VEREINBARUNG ZUR AUFTRAGSDATENVERARBEITUNG (AV-V)

1. GEGENSTAND

Gegenstand vorliegender AV-V ist die Festlegung der Bedingungen für die Verarbeitung personenbezogener Daten, die Doctolib vom Abonnenten/Nutzer für die Ausführung der Services 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 Auftragsdatenverarbeitung zu Grunde gelegten Begriffsbestimmungen sind hier einsehbar.

3. DAUER

Vorliegende Vereinbarung gilt ab Abschluss des Hauptvertrags, dem sie zugehörig ist, und für die gesamte Dauer der Vertragsbeziehung zwischen Doctolib und dem Abonnenten/Nutzer.

4. STATUS DER VERTRAGSPARTEIEN

Die Parteien haben vereinbart, dass für die Verarbeitung der in Anhang 1 aufgeführten personenbezogenen Daten der Nutzer/Abonnent der Verantwortliche und Doctolib der Auftragsverarbeiter ist. Insbesondere betrifft dies personenbezogene Daten und Gesundheitsdaten im Zusammenhang mit der Behandlung von Patienten. Dies gilt unabhängig davon, ob diese Daten durch den Nutzer/Abonnenten oder einen von ihm benannten Administrator an Doctolib direkt oder indirekt übermittelt werden.

Doctolib wird vom Nutzer/Abonnenten dazu ermächtigt, die für die Lieferung der Services erforderlichen personenbezogenen Daten zu den nachstehend genannten Zwecken und unter strikter Einhaltung der nachstehend genannten Bedingungen zu verarbeiten.

Es wird darauf hingewiesen, dass die Verpflichtung von Doctolib auf die Einrichtung und Bereitstellung der Services und das Hosting der Doctolib-Plattform sowie des Patientenportals begrenzt sind. Auf ausdrückliche Anfrage des Nutzers/Abonnenten und unter seiner Kontrolle und Verantwortung kann Doctolib diesen jedoch bei dem Import der personenbezogenen Daten seiner Patienten innerhalb der Doctolib-Plattform unterstützen.

Sobald der Verantwortliche für die Datenverarbeitung persönliche Daten von Dritten auf der Doctolib-Plattform oder im Patientenportal eingibt (z.B. Daten von Patienten oder Kollegen) muss der Verantwortliche für die Datenverarbeitung die gesetzlichen Anforderungen bezüglich der Information oder Zustimmung dieser Dritten einhalten.

4.1. Pflichten des Nutzers/Abonnenten

Der Nutzer oder Abonnent 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.

Als für die Verarbeitung Verantwortlicher ist der Nutzer oder Abonnent allein verantwortlich für die Zuverlässigkeit und Richtigkeit der übermittelten persönlichen Daten. Dies gilt insbesondere auch im Zusammenhang mit medizinische Dokumenten, die über die Plattform verwaltet werden. Der Nutzer oder Abonnent verpflichtet sich dazu

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

- Nutzerrechte festzulegen, insbesondere im Hinblick auf Gesundheitsdaten von 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 Beauftragten für den Schutz personenbezogener Daten 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

4.2.1. Doctolib verpflichtet sich dazu:

- personenbezogene Daten in Übereinstimmung mit den in dieser Vereinbarung 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 Services 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 gesammelt oder zur Verfügung gestellt wurden, einzuhalten und die Daten zu löschen/anonymisieren, wenn diese Zwecke nicht mehr bestehen, vorbehaltlich gesetzlicher Verpflichtungen;

- einen Beauftragten für den Schutz personenbezogener Daten zu benennen.

4.2.2. Darüber hinaus verpflichtet sich Doctolib sicherzustellen, dass Personen, die gemäß dieser Vereinbarung 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 Services 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/Abonnent 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 schnellstmöglich und im Rahmen des Möglichen spätestens innerhalb von 72 Stunden, 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.

6. FÜHREN EINES VERARBEITUNGSVERZEICHNISSES

Doctolib führt 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 Services 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.

Um den für die Datenverarbeitung Verantwortlichen bei dieser Informationspflicht zu unterstützen, veröffentlicht Doctolib auf seiner Webseite Datenschutzhinweise, die unter https://www.doctolib.de/terms/agreement zugänglich sind.

8. VERWALTUNG DER RECHTE

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 im Bezug auf das Recht auf Zugang, Berichtigung, Löschung und Widerspruch, Einschränkung der Verarbeitung sowie Datenübertragbarkeit.

Doctolib kann auf Wunsch des Verantwortlichen diesen bei der Bearbeitung der Anträge unterstützen, darf jedoch Anträge der genannten betroffenen Personen nicht direkt beantworten, es sei denn, dass der für die Verarbeitung Verantwortliche eine ausdrückliche Weisung hierzu erteilt hat.

9. SICHERHEIT UND VERTRAULICHKEIT

9.1 Im Hinblick auf die Services 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/Abonnenten 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 Abonnenten / Nutzers zum Schutz von Patientendaten bleiben hiervon unberührt.

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

9.2 Berufsgeheimnis: Doctolib ist bekannt, dass die bei der Nutzung der Services 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 Herr seiner Daten, die von sich auf dem Patientenportal veröffentlicht wurden. Doctolib kann aus der Veröffentlichung keine Rechte an den Daten geltend machen, die von dem Verantwortlichen veröffentlicht wurden. Die anonymisierten Nutzungsstatistiken des Patientenportals sind Eigentum von Doctolib.

10. PERSONAL VON DOCTOLIB

Für die Erbringung der Services setzt Doctolib 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

Doctolib ist zur Beauftragung der hier aufgelisteten Unterauftragsverarbeiter berechtigt, wenn dies für die Erbringung der Services 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/Abonnenten für jegliche Nichterfüllung der Pflichten durch die Unterauftragsverarbeiter bei der Verarbeitung der personenbezogenen Nutzer-/Abonnentendaten 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 Services in Verbindung stehen.

Ziel des Audits ist in keinem Fall die Überwachung oder Zugriffsanfrage (i) auf nicht spezifische personenbezogene Daten des Nutzers/Abonnenten, 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 Services, Systemen, Netzwerken, Software oder Hardware in irgendeiner Weise behindern, modifizieren oder beeinflussen darf, die nicht für die ausschließliche Nutzung durch den Nutzer/Abonnenten 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 Penetrationstest im Doctolib-Netz sind gleich aus welchem Grund untersagt und von den Audits 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 Testumfang, Daten und Uhrzeiten der geplanten Tests, Testbedingungen. 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 für die Datenverarbeitung Verantwortliche muss Doctolib alle nützlichen Information im Hinblick auf die Intrusionstests und insbesondere (i) die Kontaktdaten des Auditors und der mit dem Audit beauftragten Personen; (ii) die für die Durchführung der Intrusionstest verwendeten IP-Adressen; und (iii) die für die Tests verwendeten Tools mitteilen.

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 kann innerhalb einer Frist von drei (3) Monaten ab Erhalt des Berichts festgestellte Versäumnisse oder Nichtkonformitäten korrigieren.

13. DATENRÜCKGEWINNUNG

Der Abonnent und der Nutzer können die Daten aus ihrer Patientendatenbank sowie den Verlauf ihrer Termine am Ende des Vertrags abrufen. Diese Daten werden dem Nutzer/Abonnenten in CVS- oder Excel-Format zur Verfügung gestellt. Der Exportantrag muss per E-Mail an folgende Adresse gestellt werden: pro@doctolib.com

Doctolib verpflichtet sich dazu, für den Nutzer/Abonnenten über die gesamte Vertragslaufzeit hinweg und während des gesamten Datenrückgewinnungsprozesses eine Kopie seiner Daten zu Verfügung zu halten. Im Fall einer Aussetzung des Nutzer-/Abonnentenzugangs zur Doctolib-Plattform, gleich aus welchem Grund, ermöglicht es Doctolib dem Nutzer über eine CVS- oder Excel-Datei die Rückgewinnung der letzten Kopie seiner Patientendatenbank sowie des Verlaufs seiner Termine zu erhalten.

14. WEITERGABE PERSONENBEZOGENER DATEN

Personenbezogene Daten dürfen nur zu den in dieser Vereinbarung 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/Abonnenten, dass persönliche Daten von Doctolib auch in Drittländer an seine Unterauftragsverarbeiter übertragen werden können, falls eine solche Übertragung für die Ausführung der bestellten Services 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 seiner Eigenschaft als Auftragsverarbeiter verpflichtet sich Doctolib dazu, die personenbezogenen Daten auf dem Gebiet der Europäischen Union zu hosten oder hosten zu lassen und, falls notwendig, alle in dieser Vereinbarung festgelegten Verpflichtungen auf den Dienstleister zu übertragen, der die personenbezogenen Daten hostet.

15. KONTAKT UND ZUSTÄNDIGE AUFSICHTSBEHÖRDEN

Bei Fragen zur der von Doctolib durchgeführten Verarbeitung personenbezogener Daten kann der Nutzer/Abonnent gemäß den vertraglichen Bestimmungen den Datenschutzbeauftragten von Doctolib unter untenstehend angegebener Adresse kontaktieren.

Datenschutzbeauftragte der Doctolib GmbH ist Frau Justine Bourdeu. Kontakt zu unserer Datenschutzbeauftragten können Sie über über datenschutz@doctolib.de aufnehmen.

Zuständige Datenschutzbehörde für die Doctolib GmbH ist die Berliner Beauftragte für Datenschutz und Informationsfreiheit, Friedrichstr. 219, 10969 Berlin.

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). Der Datenschutzbeauftragte der Doctolib SAS kann unter folgender Adresse kontaktiert werden: DOCTOLIB – DPO, 54 quai Charles Pasqua, 92300 Levallois-Perret oder contact.dataprivacy@doctolib.com.

16. ANWENDBARES RECHT

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

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 Abonnent, der ein Doctolib-Abonnement abgeschlossen hat oder Nutzer, der ein Doctolib-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.

Die Datenverarbeitungen ermöglichen insbesondere für die Betreuung von Patienten (i) die Terminplanung; (ii) die Verwaltung der Krankenakten; (iii) die Verwaltung und die Führung der erforderlichen Akten für die Weiterbehandlung des Patienten; (iv) die Durchführung von Videosprechstunden und sonstigen telemedizinischen Behandlungen; (v) die Kommunikation zwischen Gesundheitsfachkräften; (vi) die Erstellung und digitale Übersendung der Unterlagen (Behandlungsabrechnung, Krankschreibung, elektronisches Behandlungsprotokoll usw.).

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

Auftragsverarbeiter: Doctolib GmbH

Die Tätigkeiten des Auftragsverarbeiters umfassen die nachfolgend beschriebenen Services.

VERARBEITUNG NR. 1: VERWALTUNG DER ABONNENTEN- UND NUTZERKONTEN

VERARBEITUNGSVORGÄNGE:

Die Doctolib-Services umfassen die Erfassung, Speicherung, Organisation, Aufbewahrung, Extraktion, Einsichtnahme und Nutzung, Übertragung, Anonymisierung und die Löschung von untenstehend aufgelisteten personenbezogenen Daten.

DATENVERARBEITUNGSZWECKE:

- Kontenverwaltung: Bereitstellung von Nutzerkonten für die Nutzer, Abonnenten oder Administratoren (Einrichtung und Verwaltung dieser Konten), die Verwaltung der Identifizierung der Nutzer und die Sicherung des Zugangs zu den Nutzerkonten
- Technischer Support und Hilfe: Gewährleistung des technischen Supports, Anwendungsbetreuung und Bearbeitung von Nutzeranträgen, Beratung, Lagerung, Hosting und andere den Nutzern angebotene Services
- Support für personenbezogene Daten: Hilfe beim Umgang mit Datenverletzungen, Unterstützung bei der Beantwortung von Datenschutzanfragen und Anträgen auf Ausübung der Rechte der betroffenen Personen
- Rechnungslegung und Zahlungseinzug
- Marketingaktivitäten und Webanalysen, die nach der geltenden Rechtsprechung zulässig sind
- Übermittlung und Synchronisierung von Arztprofilen an öffentliche Stellen, Krankenkassen, Kooperationspartner und dort geführte Verzeichnisse
- Reporting, Debugging und Statistiken
- Sicherheit, Betrugsprävention
- Compliance mit gesetzlichen Vorgaben
- Verwaltung der Exporte des Inhalts von Terminkalendern und Terminen.

RECHTSGRUNDLAGE DER VERARBEITUNG:

Es obliegt dem für die Verarbeitung Verantwortlichen, die Rechtsgrundlage vor jeder einzelnen Verarbeitung sicherzustellen. Der Verantwortliche sichert Doctolib zu, das Vorliegen der angegebenen Rechtsgrundlage (z.B. das Vorliegen von Einwilligungen) geprüft zu haben.

BETROFFENE PERSONEN:

Diess können der Abonnent, Nutzer oder Fachangestellte wie vertraglich festgelegt sein.

ARTEN DER PERSONENBEZOGENEN DATEN:

Um die Menge der verarbeiteten personenbezogenen Daten so gering wie möglich zu halten, muss der Verantwortliche sicherstellen, dass er nur Daten sammelt und verwendet, die für die Erreichung des jeweiligen Verarbeitungszwecks, insbesondere für die medizinische und administrative Verwaltung seines Patientenstammes erforderlich und notwendig sind.

Folgende Daten werden grundsätzlich für oben genannte Zwecke als erforderlich erachtet:

a) **Identität und Kontaktdaten der Gesundheitsfachkräfte:** Geschlecht, Nachname, Vorname, Telefonnummer und E-Mail, Postanschrift, Foto, Unterschrift, Personalausweis.
b) **Berufsbezogene Daten:** Fotografie, Spezialisierung, Angaben zur Behandlung, Werdegang der Gesundheitsfachkraft, angebotene Besuchsgründe, Sprechzeiten, Besonderheiten in Verbindung mit dem Behandlungsort, Nachweise über berufliche Qualifikationen.
d) **Anbindung von Hard- und Software der Gesundheitseinrichtung**: Nutzungs- und Verbindungslogs, welche die "Aktivität" der vom Nutzer verwendeten Software- und Hardwarekomponenten abbilden (Konnektoren / Kartenlesegeräte / Verwaltungssoftware), die über die "beruflichen Aktivitäten" der Nutzer innerhalb der Doctolib-Services Auskunft geben.

Ausgenommen einer besonderen Weisung durch den für die Verarbeitung Verantwortlichen verarbeitet Doctolib alle oben genannten personenbezogenen Daten, um die Services, die Gegenstand des Vertrags sind, zu erbringen.

EMPFÄNGER UND UNTERAUFTRAGSVERARBEITER:

Siehe hierzu die in Artikel 14 der vorliegenden Vereinbarung angeführte Liste.

AUFBEWAHRUNGSDAUER:

Der für die Verarbeitung Verantwortliche muss eine genaue Aufbewahrungsdauer der Daten festlegen und Doctolib mitteilen. In Ermangelung dieser Weisung durch den für die Verarbeitung Verantwortlichen wendet Doctolib die von den Aufsichtsbehörden und der geltenden Gesetzgebung empfohlenen Aufbewahrungsfristen an.

VERARBEITUNG NR. 2: TERMIN- UND KALENDERVERWALTUNG

VERARBEITUNGSVORGANG:

Die Doctolib-Services umfassen die Erfassung, Speicherung, Organisation, Aufbewahrung, Extraktion, Einsichtnahme und Nutzung, Übertragung, Anonymisierung und die Löschung von untenstehend aufgelisteten personenbezogenen Daten.

DATENVERARBEITUNGSZWECKE:

- Unterstützung bei der Verwaltung des Imports des Inhalts von Kalendern und Terminen und - soweit erforderlich - der Patientendatenbanken der Akteure des Gesundheitswesens auf der Doctolib-Plattform
- Einhaltung der Vorschriften für eine sichere Patientenidentifikation
- Unterstützung bei der Wiederherstellung von Daten, die an Kalender angehängt sind;
- Ermöglichung der Verwaltung des Terminkalenders durch den Verantwortlichen
- Ermöglichung der Verwaltung des Behandlungsverlaufs der Patienten und ggf. deren Angehöriger durch den Verantwortlichen
- Sicherstellung von Praxisabläufen und Sicherheit im Falle von Pandemien oder sonstigen Notständen im Gesundheitswesen
- Ermöglichung der Online-Terminvereinbarung durch die Patienten selbst und deren Angehörige
- Ermöglichung der Verwaltung von Sprechstunden vor Ort oder von Videosprechstunden
- Ermöglichung der Kommunikation zwischen Akteuren des Gesundheitswesens und dem Patienten sowie Weitergabe von Informationen an die Patienten und deren Angehörige bezüglich des Nutzerprofils und ihrem Behandlungsverlauf.
- Ermöglichung der Zusendung von Unterlagen an die Patienten und deren Angehörige durch den Verantwortlichen
- Senden von E-Mails und SMS betreffend der Termindurchführung

RECHTSGRUNDLAGE DER VERARBEITUNG:

Es obliegt dem für die Verarbeitung Verantwortlichen, diese Rechtsgrundlage vor jeder einzelnen Verarbeitung sicherzustellen und zu benennen. Der Verantwortliche sichert Doctolib zu, das Vorliegen der angegebenen Rechtsgrundlage (z.B, das Vorliegen von Einwilligungen) geprüft zu haben.

BETROFFENE PERSONEN:

Patienten und deren Angehörige

ARTEN DER PERSONENBEZOGENEN DATEN:

Um die Menge der verarbeiteten personenbezogenen Daten so gering wie möglich zu halten, muss der für die Verarbeitung Verantwortliche sicherstellen, dass er nur Daten sammelt und verwendet, die für die Erreichung des jeweiligen Verarbeitungszweckesund für die medizinische und administrative Verwaltung seines Patientenstammes erforderlich sind.

Folgende Daten werden grundsätzlich für oben genannte Zwecke als erforderlich erachtet:
a) **Identität und Kontaktdaten des Patienten oder eines Angehörigen:** Geschlecht, Name, Vorname, Geburtsdatum, Geburtsort, Anschrift , E-Mail-Adresse und Telefonnummer
b) **Beruf des Patienten oder des Angehörigen**
c) **Gesundheit**: Versicherungsart, Name und Anschrift des Hausarztes, Name und Anschrift des überweisenden Arztes, Datum/Uhrzeit und Ort des Termins, Spezialisierung des Arztes und Grund der Sprechstunde, Art des Termins, medizinische Unterlagen des Patienten, ergänzende Anmerkungen durch die Gesundheitsfachkraft.
d) **Anbindung von Hard- und Software der Gesundheitseinrichtung**: Nutzungs- und Verbindungslogs, welche die "Aktivität" der vom Nutzer verwendeten Software- und Hardwarekomponenten abbilden (Konnektoren / Kartenlesegeräte / Verwaltungssoftware) die über die "beruflichen Aktivitäten" der Nutzer innerhalb der Doctolib-Services Auskunft geben.
Ausgenommen einer besonderen Weisung durch den für die Verarbeitung Verantwortlichen verarbeitet Doctolib alle oben genannten personenbezogenen Daten, um die Services, die Gegenstand des Vertrages sind, zu erbringen.

EMPFÄNGER UND UNTERAUFTRAGSVERARBEITER:

Siehe die in Artikel 14 der vorliegenden Vereinbarung angeführte Liste.

AUFBEWAHRUNGSDAUER:

Der für die Verarbeitung Verantwortliche muss eine genaue Aufbewahrungsdauer der Daten festlegen und Doctolib mitteilen. Standardmäßig und sofern vom Verantwortlichen nicht anders angewiesen, wird die Aufbewahrungsdauer auf 5 Jahre festgelegt.
Für Verwaltungszwecke der Gesundheitseinrichtung und der medizinischen oder paramedizinischen Praxis können die in der Doctolib-Plattform aufgezeichneten Daten für einen Zeitraum von 10 Jahren ab dem Datum der letzten Behandlung des Patienten aufbewahrt werden.

VERARBEITUNG NR. 3: TELEKONSULTATIONSSERVICE

VERARBEITUNGSVORGANG:

Die Doctolib-Services umfassen die Erfassung, Speicherung, Organisation, Aufbewahrung, Extraktion, Einsichtnahme und Nutzung, Übertragung, Anonymisierung und die Löschung von untenstehend aufgelisteten personenbezogenen Daten.

DATENVERARBEITUNGSZWECKE:

- Ermöglichung der Nutzung einer Videosprechstunde mit Videoübertragung
- Ermöglichung der Übertragung von Dokumenten an die Patienten über das Profil der Gesundheitsfachkraft (Rezept, medizinischer Bericht, Honorarabrechnung …) und der Erhalt derselben für die Weiterbehandlung des Patienten
- Ermöglichung der Kommunikation zwischen der Gesundheitsfachkraft und dem Patienten per Video-Chat.

- Ermöglichung der Rechnungsstellung und Übernahme der Gesundheitskosten
- Berichterstellung, Debugging und Statistik.
- Kommunikation per E-Mail und / oder SMS über das Anbieten einer Videosprechstunde.

RECHTSGRUNDLAGE DER VERARBEITUNG:

Es obliegt dem für die Verarbeitung Verantwortlichen, diese Rechtsgrundlage vor jeder Verarbeitung sicherzustellen und zu benennen. Der Verantwortliche sichert Doctolib zu, das Vorliegen der angegebenen Rechtsgrundlage (z.B, das Vorliegen von Einwilligungen) geprüft zu haben.

BETROFFENE PERSONEN:

Patienten und deren Angehörige.

ARTEN DER PERSONENBEZOGENEN DATEN:

Um die Menge der verarbeiteten personenbezogenen Daten so gering wie möglich zu halten, muss der für die Verarbeitung Verantwortliche sicherstellen, dass er nur Daten sammelt und verwendet, die zur Erfüllung der jeweiligen Verarbeitungszwecke , insbesondere für die medizinische und administrative Verwaltung seines Patientenstammes erforderlich sind.

Folgende Daten werden grundsätzlich für oben genannte Zwecke als relevant erachtet:
a) **Identität des Patienten oder des Angehörigen**: Geschlecht, Name, Vorname
b) **Der Videostream** ermöglicht die Videoübertragung zwischen dem Patienten und der Gesundheitsfachkraft bei der Telekonsultation
c) Information zur Videosprechstunde: Fehler & Bugs, Start- und Endzeit der Videosprechstunde, Video- und Audiobitrate, Information zu der für die Videosprechstunde eingesetzten Ausrüstungen (Batteriestand, Kamera- und Mikrofonzugang), Beurteilung der Telekonsultation
d) **Gesundheit:** Medizinische Unterlagen des Patienten, Aufzeichnungen durch die Gesundheitsfachkraft, die Sozialversicherungsnummer (für die Rechnungsstellung und Rückerstattung der Behandlungskosten)
e) **Anbindung von Hard- und Software der Gesundheitseinrichtung**: Nutzungs- und Verbindungslogs, welche die "Aktivität" der vom Nutzer verwendeten Software- und Hardwarekomponenten abbilden (Konnektoren / Kartenlesegeräte / Verwaltungssoftware) , die über die "beruflichen Aktivitäten" der Nutzer innerhalb der Doctolib-Services Auskunft geben.

Ausgenommen einer besonderen Weisung durch den für die Verarbeitung Verantwortlichen verarbeitet Doctolib alle oben genannten personenbezogenen Daten, um die Services, die Gegenstand des Vertrags sind, zu erbringen.

EMPFÄNGER UND UNTERAUFTRAGSVERARBEITER:

Siehe die in Artikel 14 der vorliegenden Vereinbarung angeführte Liste.

AUFBEWAHRUNGSDAUER:

Der für die Verarbeitung Verantwortliche muss eine genaue Aufbewahrungsdauer der Daten festlegen und Doctolib mitteilen.

Für Verwaltungszwecke der Gesundheitseinrichtung und der medizinischen oder paramedizinischen Praxis können die in der Doctolib-Plattform aufgezeichneten Daten für einen Zeitraum von höchstens zwanzig Jahren ab dem Datum der letzten Behandlung des Patienten aufbewahrt werden.

VERARBEITUNG NR. 4: MESSAGING-DIENST (BETA TEST)

VERARBEITUNGSVORGANG:

Doctolib-Services umfassen die Erfassung, Aufzeichnung, Organisation, Aufbewahrung, Extraktion von Daten im Zusammenhang eines Messaging-Dienstes durch Übermittlung, Anonymisierung und Löschung der nachstehend aufgeführten personenbezogenen Daten.

DATENVERARBEITUNGSZWECKE:

- Erleichterung der Kommunikation zwischen Gesundheitsfachkräften durch Bereitstellung eines sicheren Kommunikationskanals durch Instant Messaging
- Austausch von Dokumenten und Daten im Zusammenhang mit medizinischen Behandlungen
- Berichterstellung, Debugging und Statistik

ARTEN DER PERSONENBEZOGENEN DATEN:

- Identifikationsdaten
- Kontaktdetails
- Medizinische Historie
- Daten im Zusammenhang mit Behandlungen und Verschreibungen
- Biometrische und biologische Daten
- Daten zum Behandlungsteam
- Medizinische Bilder
- Die Nutzungs- und Verbindungsprotokolle sowie technische Protokolle

RECHTSGRUNDLAGE DER VERARBEITUNG:

Es obliegt dem für die Verarbeitung Verantwortlichen, diese Rechtsgrundlage vor jeder Verarbeitung sicherzustellen und zu benennen. Der Verantwortliche sichert Doctolib zu, das Vorliegen der angegebenen Rechtsgrundlage (z.B. das Vorliegen von Einwilligungen) geprüft zu haben.

BETROFFENE PERSONEN:

- Patienten, die zur Patientendatenbank des Nutzers gehören
- Gesundheitsfachkräfte

EMPFÄNGER UND UNTERAUFTRAGSVERARBEITER:

- Gesundheitsakteure mit einem Nutzerkonto
- Eingeladene Gesundheitsfachkräfte

AUFBEWAHRUNGSDAUER:

Der Konversationsverlauf, einschließlich der Dokumente, wird bis zum Löschen durch den Benutzer oder bis zur Beendigung des Dienstes aufbewahrt. Standardmäßig und sofern vom Verantwortlichen nicht anders angewiesen, wird die Aufbewahrungsdauer auf 6 Monate festgelegt.

VERARBEITUNG NR. 5: DOKUMENTENVERWALTUNG

VERARBEITUNGSVORGANG:

Die Doctolib-Services umfassen das Erstellen, Konvertieren, Signieren und Speichern von Dokumenten, insbesondere medizinischen Dokumenten im Rahmen der Behandlung des Patienten.

DATENVERARBEITUNGSZWECKE:

- Ermöglichung des Teilen von Dokumenten, vor, während und nach einer Behandlung durch den Patienten an die Gesundheitsfachkraft.
- Ermöglichung des Teilen von Dokumenten, vor, während und nach einer Behandlung durch die Gesundheitsfachkraft an den Patienten.
- Elektronisches Ausstellen von Dokumenten durch die Gesundheitsfachkraft, einschließlich des elektronischen Signierens des Dokumentes
- Konvertieren und Speichern elektronischer Dokumente im PDF Format.

RECHTSGRUNDLAGE DER VERARBEITUNG:

Es obliegt dem für die Verarbeitung Verantwortlichen, diese Rechtsgrundlage vor jeder Verarbeitung sicherzustellen und zu benennen. Der Verantwortliche sichert Doctolib zu, das Vorliegen der angegebenen Rechtsgrundlage (z.B. das Vorliegen von Einwilligungen) geprüft zu haben.

BETROFFENE PERSONEN:

Patienten und deren Angehörige.

ARTEN DER PERSONENBEZOGENEN DATEN:

Um die Menge der verarbeiteten personenbezogenen Daten so gering wie möglich zu halten, muss der für die Verarbeitung Verantwortliche sicherstellen, dass er nur Daten sammelt und verwendet, die zur Erfüllung der jeweiligen Verarbeitungszwecke , insbesondere für die medizinische und administrative Verwaltung seines Patientenstammes erforderlich sind.

Folgende Daten werden grundsätzlich für oben genannte Zwecke als relevant erachtet:
a) **Identität des Patienten oder des Angehörigen**: Geschlecht, Name, Vorname
b) **Gesundheit:** Medizinische Unterlagen des Patienten, Aufzeichnungen durch die Gesundheitsfachkraft, die Sozialversicherungsnummer (für die Rechnungsstellung und Rückerstattung der Behandlungskosten)
e) **Anbindung von Hard- und Software der Gesundheitseinrichtung**: Nutzungs- und Verbindungslogs, welche die "Aktivität" der vom Nutzer verwendeten Software- und Hardwarekomponenten abbilden (Konnektoren / Kartenlesegeräte / Verwaltungssoftware) , die über die "beruflichen Aktivitäten" der Nutzer innerhalb der Doctolib-Services Auskunft geben.

Ausgenommen einer besonderen Weisung durch den für die Verarbeitung Verantwortlichen verarbeitet Doctolib alle oben genannten personenbezogenen Daten, um die Services, die Gegenstand des Vertrages sind, zu erbringen.

EMPFÄNGER UND UNTERAUFTRAGSVERARBEITER:

Gesundheitsfachkräfte und Patienten, die sich gegenseitig über die Plattformen elektronische Dokumente teilen.

Zu den Unterauftragsverarbeitern siehe die in Artikel 14 der vorliegenden Vereinbarung angeführte Liste.

AUFBEWAHRUNGSDAUER:

Geteilte Dokumente können vom Patienten gelöscht werden oder eine Löschung kann verlangt werden.
Im Übrigen muss der für die Verarbeitung Verantwortliche eine genaue Aufbewahrungsdauer der Daten festlegen und Doctolib mitteilen.
Für Verwaltungszwecke der Gesundheitseinrichtung und der medizinischen oder paramedizinischen Praxis können die in der Doctolib-Plattform aufgezeichneten Daten für einen Zeitraum von höchstens zwanzig Jahren ab dem Datum der letzten Behandlung des Patienten aufbewahrt werden.

ANHANG 2: TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN

PRODUKTSICHERHEIT

- **Zweistufige Prüfung (2FA)**: Bei jeder Verbindung mit einer neuen Hardware muss der Nutzer sein Passwort und einen einmalig vergebenen, an den Nutzer per SMS übermittelten Identifizierungscode eingeben.

  Gewährleistung des Schwierigkeitsgrades der Passwörter: mit mindestens 8 Zeichen, darunter Zahlen, Symbole, Buchstaben und Großbuchstaben, zu einfache klassische Passwörter sind unzulässig (beispielsweise Login, Name, einfache Zahlenfolge)

  Schutz der Nutzersitzung: Offene Sitzungen können ungültig werden. Die Sitzung läuft automatisch nach einstündiger Inaktivität aus.
  Vereinfachte Entsperrung per PIN-Code.

- **Gesicherter Wiederherstellungsprozess:** Überprüfungen der Kontoinformationen vor Zulassung der Wiederherstellung.

- **Granulare Zugriffskontrolle**: die Administratoren können jedem Nutzer innerhalb ihrer Organisation spezifische Rechte zuweisen.

- **Rückverfolgbarkeit der Aktionen**: Die Aktionen der verschiedenen Nutzer einer Organisation sind hinterlegt und protokolliert.

- **Schutz vor Kontendiebstahl**: Erfolgreiche Versuche, sich von einem neuen Endgerät aus mit einem Passwort anzumelden, werden dem Nutzer über die 2FA mitgeteilt.

SICHERHEIT DER PLATTFORM - MAßNAHMEN NACH Art. 32 (1) lit. b DSGVO

- **Automatische Sicherheitsupdates:** Sicherheitspatches werden qualifiziert und automatisch auf unsere Komponenten angewendet.

- **Aktualisierte und verbesserte Betriebssysteme.**

- **Standby-Sicherheitsüberwachung:** Wir überwachen permanent Bedrohungen, Schwachstellen oder Angriffsziele, gleich ob diese bekannt oder neu sind.
  Firewall und spezifische Filtriersysteme zur Regulierung des Zugangs (Proxy, VPN ...).
  Schutz vor Denial-Of-Service Angriffen (DDoS).
  Schutz vor Software-Angriffen (WAF).

- **Rückverfolgbarkeit:** Wir speichern alle Aktionen und überwachen und alarmieren bei jedem Sicherheitsvorfall.

- **Gesicherte Datenzentren**: HDS, ISO 27001, Tier 3, hohe physische Sicherheit, Personal vor Ort 24 Stunden am Tag, 7 Tage die Woche.

VERFÜGBARKEIT - MAßNAHMEN NACH Art. 32 (1) lit. b, c DSGVO

- Alle Daten werden in mehreren Rechenzentren repliziert.
- Jedes Datenzentrum verfügt über mehrere Netzwerkverbindungen nach außen.
- Alle Dienste und Komponenten werden durch Disaster-Recovery-Verfahren, meist automatisch, abgedeckt.
- Jede Störung wird automatisch erkannt und löst einen Alarm aus aufgrund eines umfassenden Überwachungssystems für jede technische Komponente und jeden Geschäftsdienst.
- Einrichtung einer Datensicherungs- und Wiederherstellungspolitik.

DATENVERSCHLÜSSELUNG - MAßNAHMEN NACH Art. 32 (1) lit. a DSGVO

Verschlüsselung der Kommunikation:

- Alle Daten, die mit und zwischen Systemen ausgetauscht werden, werden mit TLS-Protokollen verschlüsselt.
- Der technische Zugriff erfolgt über eine verschlüsselte und stark authentifizierte Verbindung mit systematischer Validierung durch einen Peer.
- Die Vertraulichkeit der Videosprechstunden, die über den Doctolib-Dienst durchgeführt werden, wird durch die Verschlüsselung der End-to-End-Ströme von Patienten/Gesundheitsdienstleistern gewährleistet.

Pseudonymisierung - MAßNAHMEN NACH Art. 32 (1) lit a DSGVO

- Sicherer Datentransfer zwischen Gesundheitseinrichtungen und Doctolib-Rechenzentren durch Pseudonymisierung.
- Pseudonymisierung von Datenkategorien von Patienten wie Name, Geburtsdatum, Telefonnummer. Definierte Regel der Pseudonymisierung (z.B. für Namen X--------Y-----).
- Autorisiertes Doctolib-Personal mit nur pseudonymisierter Sicht auf die personenbezogenen Daten der Patienten.

Datenspeicherung - MAßNAHMEN NACH Art. 32 (1) lit. a DSGVO

- Alle unsere Datenbanken sind im Ruhezustand verschlüsselt.
- Die Verschlüsselungsschlüssel werden mit einem Hauptschlüssel verschlüsselt, der von einem europäischen Marktführer im Bereich des Schutzes kryptographischer Geheimnisse erstellt wurde.
- Sensiblere Daten unterliegen einer zusätzlichen Verschlüsselungsebene durch den Doctolib-Server. Die Verschlüsselungsschlüssel werden ebenfalls durch den geschützten Hauptschlüssel verschlüsselt.
- Die sensibelsten Daten werden von der Doctolib-Anwendung durchgehend verschlüsselt, wobei die Schlüssel nur auf der Hardware des Nutzers gespeichert werden. Diese Daten können nur für den Nutzer sichtbar sein. Doctolib ist immer für die Datenspeicherung und -verfügbarkeit zuständig, kann aber keine Gesundheitsinformationen lesen. Kein Akteur und Vermittler des Informationssystems kann diese Daten lesen.

ZUGANGSKONTROLLE DER ANGESTELLTEN - MAßNAHMEN NACH Art. 32 (1) lit. b DSGVO

- Alle Zugriffe werden bewilligt, widerrufen, geprüft und überwacht und unterliegen einem streng zentralisierten und aktualisierten Verfahren.
- Das Doctolib-Personal hat keinen Zugang zu medizinischen Daten.
- Wenn erforderlich und im Fall einer Untersuchung kann einem Mitglied des Support-Teams ein vorübergehender Zugang zu den Daten nur vom Nutzer selbst gewährt werden.
- Im Fall eines Fehlers im Zusammenhang mit der Datenspeicherung können nur wenige Mitarbeiter von Doctolib gegebenenfalls auf die Daten zugreifen.

BEWÄHRTE PRAKTIKEN ZUR ANWENDUNGSSICHERHEIT - MAßNAHMEN NACH Art. 32 (1) lit. b DSGVO

Passwortspeicherung: gestreut mittels einer soliden Hashfunktion (bcrypt).
Ratenbeschränkung: Die Services und Nutzer werden durch einen intelligenten Algorithmus, der das Teilen und den Zugang zu den Services kontrolliert und automatische Anfragen blockiert gegen Denial-Of-Service und Brute-Force Angriffe sowie gegen die automatische Wiederherstellung der Daten geschützt.

GESICHERTER SOFTWAREENTWICKLUNGSZYKLUS (S-SDLC) - MAßNAHMEN NACH Art. 32 (1) lit. b DSGVO

Sicherheitsschulung und -sensibilisierung: Die Entwickler werden im Hinblick auf die Best Practices für sichere Anwendungsentwicklung geschult und sensibilisiert.
Sicherheit von der Entwurfsphase an: Jede neue Funktion im Doctolib-Produkt wird in Zusammenarbeit mit Sicherheitsexperten entworfen.

Überprüfung des Quellcodes:

Der Doctolib-Quellcode wird bei jeder Änderung automatisch analysiert.
Manuelle Überprüfungen des Quellcodes werden durchgeführt, wenn eine sensible Komponente geändert wird.

Suche nach Schwachstellen (Maßnahmen nach Art. 32 (1) lit d DSGVO):

- Durchdringungstests:
  Doctolib beauftragt regelmäßig anerkannte Unternehmen für Durchdringungstests in seinen Anwendungen und Plattformen.
- Prämienprogramme für Schwachstellenentdeckung (Bug Bounty):
  Angestellte und externe Fachkräfte werden intensiviert, Sicherheitslücken im Doctolib-Produkt zu identifizieren.

PHYSISCHER ZUGANG DURCH MITARBEITER VON DOCTOLIB UND BESUCHER - MAßNAHMEN NACH Art. 32 (1) lit. b DSGVO

Die Büros von Doctolib sind alarmgesichert und mit den modernsten Sicherheits- und Zugangskontrollsystemen ausgestattet.
Jeder autorisierte Zugang zu den Räumlichkeiten kann vorübergehend aufgezeichnet werden.
Besucher können die Räumlichkeiten nur nach Registrierung betreten und werden von einem Doctolib-Mitarbeiter begleitet. Während der Besuche werden Dritte niemals unbeaufsichtigt oder allein gelassen.

Alle Systeme werden in zugelassenen Datenzentren betrieben. Diese verfügen über Videoüberwachung, Sicherheitssysteme und einen Sicherheitsdienst. Nur eine kleine Gruppe von speziell geschulten Doctolib-Spezialisten hat eine Zugangsberechtigung. Jeder ihrer Zugänge kann vorübergehend aufgezeichnet werden.
Sofern Mitarbeiter der Gesundheitseinrichtung zu Besuch in den Büros von Doctolib sind, sind diese auf die vorbezeichneten Maßnahmen hinzuweisen.

Verbindung mit dem Informationssystem (IS) der Gesundheitseinrichtung:
Die Verbindung mit dem Informationssystem der Gesundheitseinrichtung kann auf verschiedene Arten erfolgen.
API-Verbinder zwischen dem Doctolib-Kalender und dem Kalender des lokalen IS-Verbinders, der Doctolib Kalender ermöglicht das Abrufen des Patientendatenblattes des IS VPN IPSec zwischen dem Server und Doctolib (um die Verfügbarkeit zu bestätigen).