffene Maßnahmen zu den rechtlichen Anforderungen. Dem Verantwortlichen können die notwendigen Dokumente vorgelegt werden, damit alle Pflichten des Verantwortlichen erfüllt werden können.

	sollte die Messenger-Applikation zudem anhand des Prüfkatalogs zum technischen Datenschutz bei Apps bewertet und das Ergebnis im Rahmen der Rechenschaftspflicht (Art. 5 Abs. 2 DS-GVO) dokumentiert werden.		
13	Die Applikation muss hinsichtlich ihrer Konfigurationseinstellungen dem Grundsatz datenschutzgerechter Voreinstellungen (Art. 25 Abs. 2 DS-GVO) entsprechen.	Erfüllt	Der Betrieb von WhatsApp Business API innerhalb der Flexperto Software enthält Grundeinstellungen durch die möglichst sparsam mit der Datensammlung umgegangen wird.
14	Die App SOLLTE über (halb-) automatische Update-Verfahren verfügen.	Erfüllt	Flexperto bietet vollautomatische Updates.

II. Kommunikation

#	Anforderung	Einschätzung	Kommentar
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 (Art. 32 Abs. 1 lit. a DS-GVO).	Erfüllt	Die Nachrichtenübertragung bei WhatsApp Business API ist zwischen dem WhatsApp API Client und der WhatsApp App Ende-zu-Ende verschlüsselt. Ein Betrieb der WhatsApp Business API Infrastruktur durch einen technischen Dienstleister ist unerheblich, da dies eines in IV. 5 genehmigtes Verfahren ist. Jedoch bleibt ein Kommentar zu erwähnen, dass eine strikte, technische Ende-zu-Ende Verschlüsselung, sondern nicht per Gesetz im wörtlichen Sinne gefordert wird, sondern allgemein von einer Verschlüsselung gesprochen wird. vollständige Durchgriff auf den Dienstleister sichergestellt.
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 (Art. 32 Abs. 1 Satz 1 DS-GVO). Weiterhin muss zur Gewährleistung der Integrität der	Erfüllt	Die Integrität der Nachrichten kann durch die verwendeten Verschlüsselungen gewährleistet werden.

	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.		
3	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. Werbung) ist unzulässig.	Nicht erfüllt	Der Wunsch der Anforderung ist grundsätzlich nachzuvollziehen und zu befürworten. Aus rechtlicher Sicht hat der Nutzer von WhatsApp jedoch explizit gegenüber WhatsApp als Verantwortlichen bereits zugestimmt diese Inhalte durch die Nutzung zu teilen. Durch die ausdrückliche Einwilligung kann das hier geforderte Verbot der Verarbeitung nicht nachvollzogen werden. Ähnlich ist dies bei einem Verbot der Verarbeitung der Metadaten durch die Auftragsverarbeiter des Verantwortlichen zu beurteilen, da der Verantwortliche die notwendige Einwilligung vom Betroffenen erhält. Ferner ist die Forderung aus Sicht der heutigen Praktiken im Bereich der Bereitstellung von Software as a Service nicht zeitgemäß und praxisfremd, zumal sich wie oben die rechtliche Notwendigkeit entbehrt.
4	Es sollte zumindest optional der Einsatz offener Kommunikationsprotokolle (z.B. XMPP) möglich sein, um eine Kommunikation mit anderen Messenger-Diensten zu ermöglichen.	Erfüllt	WhatsApp verwendet das offene XMPP Protokoll für Nachrichten. Ebenfalls wird für die Verschlüsselung das offene Signal Protokoll. Flexperto nutzt ebenfalls für offene Protokolle für die hauseigenen Messaging Bridge Dienste.

III. Sicherheit der Endgeräte

#	Anforderung	Einschätzung	Kommentar
1	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.	Irrelevant	Keine Eigenschaft die WhatsApp oder Flexperto erfüllen muss.
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 ggf. erforderliche Anpassung auf den jeweiligen Gerätetyp unverzüglich vornehmen.	Irrelevant	Keine Eigenschaft die WhatsApp oder Flexperto erfüllen muss.
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 (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 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.	Irrelevant	Keine Eigenschaft die WhatsApp oder Flexperto erfüllen muss.

IV. Plattform/Betrieb

#	Anforderung	Einschätzung	Kommentar
1	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.	Vermutl. erfüllt	Gesetzgeber drängen auf die Einstufung von WhatsApp als Telekommunikationsdienst. Durch die Entscheidung des EuGH, dass Gmail kein Telekommunikationsdienst ist, ist damit auch die Einstufung von allen OTT-Messaging Apps wie WhatsApp sehr unwahrscheinlich.
2	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.	Erfüllt	Nutzer der Flexperto App müssen sich jeweils authentifizieren. Daher kann jede Kommunikation zu einer bestimmten Person zugeordnet werden. Auch ein zentrales Identitätsmanagementsystem kann durch SAML und SSO gewährleistet werden.
3	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 nichtöffentliche Plattform zum Einsatz, genügt es, eine DSFA einmalig für die Plattform durchzuführen.	Irrelevant	Obliegt dem Verantwortlichen.
4	Für die Messenger-Lösung ist durch das Krankenhaus eine regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der zur Gewährleistung	Irrelevant	Obliegt dem Verantwortlichen. Flexperto unterstützt bei den Verpflichtungen durch Vorlage geeigneter Testate Dritter.

	der Sicherheit der Verarbeitung getroffenen technischen und organisatorischen Maßnahmen vorzunehmen (Art. 32 Abs. 1 lit. 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).	Teilw. erfüllt	Ein vollständiger on-premise Betrieb ist durch Flexperto aktuell nicht möglich. Es können Teile der Lösung, wie das Hosting der WhatsApp Datenbank als on-premise Lösung angeboten werden, jedoch wird dadurch das Sicherheitsniveau nicht zwingend gesteigert, sondern ggf. verringert.
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 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.	Erfüllt	Flexperto sowie der für das Hosting der WhatsApp Clients genutzten Anbieter sind in der europäischen Union ansässig und haben Mitarbeiter nach § 203 Abs. 3 StGB sowie weiterer ggf. relevanter Vorschriften verpflichtet. Die Anforderung kann auf WhatsApp insofern nicht zutreffen, als das WhatsApp keine Gesundheitsdaten verarbeitet, da WhatsApp keine Nachrichtendaten einsehen kann.
7	Mit den insoweit eingebundenen Auftragsverarbeitern ist ein Vertrag nach Art. 28 Abs. 3 DS-GVO zu schließen. Mit Blick auf die hinreichenden Garantien technischorganisatorischer 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).	Erfüllt	Mit allen in der Verarbeitungskette tätigen Dienstleistern wird eine Auftragsverarbeitung gem. Art. 28 Abs. 3 DS-GVO geschlossen. Dies beinhaltet auch WhatsApp, dessen AGB einen elektronisch zulässigen Abschluss einer Auftragsverarbeitung ermöglicht, der die Mindestinhalte nach Art. 28 Abs. DS-GVO aufgreift.
8	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	Erfüllt	Wie in I.8 beschrieben können automatisierte Löschroutinen eingestellt werden.

	Containerlösung in der Mobile-Messenger-App		
9	Sobald verfügbar, sind insbesondere sicherheitsrelevante Updates der App zeitnah auf allen eingesetzten Geräten durchzuführen.	Erfüllt	Flexperto und Subdienstleister updaten regelmäßig die API und Software.