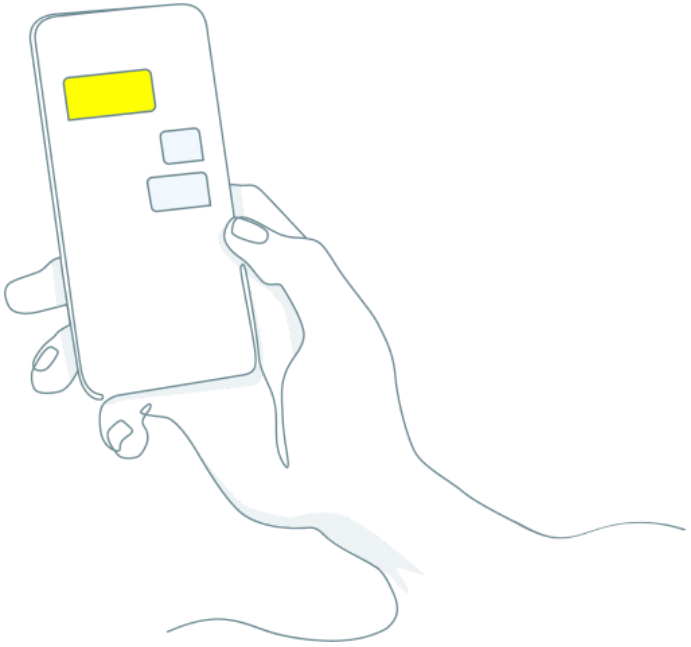
KOMMENTAR ZUM WHITEPAPER DER DATENSCHUTZKONFERENZ

# Technische Datenschutz-anforderungen an Messenger-Dienste im Krankenhausbereich



Das „Whitepaper“ der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder wurde am 07.11.2019 veröffentlicht und ist auf der Webseite der Datenschutzkonferenz abrufbar. In diesem Dokument vergleichen wir die im Whitepaper genannten Anforderungen mit den Funktionen der Siilo-App.

Whitepaper der Datenschutzkonferenz herunterladen

KAPITEL 1

# Messenger-Applikation

| Erfüllt | Anforderungen der Datenschutzaufsichtsbehörde | Wie werden diese von Siilo erfüllt? |
|---|---|---|
| ✔ | 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. | Hinweise zur Datenverarbeitung und zum Datenschutz finden Sie in der Siilo-App unter Einstellungen > Datenschutzbestimmungen. |
| ✔ | 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. | Nach Entsperrung des Mobilgeräts ist der Zugang zur Siilo-App nur nach einer weiteren Authentifizierung durch Eingabe des Siilo-PIN-Codes bzw. durch Fingerabdruck oder Face ID möglich. |
| ✔ | 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. | Siilo-Kontakte werden separat vom allgemeinen Adressbuch des Mobilgeräts in der App selbst gespeichert (sog. „Container-Lösung“). Siilo-Nutzer haben die Möglichkeit, sich automatisch mit Kontakten aus dem Adressbuch Ihres Mobilgeräts verbinden zu lassen, sofern diese Kontakte bereits Siilo-Nutzer sind. Dazu müssen Sie zustimmen, dass Siilo Zugriff auf Ihr Adressbuch bekommt. Dann werden nur die Mobilfunknummern in Ihrem Adressbuch verschlüsselt an Siilo-Server geschickt und mit ebenfalls verschlüsselten Mobilfunknummern von anderen, verifizierten Siilo-Nutzern verglichen. Bei Übereinstimmung werden die Nutzer miteinander verbunden. Nicht übereinstimmende Nummern werden sofort nach dem Abgleich vom Server gelöscht. Andere Daten wie Namen, Adressen, etc werden von Siilo nicht erfasst. |

| | | |
|---|---|---|
| | | Bilder und Videos, die mit der sicheren Siilo-Kamera erfasst werden, sowie Chat-Nachrichten und gesendete Dokumente, werden ebenfalls nur in der App, getrennt vom eigentlichen Fotoverzeichnis des Mobilgeräts, gespeichert. Der Zugang zu diesen Bildern ist daher nur nach einer Authentifizierung möglich. Die separate Speicherung im App-Container verhindert somit einen unerlaubten Zugriff (z.B. bei Verlust des Mobilgeräts) sowie die versehentliche Synchronisierung mit Cloud-Diensten (z.B. iCloud). |
| ✔ | 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 sollte nur auf der Grundlage einer verlässlichen Identifizierung und Authentifizierung der Kommunikationspartner möglich sein. | Im Profil eines jeden Siilo-Nutzer findet sich der individuelle, digitale “Fingerabdruck” des Nutzers. Dieser aus 32 Zahlen und/oder Buchstaben bestehende Code kann genutzt werden, um die Echtheit einer Nachricht zu verifizieren. Ein Nachricht ist dann echt, wenn der mit einer Siilo-Nachricht übermittelte digitale Fingerabdruck mit dem im Profil des Nutzers angegebenen Fingerabdruck übereinstimmt. Ein Nutzer hat die Möglichkeit, den Siilo-Fingerabdruck auch über ein alternatives Medium (z.B. SMS) zu verschicken, um eine Nachricht zu verifizieren und sog. “man in the middle”-Angriffe auf die Datensicherheit zu verhindern. |
| ✔ | 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. | Siilo verwendet NaCl, eine Open-Source-Bibliothek für die Verschlüsselung, Entschlüsselung und elektronische Signaturen. Jeder Nutzer, der sich bei Siilo registriert, generiert einen privaten und einen öffentlichen Schlüssel und sendet die öffentlichen Schlüssel an Siilo. Daher hat jede natürliche Person ihren eigenen Schlüssel. Nach der Registrierung werden alle Anfragen an unsere Server signiert und die Nachrichten mit diesen Schlüsseln verschlüsselt. Kontakte des Benutzers können den aktuellen öffentlichen Schlüssel des Benutzers anfordern, um ihre Nachrichten entschlüsseln zu können. Wenn die Schlüssel bzw. das Endgerät eines Nutzers kompromittiert wurde, können wir die Schlüssel dieses Nutzers ungültig machen. Dies wird daraufhin an alle Kontakte des Benutzers weitergegeben. |

| | | |
|---|---|---|
| ✔ | 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). | Über Siilo ausgetauschte Nachrichten und Dokumente können problemlos in die elektronische Krankenakte eines Patienten exportiert werden. Siilo arbeitet dabei eng mit den gängigen IT-Systemen zusammen. |
| ✔ | 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. | Nutzer können spezifische Daten (Nachrichte, Dateien, Kontakte, etc.) in der Siilo-App löschen. Diese Daten werden daraufhin sowohl vom mobilen Endgerät als auch von den Servern gelöscht.<br><br>Siilo-Nachrichten (einschließlich versendete Bilder und Dokumente) werden standardmäßig automatisch nach 30 Tagen gelöscht. Als Nutzer haben Sie die Möglichkeit, wichtige Chat-Nachrichten auch über diesen Zeitraum hinaus zu behalten. |
| ✔ | 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. | Um die Verbesserung von wesentlichen Software-Fehlern in der App zu beschleunigen, ist es wichtig, dass wir bei Siilo Rückmeldung über Abstürze der App bekommen. Siilo nutzt dazu die Dienste von Fabric.io. Abstürze der App werden über diesen Dienst anonymisiert an Siilo gemeldet. Siilo-Nutzer haben die Möglichkeit, zur Verbesserung der App durch solche Meldungen beizutragen. Während des Registrierungsprozesses werden Siilo-Nutzer dabei explizit um Ihre Erlaubnis gebeten. Unter Einstellungen>Datenschutz können Absturzmeldungen jederzeit aktiviert und deaktiviert werden. Sollten Nutzer zustimmen, werden nur anonymisierte Daten übertragen, aber keine persönlichen, identifizierbaren Daten. |
| ✔ | 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 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 | Siilo bietet den Nutzern die Möglichkeit, ein Backup ihrer Kontaktdaten und Chatinhalte zu erstellen. Die Funktion wurde so implementiert, dass nur der Nutzer den Schlüssel für diese Sicherung und Wiederherstellung besitzt. Siilo kann auf diesen Schlüssel nicht zugreifen (“zero knowledge policy”). |

| | | |
|---|---|---|
| | 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 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 | Für die Patientendokumentation relevante Chatinhalte können aus der Siilo-App exportiert werden und in die IT-Struktur eines Krankenhauses übermittelt werden. Ein Nutzer kann relevante Inhalte manuell auswählen und dann als pdf-Datei exportieren. Die Export-Funktion kann auch automatisiert erfolgen durch Integration von Siilo in das jeweilige Krankenhaus-Informationssystem. |
| ✔ | 10. 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) | Mit dem „blur"-Werkzeug haben Sie die Möglichkeit, personenbezogene Daten in mit der sicheren Siilo-Kamera gemachten Bildaufnahmen auf einfache Weise unkenntlich zu machen. Klicken Sie dazu einfach auf das Bleistift-Symbol und wählen Sie das „blur"-Werkzeug ganz rechts aus. Mit nur einem Fingerwisch können Sie nun personenbezogene Daten permanent unkenntlich machen.  |
| ✔ | 11. 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). Seitens des Krankenhauses 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. | Siilo stellt Krankenhäusern einen Auftragsdatenverarbeitungsvertrag (ADV) zur Verfügung. Darin garantiert Siilo, dass bei der Auftragsverarbeitung die Grundsätze des Datenschutzes entsprechend der DS-GVO eingehalten werden. Als Nachweis für die erfolgreiche Umsetzung technischer und organisatorischer Maßnahmen ist Siilo nach ISO27001 zertifiziert. Darüber hinaus erfüllt Siilo die Standards des britischen Gesundheitsdienstes National Health Service (NHS) sowie des US-amerikanischen Regelwerks Health Insurance Portability and Accountability Act (HIPAA). |

| | | |
|---|---|---|
| ✔ | 12. Die Applikation muss hinsichtlich ihrer Konfigurationseinstellungen dem Grundsatz datenschutzgerechter Voreinstellungen (Art. 25 Abs. 2 DS-GVO) entsprechen. | Siilo operiert nach den Grundsätzen „Privacy by Design“ und „Security by Design“. Zudem hat Siilo die erforderlichen technischen und organisatorischen Maßnahmen ergriffen, um sicherzustellen, dass standardmäßig nur personenbezogene Daten verarbeitet werden, die für den jeweiligen Zweck der Verarbeitung erforderlich sind. |
| ✔ | 13. Die Applikation soll über (halb-) automatische Update-Verfahren verfügen. | Siilo arbeitet kontinuierlich an der Verbesserung der App. Siilo-Nutzer erhalten über (halb-) automatische Verfahren regelmäßige Updates über den App Store und Google Play Store. |

KAPITEL 2

# Kommunikation

| Erfüllt | Anforderungen der Datenschutzaufsichtsbehörde | Wie werden diese von Siilo erfüllt? |
|---|---|---|
| ✔ | 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 Kommunikations-teilnehmern gewährleistet werden (Art. 32 Abs. 1 lit. a DS-GVO). | Bei Siilo werden alle Nachrichten mittels sicherer Ende-zu-Ende Verschlüsselung ausgetauscht, um die Vertraulichkeit und Integrität der Nachrichtendaten zu garantieren. Die Verschlüsselung erfolgt über NaCl, eine Open-Source-Bibliothek für die Verschlüsselung, Entschlüsselung und elektronische Signaturen. Der Schlüssel wird nur zwischen den Endgeräten von Absender und Empfänger ausgetauscht, so dass es Dritten (und auch Siilo) nicht möglich ist, ausgetauschte Nachrichten zu entschlüsseln oder gar zu lesen. |
| ✔ | 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 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. | Siilo garantiert den Nutzern, dass alle Nachrichten vollständig an den/die Empfänger übertragen werden. Der Übertragungsstatus der Nachricht wird graphisch mittels (doppelter) Häkchen, je nach Empfangsstatus in unterschiedlicher Farbe, dargestellt. Wird eine Nachricht (z.B. aufgrund fehlender Mobilfunkverbindung) nicht übertragen, wird dies für den Nutzer klar sichtbar durch eine rote Markierung der nicht-übermittelten Nachricht hervorgehoben. Bei wiederhergestellter Datenverbindung können Sie die Nachricht durch einfachen Klick erneut senden. Die Siilo-App verteilt Mitteilungen grundsätzlich nicht auf mehrere Nachrichten, sondern verschickt eine Mitteilung als eine Nachricht an den Empfänger. |

| | | |
|---|---|---|
| ✔ | 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. Werbezwecke) ist unzulässig. | Siilo nutzt Metadaten ausschließlich, um Nachrichten zu verschicken und für allgemeine statistische Zwecke. Diese Statistiken werden dem Krankenhaus zur Verfügung gestellt, um die Nutzung von Siilo innerhalb der Organisation evaluieren zu können. Ein Rückschluss auf das Verhalten einzelner Nutzer ist aber nicht möglich. |
| ✖ | 4. Es sollte zumindest optional der Einsatz offener Kommunikationsprotokolle (z.B. XMPP6 ) möglich sein, um eine Kommunikation mit anderen Messenger-Diensten zu ermöglichen. | Eine Kommunikation mit anderen Messenger-Diensten birgt das nicht unerhebliche Risiko, dass Daten/Nachrichten aus dem internen, sicheren Siilo-Netzwerk in unsichere, von Siilo nicht überprüfbare externe Strukturen mit entsprechendem Risiko von Datenschutzverletzungen übertragen werden. Auch wenn ist eine Kompatibilität mit anderen Messenger-Diensten grundsätzlich sinnvoll erscheint, halten wir bei Siilo dies aufgrund der besonderen Vertraulichkeit von Daten/Nachrichten mit medizinischen Inhalten und dem Risiko von Datenschutzverletzungen für problematisch. |

KAPITEL 3

# Sicherheit der Endgeräte

| Erfüllt | Anforderungen der Datenschutzaufsichtsbehörde | Wie werden diese von Siilo erfüllt? |
|---|---|---|
| In der Verantwortung des Mobilgerät-Besitzers | 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. | Der Zugriffsschutz zu einem persönlichen Mobilgerät liegt in der Verantwortung des Besitzers. Siilo kann hier keinen Einfluss nehmen. Für Krankenhäuser sollte dies in einer Datenschutz-Folgenabschätzung (DSFA) bzw. internen Dienstanordnung entsprechend klar geregelt werden. Siilo kann Krankenhäuser in diesem Prozess unterstützen, z.B. bei der Kommunikation von Richtlinien an die Mitarbeiter via Siilo. |
| In der Verantwortung des Mobilgerät-Besitzers | 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. | Siilo ist nur für Apple- und Android-Geräte verfügbar. Der Besitzer des Mobilgeräts ist allerdings für aktuelle Sicherheitsupdates verantwortlich. Für Krankenhäuser sollte die Aktualisierung von Sicherheitsupdates in einer Datenschutz-Folgenabschätzung (DSFA) bzw. internen Dienstanordnung entsprechend klar geregelt werden. |
| In der Verantwortung des Krankenhaus | 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 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. | Ein Krankenhaus sollte für seine Mitarbeiterinnen und Mitarbeiter ein Mobile Device Management (MDM) installieren. Siilo kann über jedes MDM betrieben werden. Seitens Siilo bieten wir die Fernlöschung der App mittels „remote wipe“ bei Verlust des Mobilgeräts an. |

KAPITEL 4

# Plattform/Betrieb

| Erfüllt | Anforderungen der Datenschutzaufsichtsbehörde | Wie werden diese von Siilo erfüllt? |
|---|---|---|
| ✔ | 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. | Bei Siilo handelt es sich um keinen Telekommunikationsdienst i.S.d. § 3 Nr. 17a Telekommunikationsgesetz (TKG). |
| ✔ | 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. | Bei Siilo werden alle Nutzer/-innen individuell verifiziert. Dies erfolgt über das Service-Desk von Siilo. Krankenhäuser/Organisationen haben darüber hinaus die Möglichkeit, Mitarbeiter/-innen über ein Mitarbeiterverzeichnis verifizieren zu lassen. Damit wird sichergestellt, dass nur zugelassene Nutzer an der Kommunikation teilnehmen können. Nutzer, die einer individuellen Verifizierung nicht zustimmen bzw. diese nicht erfüllen, werden nicht verifiziert bzw. sogar gesperrt. |
| ✔ | 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. | Eine Datenschutz-Folgenabschätzung (DSFA) zur Siilo-App liegt vor. Soweit eine datenschutzspezifische Verwendung der Siilo-App im Krankenhaus vorliegt, liegt das Erstellen einer weiteren Datenschutz-Folgenabschätzung (DSFA) im Ermessen und Verantwortungsbereich des Krankenhauses. |

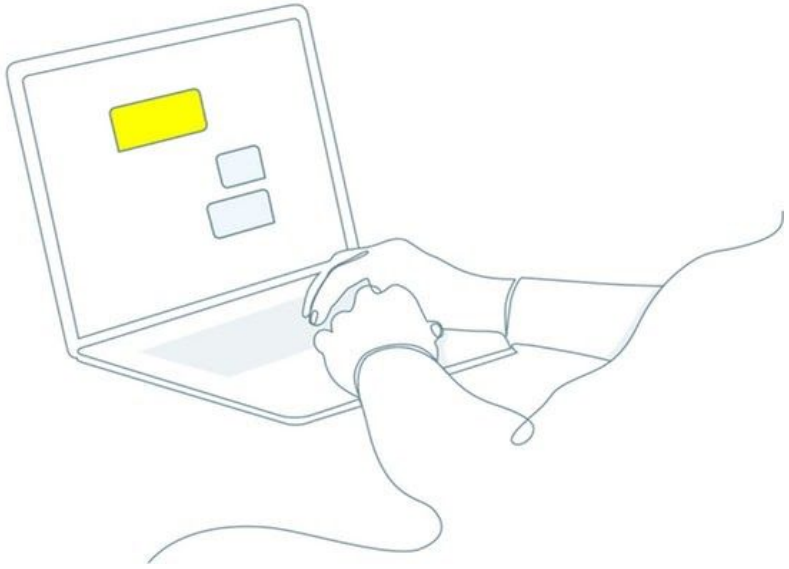
| | | |
|---|---|---|
| In der Verantwortung des Krankenhaus | 4. Für die Messenger-Lösung ist durch das Krankenhaus eine regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der zur Gewährleistung der Sicherheit der Verarbeitung getroffenen technischen und organisatorischen Maßnahmen vorzunehmen (Art. 32 Abs. 1 lit. d DS-GVO). | Siilo unterstützt Krankenhäuser bei der Überprüfung, Bewertung und Evaluierung der technischen und organisatorischen Maßnahmen. |
| ▬ | 5. Die Messenger-Lösung sollte einen Betrieb sowohl als Service eines Dienstleisters/Auftragsverarbeiters als auch der technischen Infrastruktur des Krankenhauses erlauben (On-Premises). | Siilo wird aus einer Reihe von Gründen bewusst nicht als „on-premise“ Lösung angeboten:<br>(1) Siilo bietet ein sicheres Experten-Netzwerk über die intersektoralen Grenzen von ambulanter und stationärer Medizin sowie über die Grenzen der in der Behandlung eines Patienten involvierten Fachdisziplinen (Ärzte, Apotheker, Physiotherapeuten, Pflege, etc.) hinaus. Wir glauben, dass eine Kommunikation zwischen z.B. Hausarzt und Krankenhaus im Sinne des Patienten wichtig ist. Eine Beschränkung der Kommunikation nur auf den stationären Aufenthalt wird dem Patienten nicht gerecht. Mediziner kommunizieren also regelmäßig mit Kollegen über Patienten, die (noch) nicht Patienten ihres Krankenhauses sind. Krankenhäuser sollten also keinen Zugriff auf diese Daten haben Eine Infrastruktur, die auf ein einzelnes Krankenhaus begrenzt ist, wird Siilo nicht gerecht.<br>(2) Bei den Servern zwischen den Siilo-Clients handelt es sich um "Store & Forward“ - Server. Dies bedeutet, dass die Daten nur für einen kurzen Zeitraum verfügbar sind und es daher wenig sinnvoll wäre, die Server vor Ort zu haben.<br>(3) Sicherheit durch Redundanz: Wenn die Server im Krankenhaus ausfallen, funktioniert zumindest der Messenger weiterhin. |
| ✔ | 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. | Siilo greift auf Dienste von Drittanbietern zurück, z.B. um Mobilfunknummern per SMS zu verifizieren oder aber für die sichere Videotelefonie mittels Siilo. Mit allen Drittanbieteren hat Siilo entsprechende Vereinbarungen getroffen, durch die sichergestellt wird, dass die Vorschriften der DS-GVO eingehalten 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, 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). | Siilo hat mit allen Auftragsverarbeitern entsprechende Verträge abgeschlossen, durch die sichergestellt wird, dass die Vorschriften der DS-GVO eingehalten werden. Die Auftragsverarbeiter von Siilo haben uns im Rahmen dieses Vertragsverhältnis die gewünschten Nachweise erbracht. |
| ✔ | 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 Containerlösung in der Mobile-Messenger-App. | Die bei einem Dienstleister gespeicherten Daten werden regelmäßig gelöscht. Die Speicherfrist auf Endgeräten ist seitens Siilo auf 30 Tage festgelegt. Danach werden Nachrichten automatisch gelöscht. |
| ✔ | 9. Sobald verfügbar, sind insbesondere sicherheitsrelevante Updates der App zeitnah auf allen eingesetzten Geräten durchzuführen. | Updates zur Verbesserung, insbesondere aber sicherheitsrelevante Updates werden dem Nutzer von Siilo unmittelbar nach Veröffentlichung in den jeweiligen App-Stores zur Verfügung gestellt. |

KOMMENTAR ZUM WHITEPAPER DER DATENSCHUTZKONFERENZ

# Danke für Ihr Interesse an Siilo.

Bei Rückfragen stehen wir ihnen gerne zur Verfügung: kontakt@siilo.com



Erstellt in Zusammenarbeit mit FPS

FPS
Ihre Kanzlei. Ihr Partner.