Prüfung des Einsatzes von WhatsApp in Gesundheitseinrichtungen anhand des Whitepapers „Technische Datenschutzanforderungen an Messenger-Dienste im Krankenhausbereich“

I. Messenger-Applikation	
Die App MUSS nach Art. 13 DS-GVO unterrichten. Die Informationen müssen klar erkennbar und jederzeit abrufbar sein.	☐ Erfüllt ☒ Nicht erfüllt ☐ Nicht bekannt ☐ Entbehrlich, weil keine MUSS-Vorgabe
Die App MUSS separaten Zugriffsschutz bereithalten.	☒ Erfüllt, muss aber individuell aktiviert werden. Ist manuell in den Einstellungen aktivierbar. ☐ Nicht erfüllt ☐ Nicht bekannt ☐ Entbehrlich, weil keine MUSS-Vorgabe
Die App MUSS Kontaktdaten von Kommunikationsteilnehmern in einem eigenen, vom allgemeinen Adressbuch des Smartphones getrennten Speicher ablegen können. Die App MUSS Nachrichten sowie Dateianhänge wie Bilder, Videos, Dokumente etc. ausschließlich in einem eigenen, von den allgemeinen Speicherbereichen des Smartphones getrennten Speicher in verschlüsselter Form ablegen können.	☐ Erfüllt ☒ Nicht erfüllt ☐ Nicht bekannt ☐ Entbehrlich, weil keine MUSS-Vorgabe
Die App SOLLTE für die serverseitige Authentifizierung, Verschlüsselung oder digitale Signatur benötigte Daten (z.B. Zertifikate, Schlüssel) importieren können. Eine Kommunikation über die App SOLLTE nur auf Grundlage einer verlässlichen Identifizierung und Authentifizierung der Kommunikationspartner möglich sein.	☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht bekannt ☒ Entbehrlich, weil keine MUSS-Vorgabe
Es MUSS ein Zertifikatsmanagement vorhanden sein, wenn elektronische Signaturen oder andere elektronische Zertifikate genutzt werden.	☐ Erfüllt ☒ Nicht erfüllt, da nicht vorhanden ☐ Nicht bekannt ☐ Entbehrlich, weil keine MUSS-Vorgabe
Die App SOLLTE über eine Schnittstelle verfügen, die es erlaubt, sie in IT-Strukturen und -Prozesse eines Krankenhauses einzubinden.	☐ Erfüllt ☐ Nicht erfüllt ☒ Nicht bekannt ☐ Entbehrlich, weil keine MUSS-Vorgabe

Die App MUSS über die Möglichkeit verfügen, die über sie verwalteten Daten gezielt oder allgemein zu löschen (Nachrichten, Dateien, Kontakte etc.). Die App SOLLTE über die Möglichkeit verfügen, eine Frist festzulegen, nach der Daten automatisiert gelöscht werden.	☐ Erfüllt ☒ Nicht erfüllt. Zwar können Inhalte, aber keine Kontakte gelöscht werden. ☐ Nicht bekannt ☐ Entbehrlich, weil keine MUSS-Vorgabe
Sofern die App Dienste Dritter zur Fehleranalyse einsetzt, MUSS dies offen erkennbar dargestellt und als optional gekennzeichnet werden. 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.	☐ Erfüllt ☐ Nicht erfüllt ☒ Nicht bekannt ☐ Entbehrlich, weil keine MUSS-Vorgabe
Die App MUSS die Möglichkeit der Sicherung der Kontakt- und Inhaltsdaten sowie der Kommunikationsvorgänge bieten. Die Sicherung MUSS verschlüsselt sein, wenn die Speicherung im Rahmen einer Auftragsverarbeitung erfolgt und der Dienstleister nicht die Anforderungen des Art. 9 Abs. 3 DS-GVO erfüllt.	☐ Erfüllt ☐ Nicht erfüllt ☒ Nicht bekannt ☐ Entbehrlich, weil keine MUSS-Vorgabe
Die App SOLLTE die Möglichkeit der Schwärzung von Bildteilen ermöglichen, wenn Bildaufnahmen von Patienten versandt werden, die darauf befindlichen Angaben aber nicht alle benötigt werden.	☒ Erfüllt, indem nur im Vorfeld entsprechend aufbereitete Dokumente versandt werden. ☐ Nicht erfüllt ☐ Nicht bekannt ☐ Entbehrlich, weil keine MUSS-Vorgabe
Die Gesundheitseinrichtung MUSS dokumentieren, dass Privacy by Default und die TOMs effektiv implementiert wurden und eingehalten werden (z.B. durch entsprechendes Zertifikat). Die App MUSS anhand des Prüfkatalogs zum technischen Datenschutz bei Apps bewertet und das Ergebnis dokumentiert werden.	Aufgabe des Verantwortlichen, steht nicht im direkten Zusammenhang zur App.
Die Applikation MUSS hinsichtlich ihrer Konfigurationseinstellungen dem Grundsatz Privacy by Default entsprechen.	☐ Erfüllt ☒ Nicht erfüllt, da Einschränkungen manuell gesetzt werden müssen. ☐ Nicht bekannt ☐ Entbehrlich, weil keine MUSS-Vorgabe

Die App SOLLTE über (halb-) automatische Update-Verfahren verfügen.	☒ Erfüllt, wenn auf Betriebssystemebene die Funktion aktiviert ist. ☐ Nicht erfüllt ☐ Nicht bekannt ☐ Entbehrlich, weil keine MUSS-Vorgabe
II. Kommunikation	
Die App MUSS eine Ende-zu-Ende-Verschlüsselung zwischen den Kommunikationsteilnehmern gewährleisten.	☒ Erfüllt ☐ Nicht erfüllt ☐ Nicht bekannt ☐ Entbehrlich, weil keine MUSS-Vorgabe
Die App SOLLTE Möglichkeiten bieten, die Integrität der über den Messenger-Dienst kommunizierten Daten zu gewährleisten.	☒ Erfüllt, durch die Ende-zu-Ende-Verschlüsselung wird die Integrität gewahrt. ☐ Nicht erfüllt ☐ Nicht bekannt ☐ Entbehrlich, weil keine MUSS-Vorgabe
Limitierte Speicherung der Verbindungsdaten nach Maßgabe des Erforderlichkleitsgrundsatzes MUSS gewährleistet werden. Kommunikations- bzw. Metadaten dürfen ausschließlich für eigene Zwecke des Krankenhauses genutzt werden. Keine Nutzung für andere Zwecke durch den Hersteller der Software-Lösung oder den Plattformbetreiber.	☐ Erfüllt ☐ Nicht erfüllt ☒ Nicht bekannt ☐ Entbehrlich, weil keine MUSS-Vorgabe
Die App SOLLTE den Einsatz offener Kommunikationsprotokolle ermöglichen.	☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht bekannt ☒ Entbehrlich, weil keine MUSS-Vorgabe

III. Sicherheit der Endgeräte	
Das genutzte Endgerät MUSS einen wirksamen Zugriffsschutz bieten. Der interne Speicher MUSS so verschlüsselt sein, dass eine Entschlüsselung die Kenntnis der Anmeldedaten voraussetzt.	Das ist keine Funktionalität, die dem Messenger-Dienst zuzuordnen ist.
Die genutzte Betriebssystemversion MUSS durch den Hersteller der Betriebssystemplattform mit Sicherheitspatches versorgt werden. Diese MÜSSEN zeitnah implementiert werden.	Das ist keine Funktionalität, die dem Messenger-Dienst zuzuordnen ist.
Die Endgeräte MÜSSEN über ein MDM administriert werden. Das MDM MUSS das Risiko - des Einschleusens von Schadcodes - des unbefugten Zugangs von Dritten auf das Gerät selbst und auf die verarbeiteten Daten minimieren. Der Dienst SOLLTE ebenso eine Ortung und Sperrung oder Löschung der Geräte bei Verlust ermöglichen, wobei jedoch eine permanente Lokalisierung der Besitzer auszuschließen ist.	Das ist keine Funktionalität, die dem Messenger-Dienst zuzuordnen ist.
IV. Plattform/Betrieb	
Sofern der Dienst ein Telekommunikationsdienst darstellt MUSS er die Vorgaben von DSGVO und TKG, insbesondere § 6 und Teil 7 TKG erfüllen.	☐ Erfüllt ☐ Nicht erfüllt ☒ Nicht bekannt ☐ Entbehrlich, weil keine MUSS-Vorgabe
Es MUSS gewährleistet sein, dass nur zugelassene Nutzer am Nachrichtenaustausch teilnehmen. Es bedarf eines geeigneten Registrierungsprozesses oder entsprechender Autorisierungs-/Authentifizierungsmechanismen.	☐ Erfüllt ☒ Nicht erfüllt, da die Definition eines bestimmten Nutzerkreises nicht möglich ist. ☐ Nicht bekannt ☐ Entbehrlich, weil keine MUSS-Vorgabe
Wird der Messenger-Dienst umfangreich genutzt, MUSS eine Datenschutz-Folgenabschätzung durchgeführt werden.	Das ist keine Funktionalität, die dem Messenger-Dienst zuzuordnen ist.
Die App MUSS einem regelmäßigen Review bezüglich der Wirksamkeit der zur Gewährleistung der Sicherheit der Verarbeitung getroffenen technischen und organisatorischen Maßnahmen unterzogen werden.	Das ist keine Funktionalität, die dem Messenger-Dienst zuzuordnen ist.

Die App SOLLTE den Betrieb sowohl als Service eines Dienstleisters als auch in der technischen Infrastruktur des Krankenhauses erlauben.	☐ Erfüllt ☐ Nicht erfüllt ☐ Nicht bekannt ☒ Entbehrlich, weil keine MUSS-Vorgabe
Beim Betrieb durch einen Dienstleister MUSS sichergestellt sein, dass dieser den Regelungen der DS-GVO und etwaiger Spezialgesetze unterliegt. Es SOLLTE auf Dienstleister in Deutschland, der Europäischen Union bzw. des europäischen Wirtschaftsraums zurückgegriffen werden.	☐ Erfüllt ☒ Nicht erfüllt ☐ Nicht bekannt ☐ Entbehrlich, weil keine MUSS-Vorgabe
Mit dem Dienstleister MUSS ein Vertrag zur Auftragsverarbeitung geschlossen werden.	☐ Erfüllt ☒ Nicht erfüllt, ☐ Nicht bekannt ☐ Entbehrlich, weil keine MUSS-Vorgabe
Für den Einsatz der App MUSS ein Löschkonzept bestehen.	☒ Erfüllt, die Daten befinden sich nach der Zustellung nur noch lokal auf den Geräten. Hier ist zwischen den Kommunikationspartnern mindestens durch organisatorische Maßnahmen die regelmäßige Löschung zu regeln. ☐ Nicht erfüllt ☐ Nicht bekannt ☐ Entbehrlich, weil keine MUSS-Vorgabe
Updates der App MÜSSEN zeitnah umgesetzt werden.	Das ist keine Funktionalität, die dem Messenger-Dienst zuzuordnen ist.