Stellungnahme der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 29. April 2021

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

---

[1] https://www.aerztezeitung.de/praxis_wirtschaft/datenschutz/article/902262/klinik-jeder-dritte-arzt-verschickt-patienten-daten-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/

Ein Einsatz von Messenger-Diensten im Krankenhausbereich kann in unterschiedlichen Szenarien erfolgen (z. B. krankenhausinterne Nutzung, Konsil, Kommunikation mit Rettungsdiensten, Kommunikation mit Arztpraxen, Kommunikation mit anderen Leistungserbringern, Kommunikation mit Patientinnen und Patienten). Je nach Szenario können sich dabei unterschiedliche Anforderungen ergeben. Die nachfolgenden Anforderungen setzen den Einsatz dienstlicher Endgeräte voraus und umfassen nicht den Einsatz von privaten Endgeräten durch Beschäftige. Der Anwendungsbereich des Papiers erstreckt sich auf die Kommunikation im Krankenhaus – die Kommunikation mit externen Dritten und Patientinnen sowie Patienten ist nicht betroffen.

Die nachfolgenden Anforderungen beziehen sich vorrangig auf die eigentliche Messenger-Applikation, die Kommunikation zwischen den Teilnehmerinnen und 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 Datenschutz-Grundverordnung formuliert[5], sind bei der Verarbeitung von in Art. 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 (i. S. v. Art. 4 Ziff. 7 DS-GVO) richten und in Krankenhäusern i. d. R. 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 Art. 24 Abs. 1, 25 Abs. 1 und Abs. 2, 32 Abs. 1 DS-GVO eröffneten Spielräume überlassen, welche 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. Im Ergebnis muss der Verantwortliche gewährleisten, dass die jeweilige Verarbeitung, die

[5] Siehe Erwägungsgrund 51 Satz 1 DS-GVO.

durch einen Messenger-Dienst unterstützt wird, ein dem Risiko angemessenes Schutzniveau aufweist.

I. Messenger-Applikation

1. 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.

2. Die Applikation muss über die Möglichkeit verfügen, die Nutzung und den Zugriff auf die darüber verarbeiteten Daten an eine eigene vorherige Authentifizierung (z. B. PIN, Fingerabdruck) zu knüpfen. Diese kann auf betriebssystemseitige Funktionen zurückgreifen, muss sich jedoch vom Schutz zur Entsperrung des Mobilgeräts (siehe Tz. III. 1) unterscheiden.

3. Die Applikation muss über die Möglichkeit verfügen, Kontaktdaten von Kommunikationsteilnehmerinnen und -teilnehmern in einem eigenen, vom allgemeinen Adressbuch des verwendeten Endgeräts (Smartphone, Tablet, PC etc.) 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 verwendeten Geräts 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 (z. B. Zertifikate, Schlüssel) zu importieren. Eine Kommunikation über die Messenger-Applikation darf nur auf der Grundlage einer verlässlichen Identifizierung und Authentifizierung der Kommunikationspartner möglich sein.

5. Werden elektronische Signaturen oder andere elektronische Zertifikate genutzt, muss ein Zertifikatsmanagement vorhanden sein. Insbesondere ist sicherzustellen, dass elektronische Schlüssel oder Zertifikate eindeutig einer juristischen Person (hier: dem Krankenhaus) oder einer natürlichen Person zugeordnet und regelmäßig auf Gültigkeit überprüft werden. Kompromittierte Schlüssel bzw. Zertifikate müssen unbrauchbar gemacht werden können. Dabei ist unerheblich, ob die genutzte Public Key Infrastructure (PKI) vom Verantwortlichen betrieben oder von einem Dritten zur Verfügung gestellt wird.

6. Angesichts der krankenhaus- und berufsrechtlichen Dokumentationsvorgaben und im Hinblick auf die Erfüllung von Betroffenenrechten muss das Backend 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).

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 (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.

9. Mit Blick auf die Verfügbarkeit der Daten nach Art. 32 Abs. 1 lit. b DS-GVO muss die Applikation über die Möglichkeit einer Sicherung und durchführbaren Wiederherstellung der relevanten 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.

   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 darf bei einem Einsatz von Messenger-Diensten nicht vernachlässigt werden. Eine Dokumentation, die (teilweise) im Messenger erfolgt und in der Patientendokumentation nicht nachvollziehbar ist, muss unterbleiben. Behandlungsrelevante Inhaltsdaten, die sich auf Patientinnen und 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, 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 (z. B. Patientenaufnahmen, Screenshots), bei denen darin enthaltene personenbezogene Daten für den verfolgten Zweck 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, 25 Abs. 1 DS-GVO).

11. Für die Messenger-Lösung ist durch das verantwortliche 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 und 32 DS-GVO enthaltenen Funktionen effektiv implementiert wurden sowie bei den jeweiligen Verarbeitungsvorgängen die Vorgaben der Datenschutz-Grundverordnung eingehalten werden (z. B. Zertifizierung nach Art. 42 DS-GVO, Zertifizierung nach European Privacy Seal, BSI-Grundschutz-Zertifizierung oder Vergleichbares). Seitens des Krankenhauses sollte die Messenger-Applikation zudem anhand des Prüfkatalogs zum technischen Datenschutz bei Apps[6] bewertet und das Ergebnis im Rahmen der Rechenschaftspflicht (Art. 5 Abs. 2 DS-GVO) dokumentiert werden.

12. Die Applikation muss hinsichtlich ihrer Technikgestaltung dem Art. 25 Abs. 1 DS-GVO und hinsichtlich ihrer Konfigurationseinstellungen dem Grundsatz datenschutzgerechter Voreinstellungen (Art. 25 Abs. 2 DS-GVO) entsprechen.

13. Die Applikation soll über (halb-) automatische Update-Verfahren[7] verfügen.

II. Kommunikation

1. Die Vertraulichkeit und Integrität der über den Messenger-Dienst geführten medizinischen Kommunikation muss unter Berücksichtigung des Stands der Technik über eine Ende-zu-Ende-Verschlüsselung zwischen den einzelnen oder Gruppen von Kommunikationsteilnehmerinnen und -teilnehmern bzw. den jeweiligen Diensten gewährleistet werden (Art. 32 Abs. 1 lit. 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

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

[7] Auf anstehende Updates muss automatisch täglich oder spätestens beim nächsten Aufruf der App geprüft werden. Die Updates müssen dann automatisch eingespielt oder die Benutzerinnen und Benutzer müssen vom Vorliegen eines Updates informiert werden und das Update mit einem einfachen Bedienschritt ausführen können.

Technik nachzuweisen (Art. 32 Abs. 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 bei der Empfängerin bzw. 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 der Empfängerin oder dem Empfänger mitteilen, ob die gesendete Mitteilung vollständig angekommen ist oder ob einzelne Nachrichtenteile fehlen. Dies kann z. B. durch automatisches Hinzufügen einer Sequenznummer („Teil x von y“) geschehen, so dass die Empfängerin bzw. der Empfänger sehen, ob alle Nachrichten bei ihr oder ihm angekommen sind.

3. Verbindungsdaten zu der über den Messenger-Dienst geführten Kommunikation (z. B. Kommunikationsteilnehmerinnen und -teilnehmer, Zeitpunkt, Geräte- und Standortdaten) dürfen nur solange und soweit verarbeitet werden, wie dies zur Durchführung der Übermittlung der Kommunikation oder zur Aufrechterhaltung oder Wiederherstellung der Sicherheit elektronischer Kommunikationsnetze und -dienste oder zur Erkennung von technischen Defekten und Fehlern bei der Übermittlung der elektronischen Kommunikation erforderlich ist. Die Kommunikations- und Metadaten dürfen ausschließlich für die festgelegten, eigenen Zwecke des Krankenhauses genutzt werden. Eine Nutzung für andere Zwecke durch den Hersteller der Lösung oder den Plattformbetreiber (z. B. Werbezwecke) ist unzulässig.

4. Es sollte zumindest optional der Einsatz offener Kommunikationsprotokolle[8] (z. B. XMPP[9], Matrix[10]) 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 (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.

2. Es dürfen lediglich Geräte zum Einsatz kommen, deren Betriebssystemversion durch den Hersteller der Betriebssystemplattform (insbesondere Google oder

[8] Protokolle, die einem offenen Standard genügen, entsprechend der Definition der Free Software Foundation Europe (https://fsfe.org/freesoftware/standards/def.de.html).

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

[10] Zur Spezifikation siehe https://matrix.org/docs/spec/

Apple) aktuell mit Sicherheitspatches versorgt werden und bei denen alle derartigen Sicherheitspatches unverzüglich bzw. unverzüglich nach Prüfung und Freigabe durch die institutionseigene IT-Sicherheitssicherheitsabteilung, soweit vorgesehen, angewandt wurden. Dies setzt voraus, dass die Hersteller der Endgeräte eine ggf. erforderliche Anpassung auf den jeweiligen Gerätetyp unverzüglich vornehmen.

3. Die Endgeräte müssen einem Dienst für das Mobile Device Management (MDM) oder einer gleich wirksamen Maßnahme (Konfigurationsvorgaben/Profile, Installations-/Nutzungsbeschränkungen, Lokalisierung, Fernlöschung etc.) 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 Zugriffs von Dritten auf das Gerät selbst und auf die verarbeiteten Daten

   minimiert, eine Verarbeitung unterbindet, wenn das Betriebssystem des Geräts nicht die unter Tz. III. 2 genannten Eigenschaften aufweist, die Anwendung von Sicherheitspatches und Aktualisierungen anstößt und die Installation von Apps überwacht. Der Dienst sollte ebenso nach Erforderlichkeit eine Ortung und Sperrung oder Löschung der Geräte sowie eine Löschung personenbezogener Daten bei Verlust ermöglichen, wobei jedoch eine permanente Lokalisierung der Besitzer auszuschließen ist.

IV. Plattform/Betrieb

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 der Datenschutz-Grundverordnung und des Telekommunikationsgesetzes 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.

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 Teilnehmerinnen und 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 die Erforderlichkeit einer Datenschutz-Folgenabschätzung (DSFA) nach Art. 35 DS-GVO geprüft werden. Insbesondere wenn diese Verarbeitungstätigkeiten umfangreich sind, ist eine DSFA durchzuführen (Art. 35 Abs. 3 lit. b DS-GVO). Haben mehrere Krankenhäuser ähnliche Verarbeitungstätigkeiten, die von Messenger-Diensten unterstützt werden, mit ähnlich hohem Risiko, so kann eine weitere DSFA unterbleiben, wenn ein Krankenhaus eine bereits entsprechend durchgeführte DSFA – ggf. nach erforderlichen Anpassungen – „als eigene" übernimmt (Art. 35 Abs. 1 Satz 2 DS-GVO).

4. Für die Messenger-Lösung ist durch das Krankenhaus eine regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der zum Schutz der Verarbeitung getroffenen technischen und organisatorischen Maßnahmen vorzunehmen (Art. 24 Abs. 1 Satz 2, 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).

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.

7. 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, die Verarbeitung im Einklang mit der Datenschutz-Grundverordnung sowie den Schutz der Rechte der betroffenen Personen sollte der Dienstleister über entsprechende Nachweise verfügen (z. B. Zertifizierung nach Art. 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 (vgl. Tz. I.8). Personenbezogene Patientendaten müssen auf den Servern des Krankenhauses oder dessen Auftragsverarbeitern (soweit diese nach den Vorgaben der Datenschutz-Grundverordnung – insbesondere Art. 9 Abs. 3 und 28 DS-GVO –, der bundes- bzw. landes-

datenschutzrechtlichen Regelungen und ggf. unter Beachtung spezifischer landesrechtlicher, insbesondere landeskrankenhausrechtlicher Vorgaben eingesetzt wurden) verarbeitet werden. Die temporäre Speicherung auf den Endgeräten soll daher nach dem Erforderlichkeitsgrundsatz so kurz wie möglich gehalten und in kurzen zyklischen Abständen vom Endgerät auf die vorgesehenen Serversysteme verlagert werden. Das gilt auch für eine etwaige Containerlösung in der Mobile-Messenger-App.

9. Sobald verfügbar, sind insbesondere sicherheitsrelevante Updates der App unverzüglich intern freizugeben und auf allen eingesetzten Geräten durchzuführen.