VEREINBARUNG ZUR AUFTRAGSVERARBEITUNG (AVV)

1. GEGENSTAND

Gegenstand vorliegender Auftragsverarbeitungsvereinbarung ("AVV") ist die Festlegung der Bedingungen für die Verarbeitung Personenbezogener Daten, die Doctolib vom Kunden/Nutzer für die Ausführung der Dienste zur Verfügung gestellt werden.

Im Rahmen der Vertragsbeziehungen verpflichten sich die Parteien zur Einhaltung der Bestimmungen der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016, die seit dem 25. Mai 2018 Anwendung findet (nachstehend "DSGVO") sowie der Bestimmungen des Bundesdatenschutzgesetzes ("BDSG").

2. BEGRIFFSBESTIMMUNGEN

Die vorliegender AVV zu Grunde gelegten Begriffsbestimmungen sind hier einsehbar.

3. WIRKSAMWERDEN UND DAUER

Vorliegende AVV gilt mit Abschluss des Hauptvertrages, dem es beigefügt ist, und für die gesamte Dauer der Vertragsbeziehung zwischen Doctolib und dem Kunden/Nutzer.

4. STATUS DER VERTRAGSPARTEIEN

Die Parteien sind sich einig, dass für die Verarbeitung der in Anhang 1 aufgeführten Personenbezogenen Daten und Gesundheitsdaten der Nutzer/Kunde der Verantwortliche und Doctolib und/oder Siilo die Auftragsverarbeiter sind.

Doctolib und/oder Siilo werden vom Nutzer/Kunden dazu ermächtigt, die für die Lieferung der Services erforderlichen Personenbezogenen Daten und Gesundheitsdaten zu den nachstehend genannten Zwecken und unter strikter Einhaltung der nachstehend genannten Bedingungen zu verarbeiten.

Die Verpflichtung von Doctolib ist auf die Bereitstellung der Dienste und das Hosting des Admin Tools sowie der App begrenzt.

Siilos Verpflichtung ist auf die Bereitstellung der App begrenzt.

Sobald der Verantwortliche für die Datenverarbeitung Personenbezogene Daten von Dritten in den Service eingibt (z.B. Daten von Patienten), muss der Verantwortliche für die Datenverarbeitung die gesetzlichen Anforderungen bezüglich der Information und/oder Einwilligung dieser Dritten einhalten.

4.1. Pflichten des Nutzers/Abonnenten

Der Nutzer und/oder Kunde ist in seiner Eigenschaft als Verantwortlicher für die Datenverarbeitung für die Führung seines Verzeichnisses der Verarbeitungstätigkeiten und gegebenenfalls für die Erfüllung von Anforderungen der für ihn zuständigen Datenschutzaufsichtsbehörde verantwortlich. Er ist auch dafür verantwortlich, die Patienten über die Aufnahme ihrer Personenbezogenen Daten und Gesundheitsdaten in die Dienste sowie über die Modalitäten der Ausübung ihrer Rechte zu informieren, indem er ihnen ein Informationsblatt zur Verfügung stellt.

Als für die Verarbeitung Verantwortlicher ist der Nutzer und/oder Kunde allein verantwortlich für die Zuverlässigkeit und Richtigkeit der übermittelten persönlichen Daten. Dies gilt insbesondere auch im Zusammenhang mit medizinischen Dokumenten, die über die Dienste verwaltet werden.

Der Nutzer und/oder Kunde verpflichtet sich dazu

- die ärztliche Schweigepflicht einzuhalten und für deren Einhaltung Sorge zu tragen;

- Nutzerrechte festzulegen, insbesondere im Hinblick auf Gesundheitsdaten von Patienten, entsprechend dem Willen der Patienten;

- Doctolib alle erforderlichen Daten für die Auftragsverarbeitung zur Verfügung zu stellen, darunter die Liste der zu verarbeitenden Personenbezogenen Daten, die gesetzliche Verarbeitungsgrundlage, die Verarbeitungszwecke und die Aufbewahrungsdauer der Personenbezogenen Daten;

- alle Weisungen zur Verarbeitung der Personenbezogenen Daten durch Doctolib schriftlich zu dokumentieren;

- die von Doctolib in seiner Eigenschaft als Auftragsverarbeiter durchgeführte Datenverarbeitung zu überwachen;

- einen Hauptansprechpartner, der den Verantwortlichen für die Datenverarbeitung vertritt, und ggf. einen Datenschutzbeauftragten gemäß den Bestimmungen der DSGVO zu benennen;

- in der Testphase nur Blinddaten, die keine Personenbezogenen Daten enthalten, mit Doctolib zu teilen;

- für die Einhaltung der im Übrigen in der DSGVO vorgesehenen Pflichten Sorge zu tragen.

4.2. Pflichten von Doctolib und Siilo

4.2.1. Doctolib und/oder Siilo verpflichtet sich dazu:

- Personenbezogene Daten in Übereinstimmung mit den in dieser AVV dargelegten Zwecken und Rahmenbedingungen zu verarbeiten und die für Personenbezogene Daten geltenden technischen Standards einzuhalten;

- nur auf die alleinige vorherige Weisung des für die Datenverarbeitung Verantwortlichen zu handeln. Im Falle der Unmöglichkeit oder Unzumutbarkeit, bestimmten Weisungen Folge zu leisten, wird Doctolib den Verantwortlichen schnellstmöglich informieren. Doctolib kann in diesem Fall um Befreiung von der Weisung ersuchen;

- keine Kopien Personenbezogener Daten ohne die Genehmigung oder Anweisung des für die Datenverarbeitung Verantwortlichen anzufertigen, diese nicht an Dritte weiterzugeben und nicht für andere als die im Vertrag genannten Zwecke zu verwenden;

- Personenbezogene Daten, die ihm von dem Verantwortlichen für die Datenverarbeitung anvertraut wurden, nicht im eigenen Auftrag oder im Auftrag Dritter, zu welchem Zweck und auf welche Weise auch immer, zu verwerten oder zu verarbeiten;

- alle ihm zur Verfügung stehenden Mittel gemäß den vertraglichen Bestimmungen und dem Stand der Technik einzusetzen, um die Sicherheit und die Vertraulichkeit der ihm anvertrauten Personenbezogenen Daten zu gewährleisten und insbesondere zu verhindern, dass diese verfälscht, beschädigt oder an unbefugte Dritte weitergegeben werden. Im Übrigen sind alle geeigneten technischen und organisatorischen Maßnahmen zu ergreifen, um Personenbezogene Daten gegen die unbeabsichtigte oder unrechtmäßige Zerstörung oder den unbeabsichtigten Verlust, die unbeabsichtigte Änderung und Verbreitung oder den unbefugten Zugriff sowie gegen jede Form der unrechtmäßigen Verarbeitung zu schützen;

- den für die Datenverarbeitung Verantwortlichen schnellstmöglich über jede Sicherheitslücke zu benachrichtigen, die direkt oder indirekt ihn betreffende Personenbezogene Daten oder Verarbeitungsvorgänge betrifft;

- regelmäßige Sicherungen der Personenbezogenen Daten durchzuführen;

- regelmäßige Intrusionstests durchzuführen;

- die für den störungsfreien Betrieb der Dienste erforderliche Hardware zu warten;

- die Vertraulichkeit der Personenbezogenen Daten zu gewährleisten;

- Aktualisierungen, Korrekturen, Löschungen oder sonstige Änderungen im Hinblick auf die Personenbezogenen Daten zu berücksichtigen;

- die geltende Aufbewahrungsfrist der Personenbezogenen Daten gemäß den Zwecken, für welche diese erhoben oder zur Verfügung gestellt wurden, einzuhalten und die Daten zu löschen/anonymisieren, wenn diese Zwecke nicht mehr bestehen, vorbehaltlich gesetzlicher Verpflichtungen;

- einen Datenschutzbeauftragten zu benennen.

4.2.2. Darüber hinaus verpflichtet sich Doctolib und/oder Siilo sicherzustellen, dass Personen, die gemäß dieser AVV zur Verarbeitung Personenbezogener Daten berechtigt sind

- sich zur Einhaltung der Vertraulichkeit verpflichten oder an eine angemessene gesetzliche Pflicht zur Verschwiegenheit gebunden sind;

- die für den Schutz Personenbezogener Daten erforderliche Schulung erhalten;

- die Grundsätze des Datenschutzes und des Schutzes Personenbezogener Daten als Standard bei Tools, Produkten, Applikationen oder Diensten berücksichtigen;

4.2.3. Hilfe und Beratung bei der Einhaltung der Bestimmungen:

Doctolib setzt alle erforderlichen Mittel ein, um dem Verantwortlichen bei der Durchführung von Datenschutz-Folgenabschätzungen sowie der vorangehenden Konsultation durch Aufsichtsbehörden zu helfen.

Doctolib stellt dem Verantwortlichen alle notwendigen Informationen über die Verarbeitung Personenbezogener Daten zur Verfügung, um ihn bei der Erfüllung seiner gesetzlichen und behördlichen Pflichten als Verantwortlicher der Datenverarbeitung gemäß den Bestimmungen der DSGVO (Anhang 3.1) zu unterstützen.

In Ermangelung besonderer Weisungen seitens des Verantwortlichen im Hinblick auf die Art der zu verarbeitenden Personenbezogenen Daten, deren Zwecke, Rechtsgrundlage und Aufbewahrungsfrist erkennt dieser an, dass die Personenbezogenen Daten gemäß der in den Anhängen 1 und 2 dargelegten Modalitäten verarbeitet werden. Der Nutzer/Kunde kann als Verantwortlicher der Datenverarbeitung während der Ausführung des Vertrags von seinem Weisungsrecht Gebrauch machen.

5. VERLETZUNG DES SCHUTZES PERSONENBEZOGENER DATEN

Bei jeder Verletzung des Schutzes Personenbezogener Daten benachrichtigt Doctolib den für die Datenverarbeitung Verantwortlichen unverzüglich, nachdem Doctolib hierüber Kenntnis erlangt hat.

Auf Anfrage des für die Datenverarbeitung Verantwortlichen sind dieser Benachrichtigung alle sachdienlichen Dokumentationen beizufügen, damit dieser erforderlichenfalls die zuständige Aufsichtsbehörde und gegebenenfalls die betroffenen Personen über die Verletzung unterrichten kann.

Fragen zu Vorfällen, die Auswirkungen auf die gehosteten Gesundheitsdaten haben, können an datenschutz@doctolib.de gerichtet werden.

6. FÜHREN EINES VERARBEITUNGSVERZEICHNISSES

Doctolib und Siilo führen ein Verzeichnis über alle Kategorien von Verarbeitungstätigkeiten, die im Auftrag des für die Verarbeitung Verantwortlichen ausgeführt werden gemäß den Bestimmungen der DSGVO.

7. INFORMATION UND RECHTE DER BETROFFENEN PERSONEN

Es obliegt dem für die Datenverarbeitung Verantwortlichen, (i) die betroffenen Personen über die im Rahmen der Dienste durchgeführte Verarbeitung zu informieren und, insofern dies nach geltendem Recht erforderlich ist, deren Zustimmung(en) einzuholen; (ii) die betroffenen Personen über die Rechtsgrundlage der durchgeführten Verarbeitung, die Zwecke der Verarbeitung und die Liste der Auftragsverarbeiter, welche die Personenbezogenen Daten verarbeiten können, zu informieren.

8. VERWALTUNG DER BETROFFENENRECHTE

Es obliegt dem für die Verarbeitung Verantwortlichen, Rechtsansprüchen betroffener Personen im Hinblick auf deren Personenbezogene Daten nachzukommen.

Soweit möglich kann Doctolib in seiner Eigenschaft als Auftragsverarbeiter und auf Anfrage des für die Verarbeitung Verantwortlichen diesen bei der Erfüllung seiner Pflicht, Datenschutzanfragen nachzukommen unterstützen. Hierzu zählen Anfragen in Bezug auf das Recht auf Zugang, Berichtigung,

Löschung und Widerspruch, Einschränkung der Verarbeitung sowie Datenübertragbarkeit.

9. SICHERHEIT UND VERTRAULICHKEIT

9.1 Im Hinblick auf die Dienste führt Doctolib die für die Sicherheit geeigneten technischen und organisatorischen Maßnahmen gemäß der DSGVO durch, die darauf abzielen, ein angemessenes Sicherheitsniveau in Bezug auf die Risiken zu gewährleisten, die durch die Verarbeitung Personenbezogener Daten des Nutzers/Kunden entstehen wie in Anhang 2 (Technische und organisatorische Maßnahmen) angegeben. Bei der Bewertung der angemessenen Sicherheitsstufe wird Doctolib die Risiken berücksichtigen, die sich aus der unbeabsichtigten oder unrechtmäßigen Zerstörung, Beschädigung, Verlust, Änderung, unbefugten Weitergabe oder dem unbefugten Zugang zu Personenbezogenen Daten ergeben können, die gemäß den Bestimmungen von Artikel 32 der DSGVO übermittelt, gespeichert oder anderweitig verarbeitet werden können.

Notwendige interne Maßnahmen des Kunden / Nutzers zum Schutz von Patientendaten bleiben hiervon unberührt.

Es wird zwischen den Parteien vereinbart, dass der Vertrag, der vorliegende AVV enthält, der zuständigen Aufsichtsbehörde zur Prüfung vorgelegt werden kann.

9.2 Berufsgeheimnis: Doctolib ist bekannt, dass die bei der Nutzung der Dienste durch den Verantwortlichen verarbeiteten Daten unter das Berufsgeheimnis fallen (§ 203 StGB).

Doctolib ist verpflichtet, alle bei dessen Berufsausübung erlangten Informationen, die unter die ärztliche Schweigepflicht und das Patientengeheimnis fallen, strikt geheim zu halten und vor dem Zugriff unberechtigter Dritter zu schützen. In gleicher Weise wird Doctolib seine Mitarbeiter sowie Unterauftragnehmer zur Geheimhaltung verpflichten.

9.3 Eigentum an Profildaten: Sofern keine ausdrücklichen anderen Vereinbarungen zum Datenschutz getroffen wurde, bleibt der Verantwortliche alleiniger Herr der Kunden-/Nutzerdaten, die auf den Dienste veröffentlicht wurden. Doctolib kann aus der Veröffentlichung keine Rechte an den Daten geltend machen, die von dem Verantwortlichen veröffentlicht wurden. Die anonymisierten Nutzungsstatistiken der Dienste sind Eigentum von Doctolib.

10. PERSONAL VON DOCTOLIB

Für die Erbringung der Dienste setzen Doctolib und Siilo ausreichend und qualifiziertes Personal ein, das über die für die Leistungserbringung erforderlichen technischen oder funktionalen Fähigkeiten verfügt. Personen, die zur Verarbeitung Personenbezogener Daten im Auftrag des für die Datenverarbeitung Verantwortlichen befugt sind, müssen eine Schulung zur Datenschutzgrundverordnung erhalten haben.

11. UNTERVERARBEITUNG

Die Verarbeitungstätigkeiten im Zusammenhang mit den Diensten werden für Doctolib von Siilo durchgeführt, einer hundertprozentigen Tochtergesellschaft von Doctolib, die als Unterauftragsverarbeiter von Doctolib fungiert.

Darüber hinaus ist Doctolib zur Beauftragung der hier aufgelisteten Unterauftragsverarbeiter berechtigt, wenn dies für die Erbringung der Dienste in angemessener Weise erforderlich ist. Hierbei verpflichtet sich Doctolib dazu, den Verantwortlichen mittels einer schriftlichen Ankündigung dreißig (30) Tage im Voraus über jeden beabsichtigten Wechsel durch Hinzufügung oder Ersatz eines Unterauftragsverarbeiters zu informieren. Dadurch kann der Verantwortliche Einwände, die er gegen diese Wechsel haben könnte, rechtzeitig erheben. Sollte der Verantwortliche berechtigte und nachvollziehbare Gründe haben, die Beauftragung eines neuen Unterauftragsverarbeiters abzulehnen, muss der Nutzer unverzüglich eine begründete Beschwerde bei Doctolib unter datenschutz@doctolib.de innerhalb einer Frist von dreißig (30) Werktagen nach erteilter Ankündigung einlegen.

Im Hinblick auf die Unterauftragsverarbeiter muss Doctolib (i) angemessene Sorgfalt bei der Bewertung, Ernennung und Überwachung der Tätigkeiten des Unterauftragsverarbeiters an den Tag legen; (ii) in den Vertrag zwischen Doctolib und jedem Unterauftragsverarbeiter Klauseln einfügen, mit denen ein gleichwertiger Schutz für die Personenbezogenen Daten des Nutzers gewährleistet wird; Doctolib bleibt (iii) gegenüber dem Nutzer/Kunden für jegliche Nichterfüllung der Pflichten durch die Unterauftragsverarbeiter bei der Verarbeitung der personenbezogenen Nutzer-/Kundendaten vollumfänglich haftbar.

12. AUDIT

12.1 Zur Messung der Sicherheit der Doctolib-Plattform kann der für die Datenverarbeitung Verantwortliche auf eigene Kosten IT-Sicherheitsaudits unter Einhaltung der im vorliegenden Artikel vorgesehenen Bedingungen und innerhalb eines Umfangs von einem (1) Audit pro Jahr mit einer maximalen Dauer von fünf (5) Werktagen durchführen, wobei der Zeitaufwand des Personals von Doctolib dem für die Verarbeitung Verantwortlichen in Rechnung gestellt wird.

12.2 Das Audit beschränkt sich auf die Prüfung der Prozesse, der Organisation und der Tools, die direkt und ausschließlich mit der Umsetzung der DSGVO-Bestimmungen in den betreffenden Diensten in Verbindung stehen.

Ziel des Audits ist in keinem Fall die Überwachung oder Zugriffsanfrage (i) auf nicht spezifische Personenbezogene Daten des Nutzers/Kunden, gleich ob diese vertraulich sind oder nicht, oder auf jegliche Information, deren Verbreitung nach Ermessen von Doctolib der Sicherheit der Doctolib-Plattform oder eines anderen Nutzers schaden könnte; (ii) auf die Finanzdaten von Doctolib; oder (iii) auf Personenbezogene Daten der Angestellten von Doctolib oder dessen Unterauftragsverarbeitern.

Es wird vereinbart, dass keine der im Rahmen eines Audits durchgeführten Tätigkeiten (i) den Betrieb von Diensten, Systemen, Netzwerken, Software oder Hardware in irgendeiner Weise behindern, modifizieren oder beeinflussen darf, die nicht für die ausschließliche Nutzung durch den Nutzer/Kunden bestimmt sind; (ii) die Infrastruktur beschädigen darf, die das Patientenportal und die Doctolib-Plattform beherbergt; (iii) Daten

jeglicher Art beschädigen, löschen oder modifizieren darf; (iv) unbefugten Zugriff auf die oben genannten Daten oder deren Pflege ermöglichen darf.

Jegliche Intrusions- oder Penetrationstests, die auf die Doctolib-Plattform und -Anwendung abzielen, sind gleich aus welchem Grund untersagt und von den Audits ohne die vorherige schriftliche Zustimmung von Doctolib ausgeschlossen.

Alle für die Durchführung des Audits erforderlichen Unterlagen und Informationen werden den Auditoren ausschließlich in den Geschäftsräumen von und durch Doctolib zur Verfügung gestellt, ohne die Möglichkeit, diese einzubehalten oder von diesen Kopien anzufertigen. Dieses Verbot gilt ebenfalls für alle Unterlagen und Informationen, die von den Unterauftragsverarbeitern von Doctolib zur Verfügung gestellt werden.

12.3 Der für die Datenverarbeitung Verantwortliche muss Doctolib mindestens (30) Tage vor Durchführung des Audits eine Auditvereinbarung mit folgenden Angaben zukommen lassen: Genauer Umfang, Daten und Uhrzeiten, und die Bedingungen. Der Auditor muss ebenfalls die ggf. für die Tests verwendeten Konten und Profile angeben (IP-Adresse Quellen, User Agent usw.), die verwendete Methode sowie das vom Audit betroffene Personal.

Der Inhalt der Auditvereinbarung muss vor Beginn eines jeden Audits von Doctolib vorab genehmigt worden sein.

12.4 Die im Laufe des Audits erhaltenen Informationen sind Vertrauliche Informationen und müssen als solche von dem für die Verarbeitung Verantwortlichen behandelt werden. Die o.g. Informationen dürfen ausschließlich an Personen weitergegeben werden, die zu strengster Geheimhaltung verpflichtet worden sind und die ein unmittelbares und maßgebliches Interesse an deren Kenntnis haben. Die Informationen dürfen auf keinen Fall öffentlich oder intern verbreitet werden.

Wenn der für die Datenverarbeitung Verantwortliche die Hinzuziehung eines externen Auditors wünscht, muss er hierfür vorab die schriftliche Zustimmung von Doctolib einholen, wobei davon ausgegangen wird, dass Doctolib den besagten Auditor nur bei Vorliegen berechtigter Interessen ablehnen kann.

Der externe Auditor darf in keinem Fall ein Konkurrent von Doctolib sein und muss sich schriftlich zur Einhaltung der im vorliegenden Artikel genannten Bedingungen verpflichten.

Der für die Verarbeitung Verantwortliche verpflichtet sich dazu, Doctolib den Auditbericht kostenfrei zur Verfügung zu stellen.

Doctolib wird nach Erhalt des Berichts eine angemessene Frist eingeräumt, um die festgestellten Mängel und/oder Nichtkonformitäten zu beheben.

13. DATENEXPORT

Der Kunde bzw. der Nutzer kann die Nutzer*innen-Inhalte, die in den Diensten gespeichert sind, während der gesamten Vertragsdauer exportieren, indem er direkt den (im Netzwerk-Feed geteilten) Beitrag oder die Konversation über die in der App verfügbare Exportfunktion exportiert.

Wenn der Nutzer den Sicherungs-/Wiederherstellungsdienst nicht aktiviert hat, werden die Nutzer*innen-Inhalte standardmäßig nur auf dem für die Dienste verwendeten Gerät des Nutzers gespeichert, und zwar nur für einen Zeitraum von dreißig (30) Tagen.

Bei Nutzern, die den Sicherungs-/Wiederherstellungsservice aktiviert haben, speichert Doctolib die Nutzer*innen-Inhalte auf seinen Servern und verpflichtet sich, eine Kopie der Daten für den Nutzer/Kunden während der gesamten Vertragslaufzeit bereitzuhalten.

Doctolib verpflichtet sich, die Gesundheitsdaten nach einer Frist von 7 Tagen nach Vertragsende zu vernichten, ohne eine Kopie aufzubewahren, vorbehaltlich der gesetzlichen Aufbewahrungspflichten, denen Doctolib unterliegt. Der Prozess für die Vernichtung von Gesundheitsdaten kann auf Anfrage des für die Verarbeitung Verantwortlichen mitgeteilt werden.

14. WEITERGABE PERSONENBEZOGENER DATEN

Personenbezogene Daten dürfen nur zu den in dieser AVV zum Schutz Personenbezogener Daten aufgeführten Zwecken und in Übereinstimmung mit der geltenden Gesetzgebung an Unternehmen der Doctolib Gruppe, deren Auftragnehmer oder Dienstleister übertragen werden, die in Ländern ansässig sind, die über ein angemessenes Schutzniveau verfügen oder angemessene Garantien hinsichtlich des Schutzes der Privatsphäre und der Grundrechte und -freiheiten von Personen bieten.

Doctolib informiert den Nutzer/Kunden, dass persönliche Daten von Doctolib auch in Drittländer an seine Unterauftragsverarbeiter übertragen werden können, falls eine solche Übertragung für die Ausführung der bestellten Dienste erforderlich ist. Die Liste der Unterauftragsverarbeiter ist hier verfügbar.

Wenn die Datenweitergabe in ein Drittland erfolgt, dessen Gesetzgebung über kein anerkanntes Schutzniveau für Personenbezogene Daten verfügt, stellt Doctolib sicher, dass angemessene Maßnahmen in Übereinstimmung mit der DSGVO getroffen werden, und insbesondere, falls notwendig, dass Standardvertragsklauseln oder gleichwertige Ad-hoc-Klauseln in den Vertrag aufgenommen werden, der zwischen Doctolib und dem Unterauftragsverarbeiter abgeschlossen wurde.

In ihrer Eigenschaft als Auftragsverarbeiter verpflichten sich Doctolib und Siilo dazu, die Personenbezogenen Daten auf dem Gebiet der Europäischen Union zu hosten oder hosten zu lassen und, falls notwendig, alle in dieser AVV festgelegten Verpflichtungen auf den Dienstleister zu übertragen, der die Personenbezogenen Daten hostet.

Darüber hinaus kann Doctolib auf Anfrage von Verwaltungs- und Justizbehörden Personenbezogene Daten, die sie im Namen des für die Verarbeitung Verantwortlichen verarbeitet, weitergeben, um ihren gesetzlichen Verpflichtungen nachzukommen. In diesem Fall wird Doctolib den für die Verarbeitung Verantwortlichen über die Weitergabe informieren, soweit gesetzlich zulässig.

15. KONTAKT UND ZUSTÄNDIGE AUFSICHTSBEHÖRDEN

Bei Fragen zu der von Doctolib durchgeführten Verarbeitung Personenbezogener Daten kann der Nutzer/Kunde gemäß den vertraglichen Bestimmungen den Datenschutzbeauftragten von Doctolib unter untenstehend angegebener Adresse kontaktieren.

Kontakt zu unserer Datenschutzbeauftragten können Sie über datenschutz@doctolib.de aufnehmen.

Jeder Nutzer hat die Möglichkeit, Beschwerden direkt an eine Datenschutzbehörde zu richten. Dies kann die Datenschutzbehörde am üblichen Aufenthaltsort, Arbeitsplatz, eigenen Unternehmenssitz oder am Sitz von Doctolib GmbH sein. Am Sitz von Doctolib GmbH ist die Berliner Beauftragte für Datenschutz und Informationsfreiheit zuständig, Alt-Moabit 59-61, 10555 Berlin, E-Mail: mailbox@datenschutz-berlin.de.

Federführende Aufsichtsbehörde nach Art. 56 DSGVO für die Doctolib Gruppe ist die für die Muttergesellschaft Doctolib SAS zuständige französische Aufsichtsbehörde CNIL (https://www.cnil.fr).

16. ANWENDBARES RECHT

Die AVV untersteht dem Recht des Landes, das auf den für die Datenverarbeitung Verantwortlichen Anwendung findet.

17. Geltung des AVV

Diese AVV regelt die vertraglichen Beziehungen der Auftragsvereinbarung in abschließender Weise und ersetzt alle bisherigen Vereinbarungen zur Auftragsverarbeitung.

ANHANG 1: ANGABEN ZUR VERARBEITUNG PERSONENBEZOGENER DATEN

Vorliegender Anhang 1 enthält bestimmte Angaben über die Verarbeitung Personenbezogener Daten gemäß Artikel 28 Abs. 3 DSGVO.

FÜR DIE VERARBEITUNG VERANTWORTLICHER: Der Kunde, der ein Doctolib-Abonnement abgeschlossen hat oder Nutzer, der ein Nutzerkonto besitzt.

Die Tätigkeiten des für die Verarbeitung Verantwortlichen umfassen Datenverarbeitungen, welche die Ausübung von Präventions-, Diagnose- und Behandlungstätigkeiten sowie die administrative Verwaltung seiner Gesundheitseinrichtung ermöglichen. Insbesondere, für die Zwecke der Patientenversorgung, umfasst die Verarbeitung (i) Instant Messaging (Doctolib Siilo Messenger und Docotlib Siilo Webchat), and (ii) ein Privates Organisationsnetzwerk (Doctolib Siilo für Organisationen).

Die eingesetzte Datenverarbeitung muss einem genauen Zweck entsprechen und im Hinblick auf die Aufgaben und Tätigkeiten der Medizinischen Fachkräfte gerechtfertigt sein.

Auftragsverarbeiter: Doctolib

Die Tätigkeiten des Auftragsverarbeiters umfassen die nachfolgend beschriebenen Dienste.

VERARBEITUNG NR. 1: BEREITSTELLUNG EINES INSTANT-MESSAGING-DIENSTES (Doctolib Siilo Messenger und Doctolib Siilo Webchat)

VERARBEITUNGSVORGANG :

Die Dienste beinhalten die Erhebung, Registrierung, Organisation, Aufbewahrung, Extraktion, Abfrage und Nutzung, Kommunikation durch Übertragung, Anonymisierung und Löschung der unten aufgelisteten Personenbezogenen Daten.

DATENVERARBEITUNGSZWECKE:

Der kostenlose Instant-Messaging-Dienst wurde entwickelt, um eine bessere Koordinierung der Gesundheitsfürsorge zu gewährleisten, und ermöglicht den Nutzern die Kommunikation und den Versand von Textnachrichten, Videos, Fotos, Sprachnotizen und anderen Medien. Doctolib Siilo Messenger / Doctolib Siilo Webchat ermöglicht sowohl Einzel- als auch Gruppendiskussionen.

1/ Erleichterung der Kommunikation zwischen Medizinischen Fachkräften durch Bereitstellung eines sicheren Kanals für den Austausch per Instant Messaging ;
2/ Den Austausch von Dokumenten, Daten und anderen Medien zu ermöglichen, die Personenbezogene Daten von Patienten enthalten können;
3/ Den Nutzern des Messenger-Dienstes zu ermöglichen, einen anderen Nutzer zu blockieren oder zu entsperren;
4/Reporting, Debugging und Statistiken.

RECHTSGRUNDLAGE DER VERARBEITUNG:

Es obliegt dem für die Verarbeitung Verantwortlichen, diese Rechtsgrundlage vor jeder Verarbeitung sicherzustellen und zu benennen.

Als Anhaltspunkt weisen wir darauf hin, dass ein berechtigtes Interesse die Rechtsgrundlage darstellen könnte. Es steht dem für die Verarbeitung Verantwortlichen frei, Doctolib eine andere Rechtsgrundlage zu nennen.

Für den Fall, dass der für die Verarbeitung Verantwortliche Gesundheitsdaten an eine Medizinische Fachkraft weitergibt, die nicht zum Behandlungsteam des gegebenen Patienten gehört, muss er zuvor die Einwilligung des Patienten einholen.

BETROFFENE PERSONEN:

1/ Patienten
2/ Medizinische Fachkräfte mit einem Konto.

ARTEN DER PERSONENBEZOGENEN DATEN:

Die folgenden Daten werden grundsätzlich als relevant für die oben genannten Zwecke angesehen:

- Identifikationsdaten zu Medizinischen Fachkräften;
- Kontaktdaten zu Medizinischen Fachkräften;
- Medizinische Vorinformationen (z.B. Allergien);
- Konsultationsdaten;
- Verschreibungsdaten;
- Fotos, Videos;
- Sprachnotizen
- Daten in Bezug auf das Behandlungsteam ;
- Nutzungs- und Verbindungsinformationen im Zusammenhang mit der Nutzung der Doctolib-Dienste durch den Nutzer/Kunden

EMPFÄNGER DER DATEN:

Medizinische Fachkräfte mit einem Nutzerkonto ;

AUFBEWAHRUNGSDAUER:

Sofern der Nutzer nicht die Option "Konversation aufbewahren" in den spezifischen Einstellungen der jeweiligen Konversation aktiviert hat, werden alle Nachrichten nach einer Frist von dreißig (30) Tagen gelöscht.

VERARBEITUNG NR. 2: PRIVATES ORGANISATIONSNETZWERK (Doctolib Siilo für Organisationen)

VERARBEITUNGSVORGANG:

Die Dienste umfassen die Erhebung, die Aufzeichnung, die Organisation, die Speicherung, das Abrufen, die Abfrage und die Nutzung, die Verwendung zur Kommunikation, die Offenlegung durch Übermittlung, die Anonymisierung und die Löschung der unten aufgeführten Personenbezogenen Daten.

DATENVERARBEITUNGSZWECKE:

Durch Doctolib Siilo für Organisationen können Mitarbeiter/Mitglieder der Organisation einander leicht finden und kontaktieren und Informationen über den Netzwerk-Feed austauschen. Über das Doctolib Siilo für Organisationen Admin Tool können die Mitarbeiter des Kunden ihr Organisationsnetzwerk konfigurieren und personalisieren, Nachrichten versenden, Personen einladen, dem Netzwerk beizutreten und Konversationen für Nutzer vorbereiten.

Doctolib kann auch Berichte, Fehlersuche und Statistiken für das Konto des Verantwortlichen durchführen bzw. erstellen.

RECHTSGRUNDLAGE DER VERARBEITUNG:

Es obliegt dem für die Verarbeitung Verantwortlichen, die Rechtsgrundlage vor jeder Verarbeitung zu bestimmen.

Als Anhaltspunkt weisen wir darauf hin, dass ein berechtigtes Interesse die Rechtsgrundlage darstellen könnte. Es steht dem für die Verarbeitung Verantwortlichen frei, Doctolib eine andere Rechtsgrundlage zu nennen.

BETROFFENE PERSONEN:

1/ Patienten;
2/ Medizinische Fachkräfte oder Assistenten mit Nutzerkonto.

ARTEN DER PERSONENBEZOGENEN DATEN:

Die folgenden Daten werden grundsätzlich als relevant für die oben genannten Zwecke angesehen:

- Identifikationsdaten;
- Kontaktdaten;
- Daten zu Lebensgewohnheiten, z.B. körperliche Betätigung, Diät und Essverhalten, etc. ;
- Medizinische Vorgeschichte, Familiengeschichte und Allergien ;
- Konsultationsdaten;
- Verschreibungsdaten;
- Biometrische und biologische Daten ;
- Daten über das Behandlungsteam ;
- Medizinische Bildgebung ;
- Nutzungs- und Verbindungsinformationen im Zusammenhang mit der Nutzung der Doctolib-Dienste durch den Nutzer/Kunden
- Identifikationsdaten, berufliche Daten und Kontaktdaten der Medizinischen Fachkräfte und Assistenten, die zur Organisation des für die Verarbeitung Verantwortlichen gehören;
- Identifikationsdaten der Medizinischen Fachkräfte;
- Kontaktdaten der Medizinischen Fachkräfte;
- Krankengeschichte, Familiengeschichte und Allergien;
- Konsultationsdaten;
- Verschreibungsdaten;
- Biometrische und biologische Daten;
- Daten des Gesundheitsteams;
- Medizinische Bilder;
- Fotos;
- Nutzungs- und Verbindungsprotokolle, die Aufschluss über die "geschäftlichen Handlungen" der Nutzer innerhalb der Dienste geben, sowie technische Protokolle, die Aufschluss über die "Aktivität" der vom Nutzer/Kunden verwendeten Software- und Hardwarekomponenten geben, damit Doctolib den Betrieb und den Zugang zu den angeforderten Funktionalitäten gewährleisten kann.

EMPFÄNGER DER DATEN:

Medizinische Fachkräfte mit einem Benutzerkonto

AUFBEWAHRUNGSDAUER:

Sofern der für die Verarbeitung Verantwortliche nicht ausdrücklich etwas anderes anordnet, wendet Doctolib die von den zuständigen Aufsichtsbehörden oder den geltenden Rechtsvorschriften empfohlenen Aufbewahrungsfristen an.

ANHANG 2: TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN

Die technischen und organisatorischen Maßnahmen, die Doctolib für die Bereitstellung der Dienste einsetzt, stützen sich auf die Sicherheitsmaßnahmen und -verfahren von Siilo.

Organisatorische und administrative Maßnahmen und Kontrollen

Siilo hat ein Informationssicherheitsmanagementsystem (ISMS) eingeführt und ist nach ISO27001 und NEN7510 (niederländischer Standard für das Management der Informationssicherheit im Gesundheitswesen) zertifiziert.

Als Teil des ISMS hat Siilo mehrere organisatorische und administrative Richtlinien und Kontrollen eingeführt, wie z. B. regelmäßige und standardmäßige Risikobewertungen, interne Audits, eine Informationssicherheitsrichtlinie, ein Zugriffs- und Berechtigungskonzept, Schulung des Personals, ein Verfahren für das Management von (Sicherheits-)Vorfällen und ein Verfahren zur Meldung von Verletzungen des Schutzes Personenbezogener Daten. Das Ziel des ISMS von Siilo ist es, eine weitere Verbesserung der Organisation, der Mitarbeiter und der Produkte zu ermöglichen.

Jede Lösung, die Siilo implementiert, wird einer Risikobewertung und, falls erforderlich, einer Datenschutzfolgenabschätzung unterzogen. Sie folgt einem strengen Prozess, der durch unsere ISMS-Richtlinien abgesichert und durch unsere Zertifikate ISO-27001 und NEN7510 nachgewiesen ist.

Entwicklungsprozess

Im Entwicklungsprozess von Siilo kommen mehrere Strategien zum Einsatz, um sowohl die Qualität als auch die Sicherheit der Daten zu gewährleisten:

(1) Unit-Tests: Für jede Funktion entwickelt Siilo eine Reihe von Basistests, die diese Funktion isoliert testen;

(2) Peer Code Review: Änderungen an der App werden von mindestens zwei Entwicklern überprüft, bevor sie in eine Betaversion aufgenommen werden. Bei Funktionen, die sich auf sicherheits- oder datenschutzrelevante Aufgaben auswirken, werden diese neuen Codezeilen von einem erfahrenen, teamfremden Entwickler geprüft, der sich mit den Sicherheits- und Datenschutzteams abstimmt, bevor er die neue(n) Funktion(en) für den Messenger freigibt.

(3) Manuelles Testen und begrenzte öffentliche Betaversion: Vor der Freigabe werden die Funktionen intern für manuelle Tests und oft auch für eine ausgewählte Gruppe von "freundlichen Betatestern" freigegeben.

Dieser Ansatz wird verwendet, um gerätespezifische Funktionen sowie alle Funktionen zu prüfen, die sich erst nach dem Kontakt mit einer Vielzahl von Arbeitsabläufen herauskristallisieren.

Zugriffs- und Berechtigungskonzept

Zugriffsberechtigungen werden autorisierten Mitarbeitern auf einer strengen Need-to-have-Basis gewährt. Dies wird überwacht und jährlich von einem Sicherheitsbeauftragten überprüft. Jeder Mitarbeiter, der Zugang zu Informationen außerhalb der ihm zugewiesenen Rolle benötigt, muss die Anfrage zunächst mit unserer Standardvorlage protokollieren. Diese Anträge werden einmal pro Quartal überprüft.

Technische Richtlinien und Kontrollen

Nachrichtendaten - Daten im Transit

Um die Lösungen zur Minderung der Risiken für Daten im Transit zu verstehen, lesen Sie bitte Siilos Sicherheits-Whitepaper (https://www.siilo.com/resources/security-white-paper), in dem der Security-by-Design-Ansatz, das Bedrohungsmodell und die kryptographischen Protokolle detailliert beschrieben werden.

Kurz gesagt, Siilo verwendet eine Ende-zu-Ende-Verschlüsselung, die mit LibSodium, einem Fork der NaCl Krypto-Bibliothek https://nacl.cr.yp.to/, implementiert wurde.

Das bedeutet, dass jede Nachricht zwischen Sender und Empfänger durch ein öffentliches/privates Schlüsselpaar geschützt ist. Nur Sender und Empfänger sind in der Lage, die zwischen ihnen ausgetauschten Nachrichten zu entschlüsseln und zu lesen, und die Authentizität jeder Nachricht kann empirisch überprüft werden. Dritte, einschließlich Siilo, Doctolib und deren Mitarbeiter, können sie niemals lesen.

Siilo verwendet Certificate Pinning, um so genannte "Man-in-the-Middle"-Angriffe zu verhindern, bei denen Angreifer auf den Datenverkehr zwischen den Telefonen zugreifen und versuchen, die Kommunikationsleitungen anzuzapfen, um die Nachrichten zu lesen. Die standardmäßige TLS v1.2-Kommunikation erfordert ein gültiges SSL-Zertifikat, das von einer vertrauenswürdigen Zertifizierungsstelle ausgestellt und vom Gerät erkannt wird. Certificate Pinning geht noch weiter und schreibt vor, dass diese Zertifikate nur von einer Vertrauenskette ausgestellt werden dürfen, die auf einen bestimmten Aussteller zurückgeht. Damit wird eine ganze Reihe von Sicherheitslücken geschlossen, die sich aus den Problemen bei der Schlüsselverteilung im Zusammenhang mit der Infrastruktur der Zertifizierungsstellen im Internet ergeben.

Nachrichtendaten - Daten im Ruhezustand auf dem Endgerät

Für die auf dem Gerät (iPhone, iPad, Android) ruhenden Daten gibt es die folgenden Sicherheitsvorkehrungen:

- Das gesamte "Schlüsselmaterial", auch bekannt als die vom Kryptographen verwendeten Codes, wird in der iOS KeyChain bzw. im Android KeyStore gespeichert;
- Das gesamte "Schlüsselmaterial" wird mit einem "Hauptschlüssel" verschlüsselt, der von dem vom Benutzer gewählten Pin-Code abgeleitet ist;
- Die gesamte Datenbank wird mit SQLiteCipher verschlüsselt. Alle Nachrichten, Nachrichten-Metadaten und Kontaktinformationen werden auf diese Weise gespeichert;
- Alle empfangenen Medien werden mit einem symmetrischen Einwegschlüssel verschlüsselt gespeichert. Der Zugriff auf diesen Schlüssel erfolgt über die oben erwähnte Datenbank;
- Ein Pincode-Mechanismus auf Ebene der App verhindert den Zugriff durch Menschen, die physischen Zugang zum Gerät haben. Dies verhindert die meisten Formen von Social Engineering, wie z. B. die Bitte, das Telefon für einen kurzen Anruf auszuleihen, usw.
- Alle im Messaging Service ausgetauschten Informationen werden nach 30 Tagen automatisch gelöscht. Nutzer können selbst entscheiden, ob sie einzelne Nachrichten ad hoc löschen wollen, wenn sie 30 Tage für zu lang halten. Siilo hat bewusst keine Count-Down-Timer und Nachrichtenlaufzeiten wie Sekunden/Stunden eingebaut, da dies ein Gefühl der Dringlichkeit erzeugen könnte, was zu Screenshots und anderem unerwünschten Verhalten auf der Empfängerseite führt;
- Wenn ein Benutzer weiß, dass sein Gerät verloren gegangen ist, gestohlen wurde oder anderweitig gefährdet ist, kann er/sie seine/ihre Organisation benachrichtigen (dies ist ein Doctolib Siilo für Organisationen Feature) und ein Admin kann die Siilo-Daten aus der Ferne vom Gerät löschen.

Nachrichtendaten - Daten im Ruhezustand auf Siilo Servern

Für ruhende Daten auf Siilo-Servern gibt es die folgenden Sicherheitsvorkehrungen:

- Alle Siilo Server befinden sich innerhalb der Europäischen Union mit den höchsten Sicherheits- und Compliance-Normen;
- Firewall-Regeln verhindern den Netzwerkzugriff auf die Datenbanken (MySQL und ElasticSearch) und beschränken sich auf ein Subnetz, das die Siilo-Server und ein VPN enthält, auf das eine begrenzte Gruppe von Siilo-Mitarbeitern zugreifen kann;
- Die MySQL-Datenbank ist passwortgeschützt und mit dem Industriestandard AES-256 verschlüsselt und speichert Messaging-Daten, Messaging-Metadaten, Siilo Connect-Konfigurationsdaten und Benutzerprofildaten;
- ElasticSearch verschlüsselt bestimmte Felder wie E-Mail und Telefonnummern, um einen Abgleich zu ermöglichen. Andere Profilfelder, die in der Doctolib Siilo Messenger App als "öffentlich" für die Nutzer angezeigt werden, werden im Klartext gespeichert;
- Alle Medien (die über die Anwendung versendet werden und daher als sensibel gelten) werden gespeichert und mit einem einmaligen symmetrischen Schlüssel verschlüsselt. Dieser Schlüssel wird auf keinem Siilo-Server gespeichert, außer als Teil der verschlüsselten Nachrichtendaten, die in MySQL gespeichert werden. Die Schlüssel zur Entschlüsselung dieser Daten sind nur auf den Geräten des Senders und des Empfängers verfügbar. Speicherung von Personenbezogenen Daten auf Siilo-Servern
- Die Nachrichtendaten werden auf Servern in Frankfurt (Deutschland) gespeichert und zu Sicherungszwecken werden täglich automatisierte "Snapshots" erstellt, die nicht länger als 7 Tage aufbewahrt werden. Diese Snapshots werden im Ruhezustand verschlüsselt. Die Server-Infrastruktur von Siilo wird von Amazon, Inc. gehostet. Siilo hat sich bewusst für Amazon Web Services (AWS) entschieden, da diese die höchsten Sicherheits- und Verschlüsselungsstandards anwenden und mit ihren SOC Level I-II-III, ISO9001, ISO27001, ISO27017 und ISO27018 Zertifizierungen die Einhaltung der gesetzlichen Bestimmungen (DSGVO) gewährleisten.

Benutzerdaten

Alle messagingbezogenen Daten werden auf Servern in Frankfurt (Deutschland) gespeichert. Für Dienste wie die E-Mail-Überprüfung und die Protokollierung gemäß der Sicherheitsrichtlinien für Website-Inhalte werden die Daten in Irland gespeichert.

Rufnummernabgleich im Messaging Service

Siilo ermöglicht es dem Nutzer optional, andere Siilo-Kontakte durch Abgleich mit dem Adressbuch des Telefons zu finden. Wenn der Nutzer dies wünscht, werden die folgenden Informationen über eine verschlüsselte TLS-Verbindung zum Server hochgeladen:

(1) Die ersten 64 Bits des SHA1-Hashes der E.164-normierten Form jeder Telefonnummer aus dem Adressbuch des Telefons

(2) Schlüssel: EEDAAC207FC6BA08727C

(3) Nur die Telefonnummern werden gehasht und mit Querverweisen versehen. Siilo berührt nicht die zugehörigen Namen, E-Mail-Adressen und andere Informationen, die das Adressbuch des Telefons enthält. Der Siilo-Server vergleicht dann die Liste der Hashes des Benutzers mit den bekannten Telefon-Hashes der aktuellen Siilo-Benutzer. Der Server vergleicht nur mit aktuellen Siilo-Nutzern und verwirft die übermittelten Hashes sofort, nachdem er die Übereinstimmungen an den mobilen Client zurückgegeben hat.