AUFTRAGSVERARBEITUNGSVERTRAG (AVV)

ALLGEMEINE BEDINGUNGEN

EINLEITUNG

Dieser Abschnitt stellt dar, welche Bedingungen für den Auftragsverarbeitungsvertrag (im Folgenden "AVV" genannt) je nach den von Ihnen abonnierten und genutzten Doctolib-Diensten gelten, wie dieser AVV zu lesen und zu verstehen ist sowie die Bedingungen, unter denen dieser AVV geändert werden kann und welche Version verbindlich ist.

1. GEGENSTAND

Zweck dieses AVV ist es, die Bedingungen festzulegen, unter denen Doctolib sich verpflichtet, die von Ihnen als Abonnent/Nutzer (im Folgenden "Sie") zur Verfügung gestellten personenbezogenen Daten für die Erbringung der abonnierten bzw. von Ihnen genutzten Dienste zu verarbeiten.

Im Rahmen der Vertragsbeziehungen verpflichten Sie und Doctolib (im Folgenden benannt als “Parteien”) sich 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 (im Folgenden “DSGVO”) sowie der Bestimmungen des Bundesdatenschutzgesetzes (“BDSG”).

Die nachstehenden Allgemeinen Bedingungen gelten für alle Doctolib-Dienste, während die Besonderen Bedingungen nur insoweit Anwendung finden, als der betroffene Doctolib-Dienst von Ihnen genutzt wird. Wenn Sie also einen Teil der Dienste nicht abonnieren und/oder nutzen, wird Doctolib die personenbezogenen Daten im Zusammenhang mit den jeweiligen Besonderen Bedingungen nicht verarbeiten.

Abhängig von den von Ihnen abonnierten oder genutzten Diensten gelten die folgenden Besonderen Bedingungen, welche bestimmte Einzelheiten in Bezug auf die Verarbeitung personenbezogener Daten und Gesundheitsdaten gemäß Art. 28 Abs. 3 DSGVO enthalten:

Besondere Bedingungen für Doctolib-Dienste:

- die Besonderen Bedingungen für die Verarbeitung “Konfigurierung von Abonnenten- und Nutzerkonten”
- die Besonderen Bedingungen für die Verarbeitung “Termin- und Kalender-Dienst”,
- die Besonderen Bedingungen für die Verarbeitung “Videosprechstunden-Dienst”,
- die Besonderen Bedingungen für die Verarbeitung “Patientennachrichten-Dienst”,
- die Besonderen Bedingungen für die Verarbeitung “Intelligenter Aufgaben-Manager”,
- die Besonderen Bedingungen für die Verarbeitung “Verwaltung von Dokumenten und Formularen”,
- die Besonderen Bedingungen für die Verarbeitung “Aufnahmemanagement-Dienst“,
- die Besonderen Bedingungen für die Verarbeitung “KI-Telefonassistent”,
- die Besonderen Bedingungen für die Verarbeitung “KI-Sprechstundenassistent”
- die Besonderen Bedingungen für die Verarbeitung “Behandlungs- und Abrechnungsmanagement”.
- die Besonderen Bedingungen für die Verarbeitung “ Messaging-Dienst”,
- die Besonderen Bedingungen für die Verarbeitung “Bereitstellung eines Privaten Organisations-Netzwerks”

Im Falle eines Widerspruchs zwischen den Besonderen Bedingungen und den Allgemeinen Bedingungen haben die Besonderen Bedingungen Vorrang.

Zusätzlich zu den Allgemeinen und Besonderen Bedingungen für die Verarbeitung gelten je nach den von Ihnen abonnierten oder genutzten Diensten die folgenden technischen und organisatorischen Maßnahmen:

- die allgemeinen technischen und organisatorischen Maßnahmen, die generell gelten;

- die spezifischen technischen und organisatorischen Maßnahmen, die nur dann gelten, wenn ein Konnektor eingerichtet wurde, um die Interoperabilität zwischen der Plattform und den Informationssystemen Dritter zu gewährleisten;
- die spezifischen technischen und organisatorischen Maßnahmen, die von Doctolib im Zusammenhang mit den Verarbeitungen des Messaging-Dienstes und der Bereitstellung des privaten Organisations-Netzwerks angewendet werden.

Der AVV enthält auch eine Liste der Unterauftragsverarbeiter von Doctolib, die für die Erbringung der Doctolib-Dienste eingesetzt werden.

2. BEGRIFFSBESTIMMUNGEN

Die dem AVV zugrunde gelegten Begriffsbestimmungen sind hier einsehbar.

3. INKRAFTTRETEN UND DAUER

Der vorliegende AVV gilt mit Abschluss des Hauptvertrages über das Doctolib-Abonnement und für die gesamte Dauer der Vertragsbeziehung zwischen Doctolib und Ihnen.

4. STATUS DER VERTRAGSPARTEIEN

Die Parteien haben die folgenden Definitionsbestimmungen und Pflichten vereinbart:

VERANTWORTLICHER: Sie, als Nutzer/Abonnent.

AUFTRAGSVERARBEITER: Doctolib ist der **Auftragsverarbeiter** in Bezug auf die Verarbeitung der personenbezogenen Daten und der Gesundheitsdaten, die in den oben genannten Besonderen Bedingungen für die Verarbeitung genannt werden, je nach den von Ihnen abonnierten oder genutzten Doctolib-Diensten, unabhängig davon, ob sie Doctolib direkt oder indirekt von Ihnen oder von einem Administrator, dem Sie Zugang zu den Doctolib-Diensten gewährt haben, zur Verfügung gestellt werden.

Sie beauftragen Doctolib dazu, in Ihrem Namen die im Rahmen der für die abonnierten Dienste notwendigen e personenbezogenen Daten und Gesundheitsdaten 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 Doctolib-Dienste, das Hosting der Doctolib-Plattform sowie des Patientenportals begrenzt sind. Auf Ihre ausdrückliche Anfrage und unter Ihrer Kontrolle und Verantwortung kann Doctolib Sie jedoch beim Import der Patientenstammdaten in die Doctolib-Plattform unterstützen.

Sobald Sie, als Verantwortlicher der Verarbeitung, personenbezogene Daten oder Gesundheitsdaten von Dritten in die Doctolib-Plattform oder im Patientenportal eingeben (z.B. Daten von Patienten oder Kollegen) müssen Sie die jeweiligen gesetzlichen Anforderungen bezüglich der Information und/oder Einwilligung dieser Dritten einhalten.

4.1. Ihre Pflichten als Nutzer/Abonnent in Ihrer Eigenschaft als Verantwortlicher der Verarbeitung

In Ihrer Eigenschaft als **Verantwortlicher der Verarbeitung** sind Sie allein für die Führung eines Verzeichnisses von Verarbeitungstätigkeiten und gegebenenfalls für die Erfüllung von Anforderungen der für Sie zuständigen Datenschutzaufsichtsbehörde verantwortlich. Sie sind auch dafür verantwortlich, die betroffenen Personen und insbesondere Kollegen und Patienten über die Aufnahme ihrer personenbezogenen Daten und Gesundheitsdaten in die Doctolib-Plattform sowie über die Möglichkeiten der Ausübung ihrer Rechte zu informieren, z.B. durch die Zurverfügungstellung eines Informationsblattes.

Als Verantwortlicher der Verarbeitung sind Sie allein verantwortlich für die Zuverlässigkeit, Richtigkeit und Relevanz der übermittelten personenbezogenen Daten und Gesundheitsdaten. Sie sind insbesondere verantwortlich für die Nutzung der Doctolib-Plattform und der Doctolib-Dienste sowie für die Dokumente und nutzergenerierten Inhalte, die Sie

ablegen, speichern, ansehen und aus dem Speicherplatz nehmen. Es liegt in Ihrer Verantwortung, alle notwendigen Erklärungen abzugeben, um die Konfirmität und Rechtmäßigkeit der Verarbeitungstätigkeiten sicherzustellen. Sie verpflichten sich, Doctolib, seine Vertreter, seine Angestellten und seine Unterauftragsverarbeiter zu entschädigen und von jeglicher Haftung für alle Ansprüche, Verbindlichkeiten, Schäden und Kosten (einschließlich Rechtskosten, Gebühren und Auslagen) freizustellen, die Doctolib, seinen Vertretern, Angestellten und Unterauftragsverarbeiter aufgrund der Nichteinhaltung dieser Verpflichtung auferlegt werden oder entstehen.

Die vorgenommenen Verarbeitungen müssen einem bestimmten Ziel dienen und im Hinblick auf die Aufgaben und Tätigkeiten der Gesundheitsfachkräfte gerechtfertigt sein.

Ihre Tätigkeit umfasst Verarbeitungen, welche Prävention, Gesundheitsfürsorge für den Patienten sowie die administrative Verwaltung Ihrer Gesundheitseinrichtung, Ihres Gesundheitszentrums oder Ihrer Privatpraxis ermöglichen.

Sie verpflichten sich dazu:

- die ärztliche Schweigepflicht einzuhalten und für deren Einhaltung Sorge zu tragen;
- eine interne Regelung der Autorisierung sowie der Verwaltung von Zugriffsrechten einzuführen, um die Vertraulichkeit der personenbezogenen Daten und der Gesundheitsdaten in Übereinstimmung mit den Wünschen der Patienten und ihrer Angehörigen zu gewährleisten;
- Doctolib alle erforderlichen Daten für die Auftragsverarbeitung zur Verfügung zu stellen, darunter die Liste der zu verarbeitenden personenbezogenen Daten und Gesundheitsdaten, die Rechtsgrundlage der Verarbeitung, die Verarbeitungszwecke und die Aufbewahrungsdauer der personenbezogenen Daten und Gesundheitsdaten;
- alle Weisungen zur Verarbeitung der personenbezogenen Daten und Gesundheitsdaten durch Doctolib schriftlich zu dokumentieren;
- im Vorfeld und während der gesamten Dauer der Verarbeitung sicherzustellen, dass Doctolib die in der DSGVO vorgesehenen Verpflichtungen einhält;
- die von Doctolib in seiner Eigenschaft als Auftragsverarbeiter durchgeführte Verarbeitung zu überwachen;
- einen Hauptansprechpartner, der Sie vertritt, und ggf. einen Datenschutzbeauftragten gemäß den Bestimmungen der DSGVO und des BDSG 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 als Auftragsverarbeiter

4.2.1. Doctolib verpflichtet sich dazu:

- personenbezogene Daten und Gesundheitsdaten in Übereinstimmung mit den in diesem AVV dargelegten Zwecken und Rahmenbedingungen zu verarbeiten und die für personenbezogene Daten und Gesundheitsdaten geltenden technischen Standards einzuhalten;
- nur auf Ihre alleinige vorherige Weisung zu handeln. Im Falle der Unmöglichkeit oder Unzumutbarkeit, bestimmten Weisungen Folge zu leisten, wird Doctolib Sie schnellstmöglich informieren. Doctolib kann in diesem Fall um eine schriftliche Befreiung von der Weisung ersuchen. Doctolib sollte in diesem Fall Ihre schriftliche, vorherige und spezifische Erlaubnis erhalten, um diese Befreiung anwenden zu können;
- keine Kopien personenbezogener Daten und Gesundheitsdaten ohne Ihre Erlaubnis oder Weisung anzufertigen, diese nicht an Dritte weiterzugeben und nicht für andere als die im Vertrag genannten Zwecke zu verwenden;
- personenbezogene Daten und Gesundheitsdaten, die Doctolib von Ihnen anvertraut wurden, nicht für eigene Zwecke oder im Auftrag Dritter, zu welchem Zweck und auf welche Weise auch immer, zu verwerten oder zu verarbeiten, es sei denn, es wurde von Ihnen gestattet. Insbesondere ist jede Verwendung dieser Gesundheitsdaten für Marketing-, Werbe-, kommerzielle oder statistische Zwecke untersagt;
- alle zur Verfügung stehenden Mittel gemäß den vertraglichen Bestimmungen und dem Stand der Technik einzusetzen, um die Sicherheit und die Vertraulichkeit der Doctolib anvertrauten personenbezogenen Daten und Gesundheitsdaten 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 und Gesundheitsdaten 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 Datenverarbeitung zu schützen;
- Sie schnellstmöglich über jeden Sicherheitsvorfall zu benachrichtigen, der direkt oder indirekt Sie betreffende personenbezogene Daten, Gesundheitsdaten oder Datenverarbeitungen betrifft;
- regelmäßige Sicherungen der personenbezogenen Daten und Gesundheitsdaten durchzuführen (sog. “Backups”);
- regelmäßige Penetrationstests durchzuführen;
- die für den störungsfreien Betrieb der Doctolib-Dienste erforderliche Hardware zu warten;
- die Vertraulichkeit der personenbezogenen Daten und Gesundheitsdaten zu gewährleisten;
- alle von Ihnen mitgeteilten Aktualisierungen, Korrekturen, Löschungen oder sonstige Änderungen der personenbezogenen Daten und Gesundheitsdaten zu berücksichtigen;
- die geltende Aufbewahrungsfrist der personenbezogenen Daten und Gesundheitsdaten gemäß den Zwecken, für welche diese erhoben oder zur Verfügung gestellt wurden wie vom Verantwortlichen vorgegeben, 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 sicherzustellen, dass Personen, die gemäß diesem AVV zur Verarbeitung personenbezogener Daten und Gesundheitsdaten berechtigt sind:

- sich zur Einhaltung der Vertraulichkeit verpflichten oder an eine angemessene gesetzliche Pflicht zur Verschwiegenheit gebunden sind;
- die für den Schutz personenbezogener Daten und Gesundheitsdaten erforderlichen Schulungen erhalten;
- die Grundsätze des Datenschutzes und des Schutzes personenbezogener Daten und Gesundheitsdaten als Standard bei Tools, Produkten, Applikationen oder Diensten berücksichtigen.

Unter Berücksichtigung der Art der Datenverarbeitung und der Doctolib zur Verfügung stehenden Informationen unterstützt Doctolib Sie bei der Durchführung von Datenschutz-Folgenabschätzungen sowie bei der Durchführung vorangehender Konsultation der Aufsichtsbehörden.

Doctolib stellt Ihnen alle notwendigen Informationen über die Datenverarbeitung personenbezogener Daten und Gesundheitsdaten zur Verfügung, um Sie bei der Erfüllung Ihrer gesetzlichen und behördlichen Pflichten als Verantwortlicher der Verarbeitung gemäß den Bestimmungen der DSGVO zu unterstützen.

In Ermangelung besonderer Weisungen Ihrerseits im Hinblick auf die Art der zu verarbeitenden personenbezogenen Daten und Gesundheitsdaten, deren Zwecke, Rechtsgrundlage und Aufbewahrungsfrist erkennen Sie an, dass diese personenbezogenen Daten und Gesundheitsdaten gemäß der in den Besonderen Bedingungen dargelegten Bestimmungen verarbeitet werden. Sie können als Verantwortlicher der Verarbeitung während der Ausführung des Vertrags um eine Änderung dieser Bestimmungen ersuchen.

4.3 Weiterverwendung von Daten

4.3.1 Weiterverwendung von Daten ohne Gesundheitsdaten von Patienten

Sie ermächtigen Doctolib zur Weiterverwendung der folgenden personenbezogenen Daten, die ursprünglich als Auftragsverarbeiter im Rahmen der in den besonderen Bedingungen beschriebenen Verarbeitungsaktivitäten verarbeitet wurden, als Verantwortlicher: Ihre beruflichen Daten (einschließlich verfügbarer Besuchsgründe, Besonderheiten des Behandlunsortes); Nutzungs- und Verbindungsdaten im Zusammenhang mit Ihrer Nutzung der Doctolib-Dienste; Termindaten ohne die Möglichkeit, Patienten zu identifizieren (z. B. Datum/Uhrzeit und Ort des Termins, Status des Termins).

Der Zweck dieser Weiterverwendung besteht darin, die Dienste zu verbessern, Statistiken zu erstellen, die an der Öffentlichkeit und Dritten zugänglich gemacht werden können, und die aufgeführten personenbezogenen Daten zu anonymisieren. Sie erkennen an, dass diese Zwecke mit den in den besonderen Bedingungen dieser Vereinbarung genannten Verarbeitungszwecken vereinbar sind.

Doctolib verpflichtet sich, den betroffenen Personen die Ausübung ihres Widerspruchsrechts zu ermöglichen. Wenn Sie mit dieser Weiterverwendung nicht einverstanden sind, können Sie die Admin-Einstellungen in in Ihrem Datenschutzcenter ändern.

4.3.2 Weiterverwendung von Daten, einschließlich Gesundheitsdaten von Patienten

Vorbehaltlich Ihrer ausdrücklichen Genehmigung kann Doctolib Daten der folgenden Datenkategorien als Verantwortlicher weiterverwenden: Ihre beruflichen Daten; Support- und Feedback-Daten; Nutzungs- und Verbindungsdaten im Zusammenhang mit Ihrer Nutzung der Dienste (einschließlich Protokolle); Ihre Sprachaufzeichnungen, einschließlich Sprachdiktate; die in den Besonderen Bedingungen aufgeführten personenbezogenen Daten von Patienten, insbesondere einschließlich Gesundheitsdaten und Messaging-Daten sowie Daten von Geräten und Anwendungen Dritter. Es werden keine direkt identifizierbaren Daten weiterverwendet.

Der Zweck dieser Weiterverwendung besteht darin, Forschungen und Studien durchzuführen, die Dienste von Doctolib zu verbessern und weiterzuentwickeln sowie die aufgeführten personenbezogenen Daten zu anonymisieren. Sie erkennen an, dass diese Zwecke mit den in den besonderen Bedingungen dieser Vereinbarung genannten Verarbeitungszwecken vereinbar sind.

Die Genehmigung gilt nicht voreingestellt als erteilt: Es steht Ihnen frei, zuzustimmen oder abzulehnen und Ihre Wahl jederzeit über die Admin-Einstellungen in Ihrem Datenschutzcenter zu ändern. Doctolib verpflichtet sich, den betroffenen Personen die Ausübung ihres Widerspruchsrechts zu ermöglichen.

Die Gesundheitsdaten der Patienten werden nur nach Einholung der Einwilligung der betreffenden Patienten oder nach Erhalt einer entsprechenden behördlichen Genehmigungen verarbeitet. Die Patienten behalten die endgültige Entscheidung über die Verwendung ihrer Gesundheitsdaten: Betroffen sind nur diejenigen, die über ihr Doctolib-Konto der Teilnahme an Forschungsarbeiten und der Entwicklung innovativer Produkte zugestimmt haben.

5. VERLETZUNG DES SCHUTZES PERSONENBEZOGENER DATEN

Doctolib meldet Ihnen jede Verletzung des Schutzes personenbezogener Daten und/ oder Gesundheitsdaten unverzüglich, nachdem Doctolib hierüber Kenntnis erlangt hat, per E-Mail oder über ein anderes von Ihnen zur Verfügung gestelltes Kommunikationsmittel.

Auf Ihre Anfrage wird dieser Meldung sachdienliche Dokumentation beigefügt, damit Sie erforderlichenfalls an die zuständige Aufsichtsbehörde melden und gegebenenfalls die betroffenen Personen über die Verletzung informieren können.

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

6. VERZEICHNIS VON VERARBEITUNGSTÄTIGKEITEN

Doctolib führt ein Verzeichnis über alle Kategorien von Verarbeitungstätigkeiten, die in Ihrem Auftrag ausgeführt werden, gemäß den Bestimmungen der DSGVO.

7. INFORMATION UND RECHTE DER BETROFFENEN PERSONEN

Es obliegt Ihrer Verantwortung, die betroffenen Personen gemäß den Bestimmungen der DSGVO insbesondere (i) über die im Rahmen der Dienste durchgeführte Verarbeitung zu informieren und, insofern dies nach geltendem Recht erforderlich ist, deren Einwilligung einzuholen; (ii) über die Rechtsgrundlage der durchgeführten Verarbeitung, die Zwecke der Verarbeitung und die Liste der Auftragsverarbeiter, welche die personenbezogenen Daten verarbeiten können, zu informieren.

Um Sie bei dieser Informationspflicht zu unterstützen, veröffentlicht Doctolib auf dem Patientenportal Datenschutzhinweise, die unter https://doctolib.legal/privacy-policy-B2C-D zugänglich sind.

8. VERWALTUNG VON BETROFFENENRECHTEN

Es obliegt Ihnen, den Betroffenenrechten im Hinblick auf die personenbezogenen Daten betroffener Personen nachzukommen.

Soweit möglich kann Doctolib Sie in seiner Eigenschaft als Auftragsverarbeiter und auf Ihre Anfrage bei der Erfüllung Ihrer Pflicht, Datenschutzanfragen betroffener Personen nachzukommen, unterstützen. Hierzu zählen Anfragen in Bezug auf das Recht auf Auskunft, Berichtigung, Löschung und Widerspruch, Einschränkung der Verarbeitung sowie Datenübertragbarkeit und das Recht, nicht Gegenstand eines automatisierten Verfahrens zu werden (inklusive Profiling).

Wenn sich eine betroffene Person direkt an Doctolib wendet, um Auskunft zu erhalten über Daten, die Doctolib im Auftrag verarbeitet, weist Doctolib die betroffene Person darauf hin, dass sie sich mit dieser Auskunftsanfrage an Sie wenden kann.

Doctolib kann Sie bei der Beantwortung von Anfragen unterstützen, kann jedoch in diesen Fällen nicht direkt an die betroffenen Personen antworten.

9. SICHERHEIT UND VERTRAULICHKEIT

9.1 Hinsichtlich der Dienste setzt Doctolib die für die Sicherheit geeigneten technischen und organisatorischen Maßnahmen gemäß der DSGVO um, die darauf abzielen, ein angemessenes Sicherheitsniveau in Bezug auf die Risiken zu gewährleisten, die durch die Verarbeitung der personenbezogenen Daten entstehen wie in „Technische und organisatorische Maßnahmen“ angegeben, welche wiederum je nach den von Ihnen abonnierten oder genutzten Diensten gelten. 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.

Alle Mitarbeitenden verfügen über einen Ausweis mit ihrem Foto, der ihnen entsprechend ihrer Akkreditierung innerhalb des Unternehmens Zugang zu den Räumlichkeiten gewährt. Die Akkreditierung wird entweder entsprechend der Rolle des Mitarbeitenden oder auf Antrag seiner Führungskraft festgelegt, wobei dieser Antrag von der zuständigen Abteilung validiert werden muss. Das Tragen eines Ausweises ist für jede Mitarbeiterin und jeden Mitarbeiter verpflichtend. Bei Vergessen des Ausweises muss der Mitarbeitende dem Sicherheitspersonal einen Identitätsnachweis vorlegen. Dieses prüft die Identität und stellt bei erfolgreicher Überprüfung einen Tagesausweis aus, der am selben Abend zurückzugeben ist. Diese Maßnahme dient somit auch dem Schutz der Vertraulichkeit der uns anvertrauten personenbezogenen Daten.

Die oben genannten Verpflichtungen entbinden Sie in keiner Weise davon, alle notwendigen Sicherheitsvorkehrungen zu treffen, um die Vertraulichkeit der Dokumente und der Abonnentendaten, der Patientenstammdaten, der Nutzerdaten, der personenbezogenen Daten und der Gesundheitsdaten auf der Doctolib-Plattform zu gewährleisten.

Es wird zwischen den Parteien vereinbart, dass der Vertrag, der den vorliegenden AVV umfasst, der zuständigen Aufsichtsbehörde im Falle einer Kontrolle vorgelegt werden kann.

9.2 Berechtigte Personen: Für die Erbringung der Dienste setzt Doctolib ausreichend und qualifiziertes Personal ein, das über die für die Leistungserbringung erforderlichen technischen und/oder funktionalen Fähigkeiten verfügt. Personen, die zur Verarbeitung personenbezogener Daten und/ oder Gesundheitsdaten in Ihrem Auftrag berechtigt sind, müssen in den Vorschriften zum Schutz personenbezogener Daten geschult sein.

9.3 Berufsgeheimnis: Doctolib ist bekannt, dass die bei der Nutzung der Dienste verarbeiteten personenbezogenen Daten und Gesundheitsdaten unter ein Berufsgeheimnis im Sinne von § 203 StGB fallen. Doctolib verpflichtet sich, über Berufsgeheimnisse Stillschweigen zu bewahren und sich nur insoweit Kenntnis von diesen Daten zu verschaffen, wie dies zur Erfüllung der Doctolib zugewiesenen Aufgaben erforderlich ist.

Der Verantwortliche der Verarbeitung weist Doctolib darauf hin, dass sich Personen, die an der beruflichen Tätigkeit eines Berufsgeheimnisträgers mitwirken und unbefugt ein fremdes Geheimnis offenbaren, das ihnen bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt geworden ist, nach § 203 Abs. 4 S. 1 StGB strafbar machen. Zudem macht sich eine mitwirkende Person nach § 203 Abs. 4 S. 2 StGB strafbar, sollte sie sich einer weiteren mitwirkenden Person bedienen, die ihrerseits unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, und nicht dafür Sorge getragen hat, dass diese zur Geheimhaltung verpflichtet wurde.

Doctolib stellt sicher, dass alle mit der Verarbeitung von dem Berufsgeheimnis unterliegenden Daten des Verantwortlichen befassten Beschäftigten und andere für Doctolib tätigen Personen (z.B. Unterauftragsverarbeiter), die damit befasst sind, in Textform dazu verpflichtet werden, die ihnen bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenen Berufsgeheimnisse nicht unbefugt zu offenbaren und sie über die mögliche Strafbarkeit belehrt wurden.

9.4 Inhaberschaft an den Daten: Sofern keine ausdrücklichen anderen Vereinbarungen zum Datenschutz getroffen wurden, bleiben Sie alleiniger Inhaber Ihrer Daten, die von Ihnen auf dem Patientenportal, Nutzerprofil sowie der Doctolib-Plattform veröffentlicht wurden. Doctolib kann aus der Veröffentlichung keine Rechte an den Daten geltend machen, die von Ihnen veröffentlicht wurden. Die anonymisierten Nutzungsstatistiken des Patientenportals sind Eigentum von Doctolib.

10. UNTERAUFTRAGSVERARBEITUNG

Sie erteilen an Doctolib eine allgemeine schriftliche Genehmigung für die Beauftragung der am Ende dieses AVV aufgelisteten Unterauftragsverarbeiter, wenn die Beauftragung für die Erbringung der Dienste in angemessener Weise erforderlich ist. Im Zusammenhang mit dieser allgemeinen schriftlichen Genehmigung verpflichtet sich Doctolib dazu, Sie mittels einer Ankündigung in Textform dreißig (30) Tage im Voraus über jede beabsichtigte Änderung in Form der Hinzufügung oder des Ersatzes eines Unterauftragsverarbeiters zu informieren. Dadurch können Sie potentielle Einwände gegen diese Änderung rechtzeitig erheben. Sollten Sie berechtigte und nachvollziehbare Gründe haben, die Beauftragung eines neuen Unterauftragsverarbeiters abzulehnen, müssen Sie unverzüglich eine begründete Beschwerde bei Doctolib unter datenschutz@doctolib.de innerhalb einer Frist von dreißig (30) Tagen nach erteilter Ankündigung einlegen. Andernfalls gilt der Einsatz des Unterauftragsverarbeiters als genehmigt.

Nach Gesprächen und in Ermangelung einer Einigung zwischen Doctolib und Ihnen können Sie innerhalb von dreißig (30) Tagen nach der Benachrichtigung den von der betreffenden Aktualisierung betroffenen Teil des Vertrages kündigen.

Im Hinblick auf jeden Unterauftragsverarbeiter muss Doctolib (i) angemessene Sorgfalt bei der Bewertung, Ernennung und Überwachung der Tätigkeiten des Unterauftragsverarbeiters walten lassen; (ii) in den Vertrag zwischen Doctolib und jedem Unterauftragsverarbeiter Klauseln einfügen, mit denen ein Schutz für Ihre personenbezogenen Daten und Gesundheitsdaten sowie von Patienten- und Angehörigendaten gewährleistet wird, der zu den Bestimmungen dieses AVV gleichwertig ist.

Doctolib bleibt Ihnen gegenüber für jegliche Nichterfüllung der Pflichten durch seine Unterauftragsverarbeiter bei der Verarbeitung Ihrer personenbezogenen Daten und Gesundheitsdaten gemäß den Vertragsbedingungen haftbar.

11. HDS ZERTIFIZIERUNG (Health Data Hosting)

11.1. Der Host der Doctolib-Dienste, Amazon Web Services SARL (AWS) mit Sitz in 38 avenue John F. Kennedy, L - 1885 Luxemburg ist für das Hosting von Gesundheitsdaten mit dem Zertifikat HDS (Health Data Host) zertifiziert. Dieses Zertifikat ist zwar nicht nach deutschem, aber zumindest nach französischem Recht zwingend für jeden Host, der Gesundheitsdaten speichert.

AWS hält seit dem 28. Januar 2021 die Zertifikate "Physical Infrastructure Host" und "Outsourcer Host". Gesundheitsdaten werden von AWS in der Europäischen Union gespeichert. Als Health Data Host beauftragt Doctolib AWS mit der Erbringung der folgenden Dienstleistungen im Zusammenhang mit dem Hosting der Doctolib-Plattform: "Bereitstellung und Wartung der physischen Standorte, die für das Hosting der physischen Infrastruktur des Informationssystems zur Verarbeitung von Gesundheitsdaten vorgesehen sind"; "Bereitstellung und Wartung der

physischen Infrastruktur des Informationssystems zur Verarbeitung von Gesundheitsdaten"; "Bereitstellung und Wartung der virtuellen Infrastruktur des Informationssystems zur Verarbeitung von Gesundheitsdaten"; "Bereitstellung und Wartung der Plattform für das Hosting der Anwendungen des Informationssystems; Sicherung der Gesundheitsdaten."

11.2 In Übereinstimmung mit zwingenden französischen Gesetzesbestimmungen und als zertifizierter Gesundheitsdaten-Host :

(i) verarbeitet AWS Gesundheitsdaten nur auf dokumentierte Weisung von Doctolib und ergreift Sicherheitsmaßnahmen, um den Zugang zu diesen Gesundheitsdaten zu regeln;

(ii) stellt AWS Doctolib Funktionen zur Verfügung, die es ihm ermöglichen, (a) Ihr Recht auf Übertragbarkeit zu gewährleisten und (b) einen möglichen Ausfall von AWS abzudecken und (c) bei Vertragsende die Rückgabe und/oder Löschung der von AWS gehosteten Gesundheitsdaten zu erwirken;

(iii) benachrichtigt AWS Doctolib im Falle eines Sicherheitsvorfalls so schnell wie möglich und ergreift alle angemessenen Maßnahmen, um den aus einem solchen Vorfall resultierenden Schaden zu begrenzen, und gibt Doctolib die Möglichkeit, sich bei Vorfällen, die sich auf die gehosteten personenbezogenen Daten auswirken, an einen Vertragsreferenten zu wenden;

(iv) verpflichtet sich AWS, dass seine möglichen Auftragsverarbeiter ein Schutzniveau bieten, das dem von AWS gegenüber Doctolib garantierten Schutzniveau entspricht;

(v) ermächtigt AWS Doctolib zur Durchführung von Audits, um die Einhaltung der Verpflichtungen aus seinem Vertrag mit Doctolib zu gewährleisten; die technischen und organisatorischen Sicherheitsmaßnahmen können auf Verlangen von Doctolib Gegenstand von Dokumentationsaudits sein, während die Einhaltung der Norm ISO 27001 (einschließlich der Sicherheit des Rechenzentrums) von Doctolib nach Übermittlung des jährlichen Auditberichts durch einen unabhängigen Sicherheitsexperten überprüft werden kann;

(vi) stellt AWS Doctolib über diesen Link Qualitäts- und Leistungsindikatoren zur Verfügung, die es ihm ermöglichen, das angekündigte Dienstleistungsniveau, das garantierte Niveau, die Häufigkeit ihrer Messung sowie etwaige Sanktionen bei Nichteinhaltung dieser Indikatoren zu überprüfen;

(vii) hält AWS alle Gesetze, Regeln, Vorschriften und Verordnungen ein, die für seine Tätigkeit als Gesundheitsdaten-Host gelten.

11.3. Doctolib ist seit dem 14. Oktober 2021 als "Healthcare Data Host" zertifiziert. Diese Zertifizierung umfasst alle regulierten Tätigkeiten (Tätigkeiten 1 bis 6) gemäß Artikel R1111-9 des französischen Gesundheitsgesetzbuchs (R1111-9). Detaillierte Informationen zur Zertifizierung, einschließlich Ausstellungsdatum, Verlängerung und dem Umfang der zertifizierten Tätigkeiten, sind auf der offiziellen Website der französischen Agentur für digitale Gesundheit (ANS) verfügbar.

11.4 Doctolib meldet Ihnen jede Verletzung von Gesundheitsdaten gemäß Artikel 5 dieses AVV.

11.5 Doctolib ergreift geeignete technische und organisatorische Sicherheitsmaßnahmen, um ein angemessenes Sicherheitsniveau angesichts der Risiken zu gewährleisten, die mit dem Hosting Ihrer Gesundheitsdaten verbunden sind (siehe „Technische und organisatorische Maßnahmen"). So werden die Gesundheitsdaten nur über sichere Kommunikationsnetze übermittelt.

Für den Fall, dass Doctolib diese technischen und organisatorischen Maßnahmen technisch weiterentwickelt, verpflichtet sich Doctolib, ein Sicherheitsniveau aufrechtzuerhalten, das dem in diesem AVV vorgesehenen gleichwertig ist, es sei denn, die betreffende technische Weiterentwicklung ist durch eine gesetzliche oder behördliche Verpflichtung vorgeschrieben.

11.6 Bei Vertragsende oder auf Ihren Wunsch hin, wenn Doctolib die HDS-Zertifizierung entzogen wird, können Sie die von Doctolib gehosteten Gesundheitsdaten unter den in Artikel 13 diesem AVV genannten Bedingungen zurückerhalten.

12. AUDIT

12.1 Zur Überprüfung der Sicherheit der Doctolib-Plattform können Sie 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 Ihnen in Rechnung gestellt wird.

12.2 Der 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 spezifische personenbezogene Daten von Ihnen, 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 der Unterauftragsverarbeiter von Doctolib.

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 Sie 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 Wartung ermöglichen darf.

Jegliche Intrusions- oder Penetrationstests, die auf die Doctolib-Plattform 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 Sie müssen Doctolib mindestens dreißig (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 (Ausgangs-IP-Adresse, 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 Ihnen 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 Sie die Hinzuziehung eines externen Auditors wünschen, müssen Sie 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.

Sie verpflichten sich dazu, Doctolib den Auditbericht kostenfrei zur Verfügung zu stellen. Doctolib wird Gelegenheit gegeben, zum Auditbericht Stellung zu nehmen.

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

13. RÜCKGABE DER PATIENTENSTAMMDATEN

Sie können die Patientenstammdaten (mit Ausnahme des Messaging-Dienstes, für den besondere Bedingungen gelten) sowie die Historie ihrer Termine am Ende des Vertrags zurückerlangen, es sei denn, diese Daten wurden von Ihnen unrechtmäßig erhoben. Diese Daten werden Ihnen in CVS- oder Excel-Format zur Verfügung gestellt. Der Exportantrag muss per E-Mail an folgende Adresse gestellt werden: contact@doctolib.com.

Doctolib verpflichtet sich dazu, über die gesamte Vertragslaufzeit hinweg und während des gesamten Datenrückgabeprozesses für Sie eine Kopie Ihrer Daten zur Verfügung zu halten. Im Fall einer Aussetzung Ihres Zugangs zur Doctolib-Plattform, gleich aus welchem Grund, ermöglicht Ihnen Doctolib über eine CVS- oder Excel-Datei die Rückerlangung der letzten Kopie Ihrer Patientendatenbank sowie der Historie Ihrer Termine zu erhalten (außer in Fällen, in denen diese Daten von Ihnen unrechtmäßig erhoben wurden).

Bei Beendigung des Vertrages wird Doctolib die Gesundheitsdaten löschen, ohne eine Kopie davon zu behalten, vorbehaltlich gesetzlicher Aufbewahrungspflichten, denen Doctolib unterliegt. Der Nachweis der Löschung der Gesundheitsdaten kann auf Ihre Anfrage übermittelt werden.

14. ÜBERMITTLUNG PERSONENBEZOGENER DATEN

Personenbezogene Daten dürfen nur zu den in diesem AVV aufgeführten Zwecken und in Übereinstimmung mit der geltenden Gesetzgebung an Unternehmen der Doctolib Gruppe, deren Unterauftragsverarbeiter oder Dienstleister übermittelt 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 Sie, dass personenbezogene Daten von Doctolib auch in Drittländer an seine Unterauftragsverarbeiter übermittelt werden können, falls eine solche Übermittlung für die Ausführung der bestellten Dienste erforderlich ist. Die Liste der Unterauftragsverarbeiter ist am Ende dieses AVV verfügbar.

Wenn die Datenübermittlung 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 diesem 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 in Ihrem Auftrag durch Doctolib verarbeitet werden, übermitteln, um gesetzlichen Verpflichtungen nachzukommen. In diesem Fall wird Doctolib Sie über die Übermittlung informieren, soweit gesetzlich zulässig.

15. KONTAKT UND ZUSTÄNDIGE AUFSICHTSBEHÖRDEN

Bei Fragen zu der von Doctolib durchgeführten Verarbeitung personenbezogener Daten und Gesundheitsdaten und/oder wenn Sie spezifische Weisungen zur Verarbeitung personenbezogener Daten und Gesundheitsdaten durch Doctolib haben, können Sie gemäß den vertraglichen Bestimmungen den Datenschutzbeauftragten von Doctolib unter untenstehend angegebener Adresse kontaktieren.

Die Hauptniederlassung der Doctolib Gruppe im Sinne von Art. 4 Abs. 16 DSGVO im Sinne der DSGVO ist die Muttergesellschaft Doctolib SAS (Frankreich). Die federführende Aufsichtsbehörde für grenzüberschreitende Verarbeitungen im Sinne von Art. 56 DSGVO ist daher die französische Aufsichtsbehörde CNIL (https://www.cnil.fr). Für Verarbeitungstätigkeiten, die nicht in den Zuständigkeitsbereich der federführenden Aufsichtsbehörde fallen, ist die zuständige Behörde die Berliner Beauftragte für Datenschutz und Informationsfreiheit.Der Datenschutzbeauftragte von Doctolib kann unter der Adresse Doctolib GmbH, Mehringdamm 51, 10961 Berlin oder datenschutz@doctolib.de kontaktiert werden.

16. ANWENDBARES RECHT

Dieser AVV untersteht dem Recht des Landes, das auf den Verantwortlichen der Verarbeitung Anwendung findet.

17. Geltung des AVV

Dieser AVV regelt die vertraglichen Beziehungen bezüglich der Verarbeitung im Auftrag in abschließender Weise und ersetzt alle bisherigen diesbezüglichen Vereinbarungen zwischen den Parteien, einschließlich früherer Versionen des AVV, der zwischen Ihnen und Doctolib unterzeichnet wurde.

BESONDERE BEDINGUNGEN FÜR DIE VERARBEITUNG

„KONFIGURATION VON ABONNENTEN UND NUTZERKONTEN“

ZWECKE DER VERARBEITUNG:

- Kontenverwaltung: die Nutzerkonten und die Nutzerberechtigungen zu konfigurieren;
- Technischer Support und Hilfe: Gewährleistung von technischem Supports, Wartung und Bearbeitung von Nutzeranfragen, Beratung, Hosting und andere den Nutzern angebotene Dienste;
- Support bezüglich personenbezogener Daten: Hilfe bei der Verletzung des Schutzes von personenbezogenen und Gesundheitsdaten, Unterstützung bei der Erstellung von Datenschutz-Folgenabschätzungen, Unterstützung bei der Beantwortung von Betroffenenanfragen;
- Überweisung von Patienten an eine Gesundheitsfachkraft;
- Reporting, Debugging und Statistiken;
- Verbesserung der Dienste;
- Erstellung von Statistiken im Auftrag der Gesundheitsfachkraft;
- Anonymisierung von Daten.
-

RECHTSGRUNDLAGE DER VERARBEITUNG:

Es liegt in Ihrer Verantwortung, die Rechtsgrundlage vor jeder Verarbeitung zu bestimmen.

BETROFFENE PERSONEN:

Abonnent und Nutzer, wie im AVV festgelegt.

KATEGORIEN VON PERSONENBEZOGENEN DATEN:

Um die Menge der verarbeiteten personenbezogenen Daten so gering wie möglich zu halten, müssen Sie sicherstellen, dass Sie nur Daten erheben und verwenden, die für die Erreichung des jeweiligen Verarbeitungszwecks, insbesondere für die medizinische und administrative Verwaltung seines Patientenstamms 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-Adresse, Postanschrift, Foto, Unterschrift, Personalausweis oder Pass.
b) **Berufsbezogene Daten:** Fotografie, Fachrichtung, Angaben zur Behandlung, Werdegang der Gesundheitsfachkraft, angebotene Besuchsgründe, Sprechzeiten, Besonderheiten in Verbindung mit dem Behandlungsort.
c) **Nutzungs- und Verbindungsinformationen im Zusammenhang mit Ihrer Nutzung** der Doctolib-Dienste.

AUFBEWAHRUNGSDAUER:

Spezifische von Ihnen geforderte Aufbewahrungsdauern müssen Doctolib mitgeteilt werden.

BESONDERE BEDINGUNGEN FÜR DIE VERARBEITUNG

„TERMIN- UNDKALENDERDIENST"

ZWECKE DER VERARBEITUNG:

- Unterstützung beim Hochladen und der Übertragung von Kalenderinhalten, Terminen sowie, falls erforderlich, von Patientendaten auf der Doctolib-Plattform;.
- Einhaltung der für die Identitätsüberwachung geltenden Regeln;
- Ermöglichung der Verwaltung des Kalenders und der darin enthaltenen Daten;
- Ermöglichung der Verwaltung des Versorgungspfads für Patienten und deren Angehörige;
- Ermöglichung für Patienten, online Termine für sich und ihre Angehörigen zu vereinbaren;
- Ermöglichung für Patienten, in ihrem Account ihre vollständige Terminhistorie sowie die Historie ihrer Interaktion mit Ihnen, sowohl für sich selbst als auch für ihre Angehörigen, einsehen zu können;
- Ermöglichung der Buchung von Terminen durch Patienten und deren Angehörigen über ein Google Business Profil
- Ermöglichung der Online-Terminbuchung als Teil durch öffentliche Gesundheitsbehörden vorgesehener Terminmöglichkeiten;
- Ermöglichung der Verwaltung von Terminen vor Ort oder per Videosprechstunde;
- Ermöglichung der Kommunikation zwischen der Gesundheitsfachkraft und dem Patienten und Bereitstellung von Informationen für Patienten und deren Angehörige in Bezug auf das Nutzerprofil und ihren Versorgungspfad;
- Ermöglichung des Sendens und Empfangens von Dokumenten zwischen der Gesundheitsfachkraft und dem Patienten sowie Angehörigen
- Versenden von SMS, E-Mails und Push-Benachrichtigungen (i) zur Bestätigung, Stornierung oder Erinnerung von Terminen; (ii) für Informationen über den Versand von Dokumenten; (iii) für Informationen über Erinnerungen und (iv) für Informationen im Zusammenhang mit der Versorgung des Patienten oder der Organisation seiner Tätigkeit;
- Löschung von fehlerhaften Daten, nachdem diese Fehler vom rechtmäßigen Dateninhaber gemeldet und von Doctolib überprüft wurden;
- Einräumung der Möglichkeit für die Gesundheitsfachkraft, ihren Patienten Gruppenmitteilungen informativer oder präventiver Art zu senden, insbesondere durch die Verwendung spezifischer Filter und/oder durch das Herunterladen von Empfängerlisten durch die Gesundheitsfachkraft;
- ordnungsgemäße Verwaltung im Rahmen der Online-Terminbuchung der Patientenidentität in den Doctolib-Diensten, insbesondere durch Vermeidung der Erstellung doppelter Patientendateien;
- Begrenzung der Anzahl von Terminen, die pro Nutzer für bestimmte Fachrichtungen über einen Zeitraum von 7 Tagen vereinbart werden können, um Überbuchungen zu vermeiden;
- Berichterstattung, Fehlersuchstatistiken;
- Verbesserung der Dienste;
- Erstellung von Statistiken im Auftrag der Gesundheitsfachkraft;
- Anonymisierung von Daten.

RECHTSGRUNDLAGE DER VERARBEITUNG:

Es liegt in Ihrer Verantwortung, die Rechtsgrundlage vor jeder Verarbeitung zu bestimmen.

BETROFFENE PERSONEN:

- Patienten und deren Angehörige;
- Mitarbeiter der Gesundheitsfachkräfte;
- Abonnent und Nutzer

KATEGORIEN VON PERSONENBEZOGENEN DATEN:

Um die Anzahl der zu verarbeitenden personenbezogenen Daten und Gesundheitsdaten so gering wie möglich zu halten, müssen Sie sicherstellen, dass Sie nur die personenbezogenen Daten und Gesundheitsdaten erheben und verwenden, die im Hinblick auf Ihre eigene Verwaltung und die administrative Bearbeitung Ihres Patientenstamms relevant und notwendig sind.

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

- **Identität und die Kontaktdaten des Patienten oder Angehörigen**: Geschlecht, Nachname, Vorname, Geburtsdatum, Geburtsort, Postanschrift, E-Mail-Adresse und Telefonnummer.
- **Berufliche Stellung des Patienten oder Angehörigen**: der Beruf.
- Ihre beruflichen Daten: Fachrichtung, angebotene Konsultationsgründe, Besonderheiten des Behandlungsortes, Kontaktdaten;
- **Gesundheit**: Versicherungsstatus, Identität und Kontaktdaten des behandelnden Arztes, Identität und Kontaktdaten der überweisenden Gesundheitsfachkraft , Datum/Uhrzeit und Ort des Termins, Fachgebiet der Gesundheitsfachkraft und Besuchsgrund, Status des Termins, medizinische Dokumente des Patienten, von der Gesundheitsfachkraft ausgefüllte Felder;
- **Nutzungs- und Verbindungsinformationen im Zusammenhang mit Ihrer Nutzung des Doctolib-Dienstes**.

EMPFÄNGER DER DATEN:

- Gesundheitsfachkräfte;
- Assistenten, unter Einhaltung der Bestimmungen zum Berufsgeheimnis;
- Befugte Personen von Doctolib.

AUFBEWAHRUNGSDAUER:

Spezifische von Ihnen geforderte Aufbewahrungsdauern müssen Doctolib mitgeteilt werden. Falls keine solche Weisung durch Sie vorliegt, beträgt die Aufbewahrungsfrist für die Terminhistorie standardmäßig 5 Jahre. Es steht Ihnen frei, eine andere Aufbewahrungsfrist zwischen 1 bis 20 Jahren einzustellen.

Bezüglich der an Google übermittelten Informationen (berufliche Daten), beträgt die Aufbewahrungsfrist 24 Stunden.

Im Hinblick auf Verwaltungszwecke der Gesundheitseinrichtung sowie der ärztlichen oder nichtärztlichen Praxis dürfen auf der Doctolib-Plattform gespeicherte Daten maximal zwanzig Jahre ab dem Datum der letzten Behandlung des Patienten aufbewahrt werden.

BESONDERE BEDINGUNGEN FÜR DIE VERARBEITUNG

„VIDEOSPRECHSTUNDEN-DIENST“

ZWECKE DER VERARBEITUNG:

- Ermöglichung der Nutzung eines Videosprechstundentools mit Videoübertragung;
- Ermöglichung der Übermittlung von Dokumenten an den Patienten über das Profil der Gesundheitsfachkraft (Rezept, medizinischer Bericht usw.) und den Empfang dieser Dokumente zur Nachbereitung durch den Patienten;
- Ermöglichung für den Leistungserbringer, während der Videosprechstunde Notizen zu machen;
- Ermöglichung der Bezahlung der Videosprechstunde
- Betrugsentdeckung;
- Technischer Support und Unterstützung: Erbringung von technischem Support, Wartung, Verwaltung und Bearbeitung von Anfragen von Nutzern, Abonnenten, und Patienten betreffend der Videosprechstunde und der Online-Zahlung;
- Ermöglichung, dass die Gesundheitsfachkraft Screenshots der Videosprechstunde für die Krankenakte des Patienten anfertigt;
- Ermöglichung der Kommunikation zwischen der Gesundheitsfachkraft und dem Patienten über einen Videochat;
- Berichte, Fehlerbehebung und Statistiken;
- Durchführung von Kommunikationskampagnen per E-Mail und/oder SMS an Ihre Patienten, um sie über die Möglichkeit der Videosprechstunde für die tätigen Gesundheitsfachkräfte zu informieren;
- Verbesserung der Dienste;
- Erstellung von Statistiken im Auftrag der Gesundheitsfachkraft;
- Anonymisierung von Daten.

RECHTSGRUNDLAGE DER VERARBEITUNG:

Es liegt in Ihrer Verantwortung, die Rechtsgrundlage vor jeder Verarbeitung zu bestimmen.

BETROFFENE PERSONEN:

Nutzer, Patienten und deren Angehörige

KATEGORIEN VON PERSONENBEZOGENEN DATEN:

Um die Anzahl der zu verarbeitenden personenbezogenen Daten so gering wie möglich zu halten, müssen Sie sicherstellen, dass Sie nur die personenbezogenen Daten erheben und verwenden, die im Hinblick auf Ihre eigene Verwaltung und die administrative Bearbeitung Ihres Patientenstamms relevant und notwendig sind.

Grundsätzlich gelten die folgenden Daten als relevant für die oben genannten Zwecke:

- **Identität und die Kontaktdaten des Patienten oder Angehörigen**: Geschlecht, Nachname, Vorname, E-Mail-Adresse, Patienten-Identifikationsnummer, Postleitzahl, Datum der Einrichtung des Nutzerkontos;
- **Gesundheit**: Medizinische Dokumente des Patienten, von der Gesundheitsfachkraft ausgefüllte Notizen, von der Gesundheitsfachkraft für die medizinische Nachsorge des Patienten angefertigte Screenshots;
- Die **Nutzungs- und Verbindungsinformationen im Zusammenhang mit Ihrer Nutzung der Doctolib-Plattform (z.B. Protokolldateien)**.

AUFBEWAHRUNGSDAUER:

Spezifische von Ihnen geforderte Aufbewahrungsdauern müssen Doctolib mitgeteilt werden. Falls keine solche Weisung durch Sie vorliegt, beträgt die Aufbewahrungsfrist für die Terminhistorie) standardmäßig 5 Jahre. Es steht Ihnen frei, eine andere Aufbewahrungsfrist zwischen 1 bis 20 Jahren einzustellen.

BESONDERE BEDINGUNGEN FÜR DIE VERARBEITUNG

„PATIENTENNACHRICHTEN-DIENST“

ZWECKE DER VERARBEITUNG:

- Ermöglichung für Nutzer und/oder autorisierte Mitglieder der Gesundheitseinrichtung, Nachrichten an Patienten zu senden;
- Ermöglichung für Nutzer, Nachrichten von Patienten - bzw. in manchen Fällen nicht Patienten - zu akzeptieren oder nicht;
- Ermöglichung für die Patienten, Nachrichten an Nutzer zu senden und Ermöglichung für den Nutzer zu antworten;
- Ermöglichung für Nutzer, Dokumente an Patienten zu senden und Dokumente von Patienten zu erhalten;
- Ermöglichung für Nutzer, Gesundheitsinformationen an Patienten zu übermitteln;
- Berichterstattung, Fehlersuche und Statistik;
- Verbesserung der Dienste;
- Erstellung von Statistiken im Auftrag der Gesundheitsfachkraft;
- Anonymisierung von Daten.

RECHTSGRUNDLAGE DER VERARBEITUNG:

Es liegt in Ihrer Verantwortung, die Rechtsgrundlage vor jeder Verarbeitung zu bestimmen.

BETROFFENE PERSONEN:

Patienten, Nutzer und autorisierte Mitglieder der Gesundheitseinrichtung.

KATEGORIEN VON PERSONENBEZOGENEN DATEN:

Um die Anzahl der zu verarbeitenden personenbezogenen Daten so gering wie möglich zu halten, müssen Sie sicherstellen, dass Sie nur solche Daten erheben und verwenden, die für die medizinische und verwaltungstechnische Verwaltung Ihres Patientenstamms relevant und notwendig sind, und dabei auch die Gesundheitsdaten im Zusammenhang mit der über den Dienst eingereichten Anfrage berücksichtigen.

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

- Daten von Nutzern und von autorisierten Mitgliedern der Organisation;
- **Identitäts- und Kontaktdaten des Patienten**: Geschlecht, Vorname, Nachname, Geburtsdatum, E-Mail-Adresse;
- **Gesundheit**: behandelnder und überweisender Arzt, ärztliche Verordnungen, klinische Analysen, Berichte, im Feld "Zusätzliche Informationen" enthaltene Informationen, die der Patient als notwendig, relevant und sachdienlich erachtet, um sie der Gesundheitsfachkraft für die Verwaltung der angeforderten Leistung mitzuteilen, Inhalt von Dokumenten, die Gesundheitsdaten enthalten können, Informationen, die die Gesundheitsfachkraft im Feld "Zusätzliche Informationen" eintragen kann, die Gesundheitsdaten enthalten können.
- Die Nutzungs- und Verbindungsinformationen im Zusammenhang mit Ihrer Nutzung des Doctolib-Dienstes (z.B. Protokolldateien)

Es liegt in Ihrer Verantwortung, vom Patienten nur die Gesundheitsdaten und personenbezogenen Daten anzufordern, die für die vom Patienten in diesem Zusammenhang angeforderte Gesundheitsdienstleistung erforderlich sind.

Informationen, die nicht im Zusammenhang stehen mit dem Zweck, die Patientenanfrage zu bearbeiten, oder die nicht einschlägig sind für die Patientenversorgung müssen ausgenommen werden.

AUFBEWAHRUNGSDAUER:

Spezifische von Ihnen geforderte Aufbewahrungsdauern müssen Doctolib mitgeteilt werden.

BESONDERE BEDINGUNGEN FÜR DIE VERARBEITUNG

„INTELLIGENTER AUFGABEN-MANAGER“

ZWECKE DER VERARBEITUNG:

Der intelligente Aufgaben-Manager erleichtert die Kommunikation und Organisation innerhalb einer Gesundheitseinrichtung und mit Ihrem Sekretariat: Sie können für Patienten Aufgaben anlegen, zu organisierende Termine oder administrative zu erledigende Aufgaben.

- Reporting, Debugging und Statistiken;
- Verbesserung der Dienste;
- Erstellung von Statistiken im Auftrag der Gesundheitsfachkraft;
- Anonymisierung von Daten.

RECHTSGRUNDLAGE DER VERARBEITUNG:

Es liegt in Ihrer Verantwortung, die Rechtsgrundlage vor jeder Verarbeitung zu bestimmen.

BETROFFENE PERSONEN:

Patienten und Angehörige, Gesundheitsfachkräfte oder Assistenten mit Nutzerkonto

KATEGORIEN VON PERSONENBEZOGENEN DATEN:

Um die Anzahl der zu verarbeitenden personenbezogenen Daten so gering wie möglich zu halten, müssen Sie sicherstellen, dass Sie nur solche Daten erheben und verwenden, die für diese Datenverarbeitung relevant und notwendig sind.

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

- **Identität und die Kontaktdaten der Gesundheitsfachkraft und der Assistenten**;
- **Berufsbezeichnung** der **Gesundheitsfachkraft und der Assistenten**;
- die **Identität und die Kontaktdaten des Patienten oder Angehörigen**: Geschlecht, Nachname, Vorname, Geburtstag und Geburtsort, Postadresse, E-Mail-Adresse, Telefonnummer;
- **Beruf** des Patienten oder Angehörigen;
- **Gesundheitsdaten**: Versicherungsstatus, Identität und Kontaktdaten des behandelnden Arztes, Identität und Kontaktdaten der überweisenden Gesundheitsfachkraft, Datum/Zeit und ort des Termins, Fachgebiet der Gesundheitsfachkraft und Besuchsgrund, Terminstatus, Medizinische Dokumente des Patienten, von der Gesundheitsfachkraft ausgefüllte Felder;
- Die **Nutzungs- und Verbindungsinformationen im Zusammenhang mit Ihrer Nutzung der Doctolib-Dienste (z.B. Protokolldateien)**

EMPFÄNGER DER DATEN::

- Gesundheitsfachkräfte;
- Assistenten (auf das Berufsgeheimnis verpflichtet im Sinne von § 203 StGB);

AUFBEWAHRUNGSDAUER:

Aufgaben werden gespeichert, bis sie erledigt markiert sind. Nach ‘Erledigt’-Markierung werden Aufgaben ein Jahr aufbewahrt und dann gelöscht.

BESONDERE BEDINGUNGEN FÜR DIE VERARBEITUNG

„BEREITSTELLUNG EINES MESSAGING-DIENSTES“

ZWECKE DER VERARBEITUNG:

Der Messaging-Dienst soll eine bessere Koordinierung der Behandlung gewährleisten, indem er den Nutzern die Kommunikation und den Versand von Textnachrichten, Videos, Fotos, Sprachnotizen und anderen Medien ermöglicht. Er ermöglicht sowohl Einzel- als auch Gruppendiskussionen.

- Erleichterung der Kommunikation zwischen Gesundheitsfachkräften und/oder Assistenten durch Bereitstellung eines sicheren Kanals für den Austausch per Messaging-Dienst;
- Ermöglichung des Austauschs von Dokumenten und Daten, die personenbezogene Daten von Patienten enthalten können;
- Ermöglichung für die Nutzer des Messaging-Dienstes, einen anderen Nutzer zu blockieren oder zu entsperren;
- Ermöglichung für die Nutzer des Messaging-Dienstes neue Nutzer einzuladen;
- Reporting, Debugging und Statistiken;
- Verbesserung der Dienste;
- Erstellung von Statistiken im Auftrag der Gesundheitsfachkraft;
- Anonymisierung von Daten.

RECHTSGRUNDLAGE DER VERARBEITUNG:

Es liegt in Ihrer Verantwortung, die Rechtsgrundlage vor jeder Verarbeitung zu bestimmen.

Für den Fall, dass Sie die Patientenstammdaten an eine Gesundheitsfachkraft weitergeben, die nicht zum Behandlungsteam des Patienten gehört, müssen Sie zuvor die Einwilligung des Patienten einholen.

BETROFFENE PERSONEN:

- Patienten;
- Gesundheitsfachkräfte und Assistenten mit oder ohne Doctolib-Nutzerkonto;
- Nutzer des Doctolib Connect Netzwerks, welche Sender oder Empfänger von Nachrichten sein können.

KATEGORIEN VON PERSONENBEZOGENEN DATEN:

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

- Identifikationsdaten;
- Kontaktdaten;
- Medizinische oder familiäre Informationen, Allergien;
- Untersuchungsdaten;
- Verschreibungsdaten;
- Biometrische und biologische Daten;
- Daten in Bezug auf das Behandlungsteam;
- Medizinische Bilder;
- Fotos, Videos;
- Sprachnotizen;
- Für Videos und Sprachanrufe: Video-/Sprachstream, der die Übermittlung zwischen den Gesundheitsfachkräften oder Assistenten ermöglicht;
- Nutzungs- und Verbindungsinformationen im Zusammenhang mit Ihrer Nutzung des Nachrichtendienstes (z.B. Protokolldateien).

EMPFÄNGER DER DATEN:

- Gesundheitsfachkräfte oder Assistenten mit einem Nutzerkonto;
- Gesundheitsfachkräfte oder Assistenten ohne Nutzerkonto (Nutzer des Doctolib Connect Netzwerks);

AUFBEWAHRUNGSDAUER:

Spezifische von Ihnen geforderte Aufbewahrungsdauern müssen Doctolib mitgeteilt werden.

Außer in den Fällen, in denen Sie die Funktion “Konversation aufbewahren” in den besonderen Einstellungen jeder Konversation aktiviert haben, werden alle Nachrichten nach dreißig (30) Tagen gelöscht.

Falls Sie eine solche Option aktiviert haben, werden alle von Ihnen erstellten Inhalte, die sich auf die Konversation beziehen, für einen unbegrenzten Zeitraum aufbewahrt, d.h. bis Sie sich entscheiden, Ihr Konto zu löschen, oder bis diese Aufbewahrungsoption deaktiviert wird.

Bei Vertragsende und/oder auf Ihr formelles Verlangen hin verpflichtet sich Doctolib außerdem, die nutzergenerierten Inhalte zu löschen, ohne eine Kopie aufzubewahren, vorbehaltlich gesetzlicher Aufbewahrungspflichten, denen Doctolib unterliegt.

DATENEXPORTSPEZIFISCHE BEDINGUNGEN FÜR DIE VERARBEITUNG VON NACHRICHTEN:

Sie können die nutzergenerierten Daten, die am Ende der Vertragslaufzeit noch auf den Diensten gespeichert sind, exportieren, indem Sie direkt den (im Netzwerk-Feed geteilten) Beitrag oder die Konversation über die in der App verfügbare Exportfunktion exportieren.

DATENLÖSCHUNG:

Nach Beendigung des Vertrages und/oder auf Ihr formelles Verlangen hin verpflichtet sich Doctolib, die vom Nutzer erstellten Inhalte zu vernichten, ohne eine Kopie aufzubewahren, vorbehaltlich gesetzlicher Aufbewahrungspflichten, denen Doctolib unterliegt.

BESONDERE BEDINGUNGEN FÜR DIE VERARBEITUNG

„VERWALTUNG VON DOKUMENTEN UND FORMULAREN“

.

ZWECKE DER VERARBEITUNG:

- Ermöglichung der Erstellung und Formatierung von Dokumenten;
- Ermöglichung (i) des Versands von Dokumenten durch den Patienten, einen autorisierten Angehörigen oder durch Sie und (ii) des Empfangs von Dokumenten durch den Patienten, einen autorisierten Angehörigen, Sie und/oder einen anderen Ihnen ausgewählten Empfänger;
- Ermöglichung, dass (i) Sie den Patienten oder einen befugten Angehörigen im Vorfeld und zur Erleichterung der Vorbereitung des Termins auffordert, ein oder mehrere Dokumente zu senden oder bestimmte Fragen zum Patienten zu beantworten, (ii) diese Dokumente oder Formulare bearbeitet werden, (iii) diese Dokumente und Formulare von Ihnen empfangen und gespeichert werden;
- Ermöglichung der einfachen elektronischen Signatur von Dokumenten;
- Berichterstattung, Debugging und Statistiken;
- Verbesserung der Dienste;
- Erstellung von Statistiken im Auftrag der Nutzer/Abonnenten;
- Anonymisierung von Daten.

RECHTSGRUNDLAGE DER VERARBEITUNG:

Es liegt in Ihrer Verantwortung, die Rechtsgrundlage vor jeder Verarbeitung zu bestimmen.

BETROFFENE PERSONEN :

- Patienten und/oder Angehörige;
- Gesundheitsfachkraft mit oder ohne Doctolib-Nutzerkonto.

KATEGORIEN VON PERSONENBEZOGENEN DATEN:

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

- Identifikationsdaten;
- Sozialversicherungsnummer;
- Kontaktdaten;
- Daten zu Lebensgewohnheiten, z.B. körperliche Betätigung, Diät und Essverhalten, etc.;
- Medizinische und familiäre Vorgeschichte, Allergien ;
- Untersuchungsdaten;
- Verschreibungsdaten;
- Biometrische und biologische Daten;
- Daten über das Behandlungsteam;
- Medizinische Bildgebung;
- Nutzungs- und Verbindungsinformationen im Zusammenhang mit Ihrer Nutzung der Doctolib-Dienste.

Hinsichtlich der Dokumente und Informationen, die vom Patienten oder einem befugten Angehörigen zur Vorbereitung eines Termins angefordert werden, werden Sie daran erinnert, dass Sie verpflichtet sind, den Grundsatz der Verhältnismäßigkeit oder Datenminimierung zu beachten und somit nur die Dokumente oder Informationen anzufordern, die für die Behandlung des Patienten unbedingt erforderlich sind.

EMPFÄNGER DER DATEN:

- Gesundheitsfachkräfte;
- Patienten und ihre befugten Angehörigen.

Wenn die Gesundheitsfachkraft ein Dokument oder eine Information im Rahmen der Vorbereitung oder Nachbereitung eines für den Patienten vereinbarten Termins durch einen Angehörigen weitergibt, stellt die Gesundheitsfachkraft in eigener Verantwortung sicher, dass die ärztliche Schweigepflicht im Rahmen dieser Weitergabe eingehalten wird. So stellt die Gesundheitsfachkraft sicher, dass (i) der Angehörige gesetzlich oder vertraglich berechtigt ist, den Patienten zu vertreten und auf dessen Gesundheitsdaten zuzugreifen, und/oder (ii) die Zustimmung des Patienten zur Weitergabe seiner Gesundheitsdaten an den Angehörigen, der in seinem Namen einen Termin vereinbart hat, eingeholt wird.

AUFBEWAHRUNGSDAUER:

Spezifische von Ihnen geforderte Aufbewahrungsdauern müssen Doctolib mitgeteilt werden.

Sofern Sie keine besonderen Weisungen erteilen, werden die vom Nutzer auf der Doctolib-Plattform gespeicherten Dokumente gemäß den Bedingungen der einzelnen Doctolib-Dienste oder bis zu ihrer Löschung durch den Nutzer gespeichert.

Ungeachtet des Vorstehenden und vorbehaltlich der Einholung der ausdrücklichen Einwilligung des Patienten oder eines befugten Angehörigen durch Doctolib, erteilen Sie Doctolib ausdrücklich die Erlaubnis, in seiner Funktion als Verantwortlicher, die Speicherung von Dokumenten und Formularen im Bereich „Meine Dokumente“ zu ermöglichen, um (i) dem Patienten jederzeit die Einsicht in die über sein Doctolib-Konto gesendeten oder empfangenen Dokumente und Formulare zu ermöglichen und (ii) dem Patienten die Wiederverwendung dieser Dokumente und Informationen bei der Vorbereitung zukünftiger Termine auf Doctolib zu gestatten. Die Dokumente werden solange aufbewahrt, bis der Patient das Dokument oder sein Konto löscht oder seine Einwilligung zur Speicherung der Dokumente im Bereich „Meine Dokumente“ widerruft.

BESONDERE BEDINGUNGEN FÜR DIE VERARBEITUNG

„AUFNAHMEMANAGEMENT-DIENST“

ZWECKE DER VERARBEITUNG:

- Ermöglicht Ihnen die Verwaltung von Aufnahmeunterlagen von Patienten und ihren Angehörigen;
- Ermöglicht das Ausfüllen der Aufnahmeunterlagen online durch den Patienten oder den Nutzer des Aufnahmemanagementsystems;
- Ermöglicht Ihnen dem Patienten oder dem Nutzer des Aufnahmemanagementsystems und seinen Angehörigen Informationen über seine Ankunft in der Gesundheitseinrichtung und die Vorbereitung der Aufnahme zu übermitteln;
- Versendung von SMS, E-Mails und Push-Benachrichtigungen (i) für Bestätigungen, Stornierungen oder Terminerinnerungen; (ii) Informationen über die Übersendung von vorbereitenden Unterlagen und Fragebögen; (iii) Informationen und Erinnerungen bezüglich unvollständiger vorbereitender Unterlagen und Fragebögen; (iv) Informationen in Bezug auf die Versorgung der Patienten und/oder Angehörigen oder in Bezug auf die Organisation der Untersuchung oder des Krankenhausaufenthalts oder auf die Erstellung ihrer Aufnahmeakte;
- Ermöglicht den Patienten, Ihnen Dokumente und Fragebögen zu senden, die für das medizinische oder administrative Aufnahmemanagement für erforderlich gehalten werden;
- Reporting, Debugging und Statistiken;
- Verbesserung der Dienste;
- Erstellung von Statistiken im Auftrag der Gesundheitsfachkraft;
- Anonymisierung von Daten.

RECHTSGRUNDLAGE DER VERARBEITUNG:

Es liegt in Ihrer Verantwortung, die Rechtsgrundlage vor jeder Verarbeitung zu bestimmen.

BETROFFENE PERSONEN:

- Patienten und ihre Angehörige;
- Assistenten.

KATEGORIEN VON PERSONENBEZOGENEN DATEN:
Die folgenden Daten werden grundsätzlich als relevant für die oben genannten Zwecke angesehen:

- Identifikations- und Kontaktdaten;
- Medizinische und familiäre Vorgeschichte, Allergien;
- Untersuchungsdaten;
- Verschreibungsdaten;
- Verschreibungshistorie
- Biometrische und biologische Daten;
- Daten über das Behandlungsteam;
- Alle in den übermittelten Dokumenten enthaltene Informationen;
- Nutzungs- und Verbindungsinformationen im Zusammenhang mit Ihrer Nutzung der Doctolib-Dienste (z.B. Protokolldateien).

EMPFÄNGER DER DATEN :

- Gesundheitsfachkräfte;
- Assistenten (auf das Berufsgeheimnis verpflichtet im Sinne von § 203 StGB);
- Befugte Mitarbeiter von Doctolib;

AUFBEWAHRUNGSDAUER:

Spezifische von Ihnen geforderte Aufbewahrungsdauern müssen Doctolib mitgeteilt werden.

BESONDERE BEDINGUNGEN FÜR DIE VERARBEITUNG

„PRIVATES ORGANISATIONSNETZWERK“

(DOCTOLIB CONNECT FÜR ORGANISATIONEN)

ZWECKE DER VERARBEITUNG:

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

Doctolib kann auch Berichte, Fehlerbehebungen und Statistiken für Ihr Konto erstellen und Dienste verbessern.

RECHTSGRUNDLAGE:

Es liegt in Ihrer Verantwortung, die Rechtsgrundlage vor jeder Verarbeitung zu bestimmen.

BETROFFENE PERSONEN:

- Patienten und ihre Angehörigen;
- Gesundheitsfachkräfte oder Assistenten mit einem Nutzerkonto.

KATEGORIEN VON PERSONENBEZOGENE DATEN :

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

- Identifikationsdaten, berufliche Daten und Kontaktdaten der Gesundheitsfachkräfte und Assistenten, die zur Gesundheitseinrichtung des Verantwortlichen der Verarbeitung gehören;
- Medizinische und familiäre Vorgeschichte, Allergien;
- Untersuchungsdaten;
- Verschreibungsdaten;
- Biometrische und biologische Daten;
- Daten des Gesundheitsteams;
- Medizinische Bildgebung;
- Fotos;
- Abläufe für Video- und Sprachanrufe;
- die Nutzungs- und Verbindungsinformationen im Zusammenhang mit Ihrer Nutzung des Doctolib-Dienstes (z.B. Protokolldateien).

EMPFÄNGER DER DATEN:

- Gesundheitsfachkräfte und Assistenten mit einem Nutzerkonto;

AUFBEWAHRUNGSDAUER:

Spezifische von Ihnen geforderte Aufbewahrungsdauern müssen Doctolib mitgeteilt werden.

DATENLÖSCHUNG:

Nach Beendigung des Vertrags und/oder auf Ihr formelles Verlangen hin verpflichtet sich Doctolib außerdem, die nutzergenerierten Inhalte zu löschen, ohne eine Kopie aufzubewahren, vorbehaltlich der gesetzlichen Aufbewahrungspflichten, denen Doctolib unterliegen würde.

BESONDERE BEDINGUNGEN FÜR DIE VERARBEITUNG

„KI-TELEFONASSISTENT“

ZWECK DER VERARBEITUNG:

- Bereitstellen eines KI-Telefonassistenten, der insbesondere Folgendes ermöglicht:
    - das Führen, Transkribieren und Aufzeichnen von Telefongesprächen zwischen Patienten der Gesundheitsfachkräfte, sowie sonstigen Anrufenden und dem KI-Telefonassistenten;
    - das Anzeigen von aus den oben genannten Transkriptionen generierten Mitteilungen im Patientenmitteilungsdienst und das Generieren von entsprechenden Kalendereinträgen;
    - Verbesserungen der Dienste, Statistiken und Anonymisierung von Daten
    - Erstellung von Statistiken im Auftrag von Nutzer/Abonnent

RECHTSGRUNDLAGE FÜR DIE VERARBEITUNG:

Es liegt in Ihrer Verantwortung, die Rechtsgrundlage vor jeder Verarbeitung zu bestimmen.

BETROFFENE PERSONEN:

- Patienten und Angehörige;
- sonstige Personen, die die Gesundheitseinrichtung anrufen.

KATEGORIEN VON PERSONENBEZOGENEN DATEN:

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

- Sprachaufzeichnungen der Äußerungen der Anrufenden
- In der Audioaufnahme enthaltene Daten:
    - der Name;
    - das Geburtsdatum;
    - die Krankenversicherung;
    - der Grund der Kontaktaufnahme (z.B. Anlass für den Termin, Dauer und Art der Symptome);
    - Verschreibungsdaten;
    - Medizinische und/oder familiäre Informationen, Allergien;
    - Biometrische und biologische Daten;
    - und/oder sonstige personenbezogene Daten, die die Anrufenden freiwillig kommunizieren
- Telefonnummern
- Transkription der Audioaufnahme
- Nutzungs- und Verbindungsinformationen im Zusammenhang mit Ihrer Nutzung der Doctolib-Dienste (z.B. Protokolldateien).

EMPFÄNGER DER DATEN:

- Gesundheitsfachkräfte;
- Assistenten (auf das Berufsgeheimnis verpflichtet im Sinne von § 203 StGB).

AUFBEWAHRUNGSDAUER:

Sofern der Abonnent Doctolib nicht schriftlich eine anderslautende Weisung erteilt, wird Doctolib die Tonaufnahmen zu den Transkriptionen für 60 Tage nach der jeweiligen Konversation mit dem KI-Telefonassistenten aufbewahren, damit der Abonnent die Transkriptionen bestätigen und/oder gegebenenfalls ändern kann.

Die aus den Transkriptionen resultierenden Nachrichten im Patientenmitteilungsdienst werden gemäß den für diesen Service festgelegten Aufbewahrungsfrist gespeichert.

Nach Ablauf der jeweiligen Aufbewahrungsfrist erfolgt die Löschung der Daten.

BESONDERE BEDINGUNGEN FÜR DIE VERARBEITUNG

„KI-SPRECHSTUNDENASSISTENT“

ZWECKE DER VERARBEITUNG:

- Bereitstellen eines KI-Sprechstundenassistenten, der insbesondere Folgendes ermöglicht:
  - die Aufzeichnung und Transkription von Gesprächen zwischen Gesundheitsfachkräften und Patienten;
  - das Generieren von Vorschlägen für Notizen aus der Transkription und
  - nach der Überprüfung durch die Gesundheitsfachkraft, die Patientenakte mit strukturierten Vorschlägen zu aktualisieren;
  - Sprachaufzeichnungen einer Diktierfunktion zu transkribieren
- Berichterstattung, Fehlerbehebung und Statistiken;
- Verbesserung der Dienste;
- Erstellung von Statistiken im Auftrag des Abonnenten/Nutzers;
- Produktverbesserung; Statistiken und Anonymisierung.

RECHTSGRUNDLAGE FÜR DIE VERARBEITUNG:

Es liegt in Ihrer Verantwortung, die Rechtsgrundlage vor jeder Verarbeitung zu bestimmen.

BETROFFENE PERSONEN:

- Patienten oder Angehörige,
- gegebenenfalls Begleitpersonen des Patienten,
- Gesundheitsfachkräfte (Nutzer*innen).

KATEGORIEN VON PERSONENBEZOGENEN DATEN:

Um die Menge der verarbeiteten personenbezogenen Daten und Gesundheitsdaten zu minimieren, müssen Sie sicherstellen, dass Sie nur die für diese Verarbeitung personenbezogenen Daten erforderlichen Informationen erheben und verarbeiten.
Grundsätzlich gelten die folgenden Daten für die oben genannten Zwecke als relevant:

- Stimme und Daten in der Audioaufzeichnung;
- Transkription der Audioaufzeichnung;
- Gesundheitsdaten von Patienten, insbesondere Daten aus der Patientenakte betreffend die Behandlung in Ihrer Gesundheitseinrichtung: Vorerkrankungen, Medikation, Angaben zum körperlichen Allgemeinzustand, Anamnesen, Diagnosen, Behandlungsverläufe und -dokumentation, Rezepte, zugehörige Korrespondenz mit anderen Gesundheitseinrichtungen, abrechnungsrelevante Informationen;
- Die Nutzungs- und Verbindungsinformationen im Zusammenhang mit Ihrer Nutzung des Doctolib-Dienstes (z.B. Protokolldateien)
- Sprachaufzeichnung.

EMPFÄNGER DER DATEN:

- Gesundheitsfachkräfte;
- Assistenten (auf das Berufsgeheimnis verpflichtet im Sinne von § 203 StGB);

AUFBEWAHRUNGSDAUER:

Die Vorschläge für Notizen und Transkriptionen werden nach der Konsultation 48 Stunden lang aufbewahrt, damit Sie die Vorschläge bestätigen oder bei Bedarf ändern können. Sobald die Informationen aus den Vorschlägen in die Patientenakte eingetragen wurden, werden die Daten gemäß der für die Praxismanagement-Software festgelegten Aufbewahrungsfrist aufbewahrt.

Nach Ablauf der jeweiligen Aufbewahrungsfrist erfolgt die Löschung der Daten.

BESONDERE BEDINGUNGEN FÜR DIE VERARBEITUNG

„BEHANDLUNGS- UND ABRECHNUNGSMANAGEMENT“

ZWECKE DER VERARBEITUNG:

- Datenmigration aus dem Alt-System in das Doctolib PVS;
- Bereitstellung des Behandlungs- und Abrechnungsmanagement inklusive der jeweils abonnierten Dienste, zur Unterstützung der allgemeinen administrativen Vorgänge in der Gesundheitseinrichtung;
- Kontenverwaltung: Konfiguration der Nutzerkonten und Nutzerberechtigungen;
- Technischer Support und Hilfe: Gewährleistung von technischem Support, Wartung und Bearbeitung von Nutzeranfragen, Beratung, Hosting und andere den Nutzern angebotene Dienste;
- Support bezüglich personenbezogener Daten: Hilfe bei der Verletzung des Schutzes von personenbezogenen und Gesundheitsdaten, Unterstützung bei der Erstellung von Datenschutz-Folgenabschätzungen, Unterstützung bei der Beantwortung von Betroffenenanfragen;
- Überweisung von Patienten an eine Gesundheitsfachkraft;
- Reporting, Debugging und Statistiken;
- Produktverbesserung, Statistiken und Anonymisierung.

RECHTSGRUNDLAGE FÜR DIE VERARBEITUNG:

Es liegt in Ihrer Verantwortung, die Rechtsgrundlage vor jeder Verarbeitung zu bestimmen.

BETROFFENE PERSONEN:

- Abonnent und Nutzer
- Patienten

KATEGORIEN VON PERSONENBEZOGENEN DATEN:

Um die Menge der verarbeiteten personenbezogenen Daten so gering wie möglich zu halten, müssen Sie sicherstellen, dass Sie nur Daten erheben und verwenden, die für die Erreichung des jeweiligen Verarbeitungszwecks, insbesondere für die medizinische und administrative Verwaltung Ihres Patientenstamms, erforderlich und notwendig sind.

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

- Identität und Kontaktdaten der Gesundheitsfachkräfte: Geschlecht, Nachname, Vorname, Telefonnummer und E-Mail-Adresse, Postanschrift, Foto, Unterschrift, Personalausweis oder Pass.
- Berufsbezogene Daten: Fotografie, Fachrichtung, Angaben zur Behandlung, Werdegang der Gesundheitsfachkraft, angebotene Besuchsgründe, Sprechzeiten, Besonderheiten in Verbindung mit dem Behandlungsort.
- Nutzungs- und Verbindungsinformationen im Zusammenhang mit Ihrer Nutzung der Doctolib-Dienste.
- Identität und Kontaktdaten der Patienten: Geschlecht, Nachname, Vorname, Telefonnummer und E-Mail-Adresse, Postanschrift, Foto, Unterschrift, Gesundheitskarte, Versicherungsstatus
- Gesundheitsdaten von Patienten, insbesondere betreffend die Behandlung in Ihrer Gesundheitseinrichtung: Vorerkrankungen, Medikation, Angaben zum körperlichen Allgemeinzustand, Anamnesen, Diagnosen, Behandlungsverläufe und -dokumentation, Rezepte, zugehörige Korrespondenz mit anderen Gesundheitseinrichtungen, abrechnungsrelevante Informationen.

EMPFÄNGER DER DATEN:

- Gesundheitsfachkräfte;
- Assistenten (auf das Berufsgeheimnis verpflichtet im Sinne von § 203 StGB);

AUFBEWAHRUNGSDAUER:

Spezifische von Ihnen geforderte Aufbewahrungsdauern müssen Doctolib mitgeteilt werden.

Sofern Sie keine besonderen Weisungen erteilen, werden die vom Nutzer auf der Doctolib-Plattform gespeicherten Dokumente gemäß den Bedingungen der einzelnen Doctolib-Dienste oder bis zu ihrer Löschung durch den Nutzer gespeichert.
Nach Ablauf der jeweiligen Aufbewahrungsfrist erfolgt die Löschung der Daten.

ALLGEMEINE TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN

[Hinweis: Diese technischen und organisatorischen Maßnahmen sind standardmäßig anwendbar (außer in dem Fall, in dem ein Konnektor zwischen der Doctolib-Plattform und Informationssystemen Dritter eingerichtet wird). Weitere Informationen zu den angewendeten Maßnahmen finden Sie im Vertrag.]

SICHERHEITSZERTIFIZIERUNGEN

Nachfolgend sind die bestehende Sicherheitszertifizierungen von Doctolib aufgelistet:

- Hébergement de Données de Santé (Hosting von Gesundheitsdaten)
- ISO/IEC 27001:2022
- ISO/IEC 27701:2019
- BSI C5
- TÜV (Videosprechstunde)

PRODUKTSICHERHEIT

- Zwei-Faktor-Authentifizierung: Bei jeder Anmeldung von einem neuen Gerät muss der Nutzer sein Passwort und einen zweiten Faktor (2FA) eingeben, der per E-Mail, SMS oder über eine Einmalpasswort-App (z. B. Authenticator App) bezogen wird.

- Passwortrichtlinie: Das Passwort muss aus mindestens 8 Zeichen bestehen (Zahlen, Symbole, Buchstaben, Großbuchstaben); gebräuchliche Passwörter sind verboten (z. B. Login, Name, einfache Zahlenfolgen). Das Passwort muss einen dynamisch berechneten Komplexitätstest bestehen, der die Schwierigkeit der Entschlüsselung analysiert. Um Zugriff auf die Dienste zu erhalten, muss der Nutzer seine Login-ID und sein Passwort verwenden.

- Schutz von Nutzersitzungen:
  Offene Sitzungen können auf zwei Arten entsperrt werden:
  1. Durch Passwort (die Sitzung läuft dann automatisch ab).
  2. Durch PIN-Code:
     - Einfache PIN-Codes sind verboten.
     - Die Sitzung wird nach 1 Stunde Inaktivität automatisch mit dem PIN-Code gesperrt.
     - Die Sitzung läuft jede Nacht automatisch ab.

- Wiederherstellungsprozess:
  Konten können auf zwei Wegen wiederhergestellt werden:
  1. Passwort-Reset per E-Mail.
  2. Passwort-Reset per SMS mit Unterstützung von Doctolib nach Überprüfung der Kontoinformationen.

  Die erfolgreiche Wiederherstellung führt zur automatischen Ungültigkeit aller aktiven Sitzungen.

- Granulares Zugriffsmanagement: Administratoren können jedem Nutzer spezifische Rechte innerhalb ihrer Organisation zuweisen.

- Nachvollziehbarkeit von Aktivitäten: Die Aktivitäten der verschiedenen Nutzer werden protokolliert. Sensible Aktivitäten (z. B. Änderung von Kalenderzugriffen, Anlage von Administrator-Konten) lösen Sicherheitsbenachrichtigungen aus.

- Schutz vor Kontodiebstahl: Erfolgreiche Logins von neuen Geräten werden dem Nutzer per E-Mail mitgeteilt.

PLATTFORMSICHERHEIT

- Anwendungs-Workloads und Daten werden sicher in Europa gespeichert.
- Betriebssysteme (insbesondere Linux) und Middleware-Software werden regelmäßig aktualisiert; sicherheitskritische Hotfixes werden umgehend eingespielt.

- Doctolib setzt Linux-Betriebssysteme mit minimal gehärteten Kerneln und Konfigurationen ein.
- Strikte Netzwerksegmentierung zwischen Produktions- und Nicht-Produktionsumgebungen durch voneinander isolierte Umgebungen.
- Eingehender Anwendungstraffic wird durch eine Web Application Firewall (Cloudflare) und Ingress-Load-Balancer geschützt; ausgehender Anwendungstraffic wird durch einen HTTP-Proxy mit Whitelisting abgesichert.
- Doctolib nutzt Cloudflare zum Schutz vor volumetrischen DDoS-Angriffen.
- Sicherheitsüberwachung: Permanente Überwachung auf bekannte und neue Bedrohungen, Schwachstellen oder Angriffe.
- Nachvollziehbarkeit: Jede Aktivität wird protokolliert, überwacht und bei sicherheitsrelevanten Vorfällen erfolgt eine Benachrichtigung.
- Zertifizierte Rechenzentren: HDS, ISO 27001, BSI C5 Typ 2

VERFÜGBARKEIT

- Die Service-Architektur von Doctolib ist auf hohe Verfügbarkeit und Ausfallsicherheit ausgelegt. Doctolib betreibt zwei vollständig redundante Datenspeicher: ein primäres Cluster in der AWS-Region Frankfurt und ein sekundäres Cluster in der AWS-Region Paris.
- Kritische Systeme sind redundant ausgelegt und oft über mehrere Verfügbarkeitszonen verteilt, um einen unterbrechungsfreien Betrieb sicherzustellen.
- Im Falle einer regionalen Störung sieht der Notfallwiederherstellungsplan detaillierte Maßnahmen vor, um die volle Funktionalität innerhalb von 30 Minuten (RTO: Recovery Time Objective) wiederherzustellen und Ausfallzeiten sowie Unterbrechungen zu minimieren.
- Zur Sicherstellung der Betriebsbereitschaft führt das Team mindestens zweimal jährlich umfassende Tests zur Geschäftskontinuität und Notfallwiederherstellung durch.
- Bei einem größeren Ausfall in der primären Region kann Doctolib nahtlos innerhalb von weniger als 10 Minuten auf das sekundäre Datenbank-Cluster umschalten, um eine minimale Beeinträchtigung der Services und die Aufrechterhaltung der Geschäftskontinuität zu gewährleisten.

DATENVERSCHLÜSSELUNG

Verschlüsselung der Kommunikation:

- Sämtliche Daten, die über öffentliche Netzwerke übertragen werden, sind verschlüsselt. Es wird das Industriestandard-Protokoll TLS 1.2 in Kombination mit einem sicheren 4096-Bit-SSL-Zertifikat einer renommierten Zertifizierungsstelle verwendet.
- Der Videosprechstunden-Dienst von Doctolib erfüllt höchste Sicherheitsstandards und stellt die Ende-zu-Ende-Verschlüsselung sowohl für Video- als auch für Audio-Kommunikation sicher (ausschließlich während der Übertragung). Video-Sprechstunden werden niemals über die Server von Doctolib übertragen oder gespeichert, sodass vertrauliche Interaktionen zwischen Patient und Arzt privat bleiben.

Datenspeicherung:

- Zum Schutz ruhender Daten kommt ein zweistufiges Verschlüsselungsmodell zum Einsatz, das starke kryptografische Standards mit Leistungs- und Geschäftsanforderungen in Einklang bringt.
- Basisschutz für alle ruhenden Daten: Die erste Ebene der Verschlüsselung wird universell auf sämtliche von Doctolib gespeicherten Daten angewendet, sodass jegliche Daten – unabhängig davon, ob sie gesundheitsbezogen sind oder nicht – auf physischer Speicherebene verschlüsselt werden. Diese Basisschicht wird durch die Cloud-Infrastruktur mittels AES-256 bereitgestellt. Die Verschlüsselung erfolgt direkt auf dem Speichermedium und schützt sämtliche Daten vor unbefugtem Zugriff auf Hardwareebene. Das Schlüsselmanagement erfolgt separat, die Master-Keys werden sicher in einem Hardware Security Module (HSM) von Evidian verwahrt.
- Zweite Verschlüsselungsebene für Gesundheitsdaten: Diese Ebene erzwingt eine AES-256-Server-seitige Verschlüsselung (entweder auf Datenbank-Spaltenebene oder auf Datei-Ebene). Dadurch bleiben verschlüsselte Daten auch im Fall eines Datenbankzugriffs ohne die entsprechenden Entschlüsselungsschlüssel unzugänglich. Die Verschlüsselungsschlüssel werden sicher in einem virtuellen Hardware Security Module (HSM) gespeichert, was den Zugriff streng reglementiert, auditierbar und von der Anwendungsumgebung isoliert, um das Risiko einer unbefugten Schlüsselverwendung zu minimieren.

ZUGRIFFSKONTROLLE

- Doctolib setzt ein Zero-Trust-Sicherheitsmodell ein, um einen umfassenden Schutz aller von Mitarbeitenden und Dienstleistern genutzten Backoffice-Anwendungen zu gewährleisten. Der Zugang zu diesen Anwendungen erfolgt über individuelle Konten, die per Single Sign-On (SSO) verwaltet und durch verpflichtende Zwei-Faktor-Authentifizierung (2FA) abgesichert werden.
- Im Einklang mit dem Least-Privilege-Prinzip wird der Zugriff auf die Datenbank sorgfältig gesteuert. Es existieren mehrere Konten mit unterschiedlichen Berechtigungsstufen, abgestimmt auf die jeweiligen Anforderungen des Infrastrukturteams. Für privilegierte Konten gilt das Vier-Augen-Prinzip: Aktionen müssen vor Durchführung von einer weiteren Person oder dem Sicherheitsteam validiert werden.
- Darüber hinaus wird sichergestellt, dass Zugriffsrechte umgehend angepasst werden, wenn sich die Aufgaben eines Nutzers ändern, um das Least-Privilege-Modell konsequent einzuhalten.
- Der Zugriff auf personenbezogene Daten (PII) zu Supportzwecken ist streng reguliert. Jeder Zugriff erfordert eine nachvollziehbare Supportanfrage, und es wird automatisch eine Benachrichtigung an das Sicherheitsteam ausgelöst. Dieser Prozess wird durch ein internes Tool namens Patient Privacy Patrol unterstützt.

ANWENDUNGSSICHERHEIT

- Security and Privacy by Design: Sicherheit und Datenschutz werden bei Doctolib bereits frühzeitig im Entwicklungsprozess durch eine "Shift-left"-Strategie berücksichtigt und von Anfang an in die Arbeitsabläufe von Engineering und Produktmanagement integriert.
- Richtlinien für sichere Entwicklung und Schulungen: Die Richtlinien für die sichere Entwicklung bei Doctolib orientieren sich an den OWASP-Standards und sind auf die verwendeten Programmiersprachen, Frameworks und die Architektur des Unternehmens zugeschnitten.
- Code-Review und Änderungsmanagement: Jede Änderung am Anwendungscode wird durch das Quellcodeverwaltungstool (z. B. Github) nachverfolgt. Der Änderungsprozess basiert technisch auf dokumentierten Änderungen, die im Vier-Augen-Prinzip freigegeben werden.
- Nicht-Regressionstests: Die Doctolib CI/CD-Pipeline umfasst rund 50.000 Unit- und End-to-End-Tests sowie Feature-Schalter und ermöglicht einen schnellen Rollback bei Bedarf.
- Management von Drittanbieter-Bibliotheken: Alle externen Bibliotheken, die in den Doctolib-Quellcode integriert werden, unterliegen einer strengen Überwachung und Verwaltung, um Risiken aus Supply-Chain-Schwachstellen und Schadcode zu minimieren.
- Statische Anwendungssicherheitstests (SAST): In die Continuous-Integration-Pipeline (CI) von Doctolib ist eine umfassende Suite statischer Sicherheitstest-Tools integriert.
- Bot- und Missbrauchsschutz: Doctolib nutzt IP-Reputationsscoring, CAPTCHA und Ratelimiting, um bösartige Aktivitäten zu erkennen und einzuschränken.
- Penetrationstests: Mindestens einmal jährlich werden umfassende Penetrationstests durch ein externes, spezialisiertes Unternehmen nach OWASP-Standards durchgeführt, um die Sicherheitssysteme gründlich zu überprüfen und potenzielle Schwachstellen zu identifizieren und zu beheben.
- Öffentliches Bug-Bounty-Programm: Doctolib betreibt ein dauerhaftes öffentliches Bug-Bounty-Programm, um durch das Know-how der Whitehat-Community die eigene Sicherheitslage kontinuierlich zu stärken.

PHYSISCHER ZUGANG ZU DOCTOLIB-STANDORTEN

- Die Büros von Doctolib sind alarmgesichert und mit modernsten Sicherheits- und Zutrittskontrollsystemen ausgestattet – sowohl am Eingang, in Aufzügen als auch auf Etagen mit sogenannten sensiblen Bereichen.
- Jeder autorisierte Zutritt zu den Räumlichkeiten wird protokolliert.
- Besucher können die Räumlichkeiten nur nach vorheriger Anmeldung betreten und werden stets von einem Doctolib-Mitarbeiter begleitet. Während des Besuchs werden Besucher nie unbeaufsichtigt oder alleine gelassen.
- Alle Systeme werden in lizenzierten Rechenzentren betrieben. Diese verfügen über Videoüberwachung, Sicherheitssysteme und einen Sicherheitsdienst. Nur eine kleine Gruppe speziell geschulter Doctolib-Spezialisten erhält Zugang; jeder Zutritt wird protokolliert.

Zugang für Mitarbeitende des Unternehmens:

- Alle Mitarbeitenden verfügen über einen Ausweis mit Foto, der ihnen den Zutritt zu den Räumlichkeiten entsprechend ihrer unternehmensinternen Akkreditierung ermöglicht. Die Akkreditierung richtet sich entweder nach der Rolle des Mitarbeitenden oder nach Antrag des Vorgesetzten, der von der zuständigen

Abteilung freigegeben werden muss. Das Tragen des Ausweises ist für alle Pflicht. Bei Vergessen des Ausweises muss sich der Mitarbeitende am Empfang mit einem Ausweis oder Reisepass ausweisen; nach erfolgreicher Identitätsprüfung wird ein temporärer Ausweis ausgehändigt, der spätestens am selben Tag zurückgegeben werden muss.

Anbindung an das Informationssystem der Einrichtung:
Die Anbindung an das Informationssystem der Einrichtung ist auf verschiedene Weise möglich:

- API-Connector zwischen Doctolib-Kalender und IS-Kalender
- Lokaler Connector: Der Doctolib-Kalender ermöglicht den Upload der Patientenakte aus dem IS
- IPsec-VPN zwischen Server und Doctolib (nach Verfügbarkeit)

Besondere technische und organisatorische Maßnahmen
Nur anwendbar, wenn ein Konnektor eingerichtet wurde, um die Interoperabilität zwischen der Doctolib-Plattform
und Informationssystemen Dritter zu gewährleisten

[Hinweis: Weitere Einzelheiten zu den angewendeten Maßnahmen finden Sie im Abonnementvertrag]

Systemübergreifende Interoperabilität

- Besteht ein Connector zwischen den Informationssystemen des Kunden und denen von Doctolib, werden zur Gewährleistung der Interoperabilität die über die APIs übertragenen Datenströme und Dokumente vor der Weiterleitung durch die Doctolib-Anwendung entschlüsselt.
- Doctolib stellt dem Kunden einen geheimen Schlüssel zur Verfügung, damit sich das Informationssystem des Kunden gegenüber dem Doctolib-System authentifizieren kann. Der Kunde ist für die Vertraulichkeit dieses Schlüssels und dessen Schutz nach Best-Practice-Standards verantwortlich, insbesondere für die Verschlüsselung des Schlüssels im Ruhezustand und den Zugriffsschutz.
- Der Kunde muss sicherstellen, dass sein Informationssystem zur Authentifizierung fähig ist und eine Wiederholungsmechanik (Retry-Mechanismus) implementiert.
- Bei Verdacht auf eine Kompromittierung des geheimen Schlüssels ist Doctolib unverzüglich zu benachrichtigen, um ein Verfahren zur Schlüsselerneuerung einzuleiten.
- Doctolib bietet dem Kunden an, die Nutzung des geheimen Schlüssels auf eine festgelegte Menge von festen IP-Adressen des Informationssystems zu beschränken. Entscheidet sich der Kunde gegen diese Beschränkung, gilt als vereinbart, dass im Falle einer Kompromittierung des Schlüssels Doctolib nicht für eine missbräuchliche Verwendung durch unbefugte Personen oder Systeme haftbar gemacht werden kann.
- Die API verwendet einen Keyed-Hash Message Authentication Code (HMAC), um die Authentizität und Integrität aller ausgetauschten Nachrichten zu gewährleisten. Dies stellt sicher, dass die Daten während der Übertragung geschützt und manipulationssicher bleiben.

Besondere technische und organisatorische Maßnahmen, die von Doctolib im Zusammenhang mit den Verarbeitungstätigkeiten des Messaging-Dienstes und des Privaten Organisationsnetzwerks angewendet werden

Organisatorische und administrative Maßnahmen und Kontrollen

Doctolib hat ein Informationssicherheits-Managementsystem (ISMS) implementiert und ist nach ISO 27001 sowie nach NEN 7510 (niederländischer Standard für Informationssicherheit im Gesundheitswesen) zertifiziert.

Nachrichtendaten – Datenübertragung

- Lösungen zur Risikominimierung bei der Datenübertragung sind im Security White Paper von Doctolib (https://www.siilo.com/resources/security-white-paper) beschrieben. Das White Paper erläutert im Detail den Security-by-Design-Ansatz, das Bedrohungsmodell und die eingesetzten kryptografischen Protokolle.
- Zusammengefasst verwendet Doctolib eine Ende-zu-Ende-Verschlüsselung, die mit LibSodium (einem Fork der NaCl-Krypto-Bibliothek, https://nacl.cr.yp.to/) implementiert ist. Jede Nachricht zwischen Absender und Empfänger ist durch ein Public-/Private-Key-Paar geschützt. Nur Absender und Empfänger können die Nachrichten entschlüsseln und lesen; die Authentizität jeder Nachricht kann empirisch überprüft werden. Dritte, einschließlich Doctolib und deren Mitarbeitende, können die Nachrichten niemals lesen.
- Doctolib nutzt Certificate Pinning, um sogenannte „Man-in-the-Middle"-Angriffe zu verhindern. Dabei versuchen Angreifer, den Datenverkehr zwischen den Geräten abzufangen und mitzulesen. Standardmäßige TLS v1.2-Kommunikation erfordert bereits ein gültiges SSL-Zertifikat einer vertrauenswürdigen Zertifizierungsstelle. Certificate Pinning geht noch weiter und verlangt, dass die Zertifikate nur aus einer definierten Vertrauenskette stammen dürfen. Dies schließt zahlreiche Schwachstellen aus, die mit der Verteilung von Schlüsseln im Rahmen der Zertifizierungsstellen-Infrastruktur des Internets verbunden sind.

Nachrichtendaten – ruhende Daten auf dem Endgerät

Für ruhende Daten auf dem Gerät (iPhone, iPad, Android) gelten folgende Schutzmaßnahmen:

- Sämtliches „Schlüsselmaterial" (alle kryptografischen Codes) wird – je nach Plattform – im iOS KeyChain bzw. im Android KeyStore gespeichert.
- Das gesamte "Schlüsselmaterial" ist durch einen „Master Key" verschlüsselt, der aus dem vom Nutzer gewählten PIN-Code abgeleitet wird.
- Die gesamte Datenbank ist mithilfe von SQLiteCipher verschlüsselt. Alle Nachrichten, Metadaten und Kontaktdaten werden auf diese Weise gespeichert.
- Alle empfangenen Mediendateien werden jeweils mit einem einmaligen, symmetrischen Verschlüsselungsschlüssel verschlüsselt gespeichert. Dieser Schlüssel ist über die oben genannte Datenbank zugänglich.
- Ein PIN-Code auf Anwendungsebene verhindert einen Zugriff durch Personen, die physischen Zugang zum Gerät besitzen. Dadurch werden viele Formen des Social Engineerings – z. B. das „kurze Ausleihen" des Handys – unterbunden.
- Sämtliche ausgetauschte Informationen im Messaging-Dienst werden nach 30 Tagen automatisch gelöscht. Nutzer können einzelne Nachrichten auch jederzeit manuell löschen, wenn ihnen 30 Tage zu lang erscheinen. Doctolib verzichtet bewusst auf Countdown-Timer und kurze Nachrichtenlebensdauern (z. B. Sekunden/Stunden), um keinen Druck zu erzeugen, der zu Screenshots oder unerwünschtem Verhalten beim Empfänger führen könnte.
- Wenn ein Nutzer weiß, dass sein Gerät verloren, gestohlen oder anderweitig kompromittiert wurde, kann er seine Organisation benachrichtigen (Funktion von Doctolib Connect für Organisationen). Ein Administrator kann dann die Doctolib Daten aus der Ferne vom Gerät löschen.

Nachrichtendaten – ruhende Daten auf den Servern von Doctolib

Für ruhende Daten auf den Servern von Doctolib gelten folgende Schutzmaßnahmen:

- Sämtliche Mediendateien (die über die Anwendung versendet werden und daher als sensibel gelten) werden mit einem einmaligen, symmetrischen Verschlüsselungsschlüssel gespeichert und verschlüsselt. Dieser Schlüssel wird auf keinem Server von Doctolib gespeichert. Die Schlüssel zur Entschlüsselung dieser Daten befinden sich ausschließlich auf den Geräten des Absenders und des Empfängers. Die Speicherung personenbezogener Daten auf Servern von Doctolib erfolgt entsprechend.

- Nachrichtendaten werden auf Servern in Frankfurt (Deutschland) gespeichert. Für Sicherungszwecke werden täglich automatisierte „Snapshots“ erstellt, die maximal 7 Tage gespeichert und im Ruhezustand verschlüsselt werden.

Nutzerdaten

- Nutzerdaten werden auf Servern in Dublin (Irland) gespeichert, täglich gesichert und maximal 30 Tage in einem vorkonfigurierten, im Ruhezustand verschlüsselten Bucket gespeichert.

Abgleich von Telefonnummern im Messaging-Dienst

- Doctolib ermöglicht es optional, andere Doctolib Connect-Kontakte durch Abgleich mit dem Adressbuch des Telefons zu entdecken. Entscheidet sich der Nutzer dafür, werden die Telefonnummern gehasht und über eine verschlüsselte TLS-Verbindung an den Server übertragen (erste 64 Bit des SHA1-Hashes der E.164-normalisierten Form jeder im Adressbuch gefundenen Telefonnummer).
- Es werden ausschließlich die Telefonnummern gehasht und abgeglichen. Doctolib erhält keinen Zugriff auf zugehörige Namen, E-Mail-Adressen oder andere im Adressbuch gespeicherte Informationen. Der Server von Doctolib vergleicht die Hash-Liste des Nutzers mit den bekannten Telefon-Hashes aktueller Doctolib Connect-Nutzer. Nach Rückgabe der Übereinstimmungen an den mobilen Client werden die eingereichten Hashes vom Server sofort gelöscht.

Liste der Unterauftragsverarbeiter

Um seine Dienstleistungen zu erbringen, bedient sich Doctolib Dienstleistern, die als seine Unterauftragsverarbeiter im Sinne der DSGVO handeln. Letztere dürfen nur im Rahmen und zum Zweck der unten genannten Tätigkeiten Zugang zu den von Doctolib erhobenen Personenbezogenen Daten haben. Doctolib stellt sicher, dass jeder dieser Unterauftragsverarbeiter geeignete technische und organisatorische Maßnahmen ergreift, um die Sicherheit und Vertraulichkeit der verarbeiteten Daten zu gewährleisten.

Im Falle einer Übermittlung außerhalb des Europäischen Wirtschaftsraums (wenn sich der Serverstandort außerhalb des EWR befindet) oder im Falle des Risikos einer solchen Übermittlung (wenn sich der Serverstandort innerhalb des EWR befindet, aber das Herkunftsland des Dienstleisters außerhalb des EWR liegt), nutzt Doctolib die Dienste des Auftragsverarbeiters auf der Grundlage eines gültigen Übermittlungsinstruments gemäß der DSGVO und hat zusätzliche Maßnahmen ergriffen, um ein Datenschutzniveau zu gewährleisten, das im Wesentlichen dem der DSGVO entspricht.

In Übereinstimmung mit der DSGVO und im Interesse der Transparenz teilt Doctolib im Folgenden die Liste seiner Unterauftragsverarbeiter mit.

Liste der Unterauftragsverarbeiter, die im Zusammenhang mit der Erbringung der Doctolib-Dienste eingesetzt werden, aufgeschlüsselt nach Kategorien von Haupttätigkeiten:

Datenspeicherung :

Unterauftrags-verarbeiter	Unternehmens-herkunft	Serverstandort	Art der Verarbeitung
Atos	Frankreich	Frankreich	Speichert Doctolib's Datenverschlüsselungs-Schlüssel
AWS EMEA	Muttergesellschaft: USA Vertragspartner: Irland	EU	Speicherung der Daten der Doctolib-Dienste
Cloudinary	USA	USA	Speicherung von Fotografien von Gesundheitsfachkräfte
S3NS	Frankreich	Niederlande	Speicherung der Daten für die Doctolib-Dienste

Kundendienst:

Unterauftrags-verarbeiter	Unternehmens-herkunft	Serverstandort	Art der Verarbeitung
Teamviewer	Germany	EU	Anbieter eines Fernsupports unter Aufsicht des Abonnenten/Nutzers
Microsoft	USA	EU	Speicherung von Aufzeichnungen, die im Rahmen von Supportmaßnahmen durchgeführt werden
Walkme	Israel	EU	Anzeigen und Verwalten von Inhalten in der Anwendung
Salesforce	Muttergesellschaft: USA Vertragspartner:	Frankreich	Verwalten von Kundenanfragen

	Frankreich		
Webhelp	Frankreich	Frankreich	Verwalten telefonischer Supportanfragen von Nutzern
Calendly	USA	EU	Erleichterung der Terminvereinbarung mit Nutzern/Abonnenten
Atlassian	**Muttergesellschaft: Australien Vertragspartner: Frankreich**	EU	Verwalten telefonischer Supportanfragen von Nutzern
Datadog	USA	EU	überwachung und Untersuchungs von Warnungen und Störungen

Telekommunikation:

Unterauftrags-verarbeiter	Unternehmens-herkunft	Serverstandort	Art der Verarbeitung
Iagility	Frankreich	EU	Stellt Terminerinnerungen an Patienten zu Verfügung (SMS)
Sinch	Schweden	EU	Stellt Terminerinnerungen an Patienten zu Verfügung (SMS)
Sendinblue	Frankreich	EU	Stellt Terminerinnerungen an Patienten zu Verfügung (E-Mail)
Flowmailer	Niederlande	EU	Stellt Terminerinnerungen an Patienten zu Verfügung (E-Mail)
SMSMODE (Calade Technologie)	Frankreich	EU	Stellt Terminerinnerungen an Patienten zu Verfügung (SMS)
Braze	USA	EU	Ermöglicht Kampagnen mit den Nutzer/Abonnenten zu bewerten, um den Inhalt der Kampagnen zu verbessern

Marketing:

Unterauftrags-verarbeiter	Unternehmens-herkunft	Serverstandort	Art der Verarbeitung
Guideflow	EU	EU	Hilft Doctolib Produktdemonstrationen vorzunehmen

IT-Sicherheit :

Anbieter	Unternehmens-herkunft	Serverstandort	Art der Verarbeitung
Cloudflare	USA	EU	Hilft Doctolib, sich vor Angriffen des Typs CDS und DDos zu schützen

Sonstige Anbieter:

Anbieter	Unternehmens-	Serverstandort	Art der	Art der Verarbeitung

	herkunft		beauftragten Dienstleistung	
Doctolib SAS	Frankreich	EU	Technische Infrastruktur	Zurverfügungstellung zentraler technischer Infrastruktur für die Doctolib Gruppe
Zapier	USA	USA	Automatisierung von Abläufen zwischen Webanwendungen	Ermöglicht es Doctolib, die Übertragung von Datenströmen zwischen verschiedenen Webanwendungen zu automatisieren.
Microsoft Azure	USA	EU	Suche und Diensteentwicklung	Verarbeitung und Analyse von Daten
Adyen	Niederlande	EU	Finanzen	Verwaltung von Online-Zahlungen.
Anthropic	USA	EU	Bereitstellung von LLM	Analyse und Inhaltserstellung für Zwecke der Aufgabenautomatisierung

Liste der Unterauftragsverarbeiter zur Erbringung des Messaging-Dienstes und Privaten Organisationsnetzwerks (Docotlib Connect für Organisationen) :

Unterauftrags-verarbeiter	Unternehmens-herkunft	Serverstandort	Art der beauftragten Dienstleistung	Art der Verarbeitung
AWS EMEA	Muttergesellschaft: USA Vertragsschließende Einheit : Irland	EU	Hosting	Hosting der Doctolib-Daten
Twilio	USA	Irland	VOIP Telefonie	Twilio wird verwendet, um die Doctolib In-App VOIP- (Anrufe über das Internet) und Videoanruf-Funktionalität bereitzustellen.
CM.com	Niederlande	Niederlande	Telekommunikation	Sendet SMS-Nachrichten mit einem Code an Benutzer, um zu bestätigen, dass sie tatsächlich Zugriff auf das Gerät haben, das mit einer bestimmten Nummer verbunden ist.
Firebase	USA	EU	Analyse und Crash-Reporting	Firebase wird von Doctolib für Analytics und Crash-Reporting in den mobilen iOS- und

				Android-Anwendungen verwendet, um Push-Benachrichtigungen für die Android-Anwendung zu senden und um dynamische Links für Nicht-Nutzer zu erstellen.
Sentry	USA	USA	Analyse und Crash-Reporting	Hilft Doctolib bei der Kontrolle und Verfolgung von Fehlern in der Anwendung
ZenDesk	USA	EU	Ticketing-System	Nutzer können über die Doctolib Connect Messenger App Feedback geben. Aufgrund des hohen Volumens dieser Interaktionen hat Doctolib Connectein Ticketing-System, das eine Software namens ZenDesk verwendet, um den Austausch zwischen Mitarbeitern und Nutzern zu verfolgen.
Looker	USA	USA, aber es werden keine personenbezogenen Daten in Looker's Datenbank gespeichert	Dashboarding	Doctolib verwendet Looker als Plattform für Dashboarding und BI (Business Intelligence), die sich mit dem Amazon Redshift Data Warehouse verbindet. Während keine Daten dauerhaft bei Looker gespeichert werden, werden die Daten verarbeitet und visualisiert und benötigen dafür eine laufende Verbindung und einen temporären Cache aus dem Redshift-Warehouse.