Doctolib

Datenschutz und Datensicherheit bei Doctolib

Inhaltsverzeichnis

Die Datenschutz-organisation im Überblick

Grundsätze und Prozesse

DSGVO-Konformität durch strenge Beachtung der Grundsätze für die Verarbeitung und umfassendes Datenschutzmanagement

Doctolib stellt die Beachtung der Grundsätze für die Verarbeitung personenbezogener Daten durch sorgfältige Vorabprüfung sicher. Ein umfassendes Datenschutzmanagement gewährleistet die Einhaltung sämtlicher Anforderungen der DSGVO und anderer geltender Bestimmungen.

- Das Datenschutzteam von Doctolib prüft jede Verarbeitungstätigkeit insbesondere bezüglich der Rechtsgrundlage, Zweckbindung, Datenminimierung, Speicherdauer. Jede Verarbeitungstätigkeit im Auftrag wird detailliert im Auftragsverarbeitungsvertrag (AVV) beschrieben, inklusive der technischen und organisatorischen Maßnahmen.
- Doctolib ist Auftragsverarbeiter für die Verwaltung der Nutzerkonten auf Klinik-/Krankenhausseite, die Terminverwaltung, die Videosprechstunde, den Patientenanfragen-Dienst, die Dokumentenverwaltung und die Erstellung von Statistiken für die Klinik/das Krankenhaus. Im Auftrag verarbeitete Daten werden nicht für eigene Zwecke verwendet. Die Rolle des Auftragsverarbeiters wird sorgfältig anhand der verfügbaren Abgrenzungsprinzipien ermittelt.
- Doctolib ist durch seine AGB an die Schweigepflicht gebunden (§§ 203, 204 StGB). Doctolib gibt diese Verpflichtung an die eigenen Mitarbeitenden und an die Auftragsverarbeiter weiter. Eine Entbindung von der Schweigepflicht findet nicht statt.
- Patient:innen können sich ein Doctolib-Nutzerkonto anlegen, wenn sie Termine selbst online buchen, Anfragen stellen oder Dokumente verwalten möchten. Wird Doctolib von einer Klinik/einem Krankenhaus eingesetzt, werden auch die Daten von Patient:innen ohne Doctolib-Nutzerkonto verarbeitet, da Doctolib das System zur Verwaltung der Patientenbeziehung darstellt, unabhängig davon, ob ein:e Patient:in ein Online-Nutzerkonto hat oder nicht.

- Doctolib führt eine vollständige Datenschutzdokumentation (Verzeichnis der Verarbeitungstätigkeiten etc.) und aktualisiert sie regelmäßig. Die Dokumentation wird Behörden auf Anfrage sowie externen Auditoren vorgelegt.
- Doctolib hat einen Datenschutzbeauftragten bestellt, der als Konzerndatenschutzbeauftragter für die gesamte Unternehmensgruppe die Einhaltung der Datenschutzvorschriften überwacht. Der Datenschutzbeauftragte wird durch ein Datenschutzteam unterstützt, das eng mit weiteren Teams der Rechtsabteilung sowie mit den Datensicherheitsteams von Doctolib zusammenarbeitet.
- Doctolib hat entsprechend den Datenschutzvorschriften Datenschutz-Folgenabschätzungen für Verarbeitungstätigkeiten, für die Doctolib Verantwortlicher der Datenverarbeitung ist, durchgeführt.
- Verarbeitungstätigkeiten im Auftrag sind im AVV ausführlich dargestellt. Über Verarbeitungstätigkeiten als Verantwortlicher informiert Doctolib transparent in den Datenschutzhinweisen für Gesundheitsfachkräfte. Patient:innen stehen die Datenschutzhinweise auf der Patientenwebsite von Doctolib zur Verfügung.
- Jeder von Doctolib ausgewählte Dienstleister wird einem strengen Prüfverfahren unterzogen, um zu überprüfen, ob er angemessene Sicherheits- und Datenschutzmaßnahmen ergreift, die den spezifischen Merkmalen jedes Verarbeitungsvorgangs Rechnung tragen, einschließlich der strategischen Relevanz und des Risikos, das mit dem erbrachten Dienst verbunden ist. Soweit erforderlich, ergreift Doctolib vertragliche, organisatorische und technische Maßnahmen, um sicherzustellen, dass die Dienstleister ein Schutzniveau bieten, das den Anforderungen entspricht, die Doctolib, die europäischen Datenschutzvorschriften und die Datenschutzbehörden vorgeben.

Nachweis durch Zertifikate

Doctolib durchläuft bereits seit vielen Jahren externe Zertifizierungsprogramme. Dadurch wird sichergestellt, dass die aufgebaute Datenschutzorganisation einer externen Prüfung nach festgelegten Kriterien standhält, bestimmte Verarbeitungen im Detail geprüft werden und eine kontinuierliche Verbesserung stattfindet. Doctolib absolviert – je nach Zertifikat – alle 2 oder 3 Jahre ein Vollaudit und Überwachungsaudits in den Jahren dazwischen. Die datenschutzrelevanten Zertifikate werden auf den folgenden Seiten kurz vorgestellt.

Doctolib hat das TÜV-Zertifikat „Geprüfter Datenschutz“ für das Online-Patientenportal erhalten

Das TÜV-Zertifikat „Geprüfter Datenschutz“ (TÜV Saarland) weist ein ordnungsgemäßes und funktionierendes Datenschutzsystem aus. Die Zertifizierung basiert auf den geltenden europäischen Datenschutzgesetzen und -vorschriften sowie auf internationalen Sicherheitsnormen wie ISO 27001, ISO 27002 und ISO 18028.

Bei der im 2-Jahres-Rhythmus zu durchlaufenden Rezertifizierung werden folgende Aspekte geprüft:

- Grundanforderungen an die Datenschutzorganisation (Data Protection Officer (DPO), Datengeheimnis, Meldepflichten, Verfahrens-verzeichnis, Vorabkontrolle)
- Technische und organisatorische Maßnahmen (Zutritt, Zugang, Zugriff, Verfügbarkeit bis hin zur Datentrennung)

Zwischen den Rezertifizierungen absolviert Doctolib jährlich ein Überwachungsaudit zu folgenden Punkten:

- Anforderungen an die Datensicherheit im Rahmen des Datenschutzes (Betrachtung von Netzwerk, IT- Support, Wartung, Change- und Patch-Management sowie Sicherungsverfahren)
- Datenschutzkonformität von Prozessen mit personenbezogenen Daten

TÜV SAARLAND Geprüfter Datenschutz Systemprüfung
tuev-saar.de/TK45284

Doctolib ist ISO-27001- und ISO-27701-zertifiziert

bsi.

Certificate of Registration

INFORMATION SECURITY MANAGEMENT SYSTEM - ISO/IEC 27001:2013

This is to certify that: Doctolib SA
54 Quai Charles Pasqua
Levallois-Perret
92300
France

Holds Certificate No: **IS 748307**

and operates an Information Security Management System which complies with the requirements of ISO/IEC 27001:2013 for the following scope:

Corporate Management, Information System Security, Customer Operations (including Customer Onboarding, Retention and KYC, Customer Care, Tech Services), Product & Engineering, Data Foundation, HR, Procurement, Legal, and Hosting of Personal Data. In accordance with the Statement of Applicability (SoA) version 1.2 Sept 2021.

For and on behalf of BSI:

Andrew Launn, EMEA Systems Certification Director

Original Registration Date: 2021-10-14
Latest Revision Date: 2021-10-14

Effective Date: 2021-10-14
Expiry Date: 2024-10-13

Page: 1 of 2

...making excellence a habit.

This certificate was issued electronically and remains the property of BSI and is bound by the conditions of contract.
An electronic certificate can be authenticated online.
Printed copies can be validated at www.bsigroup.com/ClientDirectory

Information and Contact: BSI, Kitemark Court, Davy Avenue, Knowlhill, Milton Keynes MK5 8PP. Tel: + 44 345 080 9000

BSI Assurance UK Limited, registered in England under number 7805321 at 389 Chiswick High Road, London W4 4AL, UK.

ISO 27001 ist die international führende Norm für Informationssicherheits-Managementsysteme und wurde von der ISO (International Organization for Standardization) entwickelt. Das Informationssicherheits-Managementsystem, oft kurz als ISMS bezeichnet, definiert Regeln und Methoden, um die Informationssicherheit in einem Unternehmen oder in einer Organisation zu gewährleisten. Das ISO-27001-Zertifikat ist die wichtigste Cybersecurity-Zertifizierung. Dieser weltweit anerkannte Standard definiert die Anforderungen, die an die Einführung, Umsetzung, Dokumentation und Verbesserung eines ISMS gestellt werden.

- Kontinuierliche Informationssicherheit: Vertraulichkeit, Integrität und Verfügbarkeit
- Risikominderung: Erfüllung international anerkannter Anforderungen

bsi.

Certificate of Registration

PRIVACY INFORMATION MANAGEMENT SYSTEM - ISO/IEC 27701:2019

This is to certify that: Doctolib SAS
54 Quai Charles Pasqua
Levallois-Perret
92300
France

Holds Certificate No: **PM 775486**

and operates a Privacy Information Management System which complies with the requirements of ISO/IEC 27701:2019 for the following scope:

Protection & Security of Personal Identifiable & Health Information (PII & PHI), Employees PII and other Sensitive Data/Information, in accordance with the Statement of Applicability (SoA) version 2.1 dated August/22/2022 for treatments (either as a Data Controller (DC) and/or as a Data Processor (DP)) related to the following processes : Information System Security & Privacy (DC), Global Customer Care (DC & DP), Product & Engineering (DC & DP), Data Foundation (DC), IT Services (DC & DP), HR (DC), Procurement (DC), Legal (DC), Finance (DC), Sales & Marketing (DC) In accordance with the Statement of Applicability (SoA) version 2.1 dated August 2022.

For and on behalf of BSI:

Andrew Launn, EMEA Systems Certification Director

Original Registration Date: 2022-11-18
Latest Revision Date: 2022-11-18

Effective Date: 2022-11-18
Expiry Date: 2025-11-17

Page: 1 of 2

...making excellence a habit.

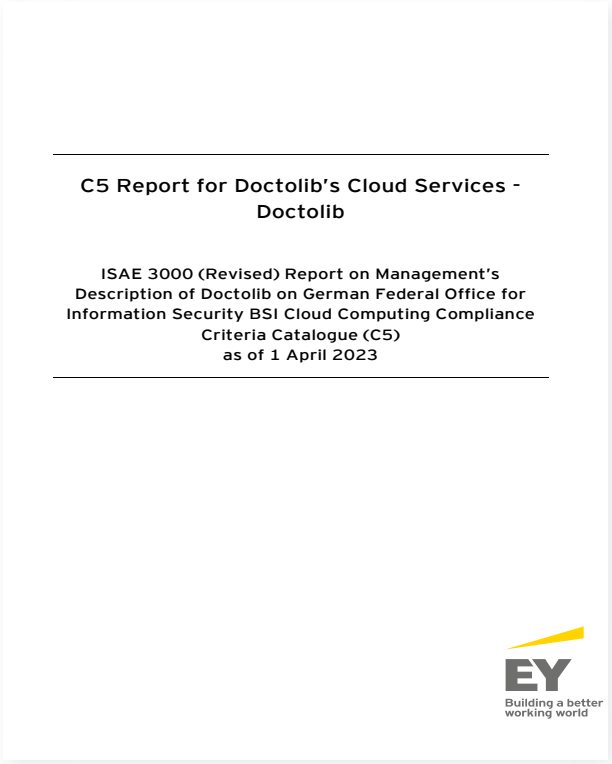
This certificate was issued electronically and remains the property of BSI and is bound by the conditions of contract.
An electronic certificate can be authenticated online.
Printed copies can be validated at www.bsigroup.com/ClientDirectory

Information and Contact: BSI, Kitemark Court, Davy Avenue, Knowlhill, Milton Keynes MK5 8PP. Tel: + 44 345 080 9000
BSI Assurance UK Limited, registered in England under number 7805321 at 389 Chiswick High Road, London W4 4AL, UK.
A Member of the BSI Group of Companies.

Die ISO-27701-Zertifizierung ist eine Datenschutzerweiterung der international anerkannten ISO-27001 Zertifizierung und beinhaltet zusätzlich Richtlinien sowie Anforderungen für die Implementierung, Aufrechterhaltung und kontinuierliche Verbesserung eines Privacy-Information-Managementsystems (PIMS).

- Ansatz der vollständigen Integration von Datensicherheit und Datenschutz
- Jährliche Überprüfung der kontinuierlichen Verbesserung von Maßnahmen und Prozessen

Doctolib hat das C5-Testat erhalten



C5 Report for Doctolib's Cloud Services - Doctolib

ISAE 3000 (Revised) Report on Management's Description of Doctolib on German Federal Office for Information Security BSI Cloud Computing Compliance Criteria Catalogue (C5) as of 1 April 2023

EY Building a better working world

Das C5-Testat (Cloud Computing Compliance Criteria Catalogue) des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ist derzeit die anspruchsvollste Attestierung für Cybersicherheit von Cloud-Services und anerkannter Sicherheitsstandard für SaaS-Lösungen. Doctolib-Services (Doctolib Patient, Doctolib Practice, Doctolib Siilo, Doctolib Telehealth and Doctolib Admission/ Hospital) erfüllen alle C5-Basisanforderungen vollständig und ohne Abweichungen. Die Attestierung bestätigt Doctolibs modernes und zeitgemäßes Sicherheitsniveau entsprechend den hohen Kriterien des BSI.

- Mehr als 120 Sicherheitsmaßnahmen u. a. in den Bereichen physische Sicherheit, Netzwerksicherheit, System- und Anwendungssicherheit
- Eine der anspruchsvollsten Prüfungen für Cloud-Service-Anbieter
- Attestiert die Einhaltung höchster Standards in der IT-Sicherheit

Doctolib ist selbst HDS-zertifiziert

bsi.

Certificate of Registration

Health Data Hosting Provision - Requirements and Controls - HDS:2018

This is to certify that:

Doctolib SA
54 Quai Charles Pasqua
Levallois-Perret
92300
France

Holds Certificate No: **HDS 748333**

and operates an Information Security Management System for Health Information Hosting provision which complies to the requirements of the HDS Certification Standard - Requirements and Controls - rev. 1.1. of June 2018 for the following scope:

IT Managed Services including Personal Identifiable/Health & Medical Information (PII/PHI/MI), covering ANS Activities #5 & #6 of HDS Reference System version 1.1 (2018) and in accordance with the Statement of Applicability (SoA) version 1.2 Sept 2021. The organization is certified according to ISO 27001:2013.

For and on behalf of BSI:

Luigi Brusamolino - Managing Director, Europe

Original Registration Date: 2021-10-14
Latest Revision Date: 2021-10-14

Effective Date: 2021-10-14
Expiry Date: 2024-10-13

Page: 1 of 2

...making excellence a habit.

Doctolib ist selbst als Managed Services Provider zertifiziert. Dieses Zertifikat setzt auf die ISO-27001-Zertifizierung von Doctolib auf und zertifiziert Doctolib zusätzlich für:

- Verwaltung und Betrieb eines Informationssystems, das Gesundheitsdaten enthält, und
- externalisierte Speicherung von Gesundheitsdaten. Über ISO 27001 hinaus werden dafür 44 weitere Anforderungen geprüft und zertifiziert.

Doctolib ist zertifizierter Videosprechstundenanbieter

Zertifikat

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH bescheinigt als Ergebnis der Zertifizierungsentscheidung vom 19.07.2022 gemäß Art. 42 Abs. 5 DS-GVO, dass

Doctolib GmbH
Mehringdamm 51
10961 Berlin

als Verantwortlicher gemäß Art. 4 Nr. 7 DS-GVO innerhalb des Geltungsbereichs Deutschland die Datenverarbeitung durch informationsverarbeitende Systeme

Doctolib Videosprechstunde

gemäß Anlagen 1 (erlaubter Einsatz) und 2 (Nutzungsausschlüsse) konform zu den Anforderungen der EU Verordnung 2016/679 (DS-GVO) und zu den zusätzlichen Anforderungen der Datenschutzaufsichtsbehörden betreibt und während der Laufzeit des Zertifikats überwacht wird.

Die Information der Datenschutzaufsichtsbehörde NRW gemäß Art. 43 Abs. 5 DS-GVO ist erfolgt am: 11.03.2022.

Evaluierungsgrundlage: Zertifizierungsprogramm DS-GVO, Version 0,97 Trusted Site Data Privacy, Version 2.4

Data Privacy TÜVIT 2022 Trusted Site

Certificate ID: 5604.22

© TÜVIT – TÜV NORD GROUP – www.tuvit.de

Letzter Audittag: 23.03.2022
Überwachung bis: 29.03.2023
Zertifikatsgültigkeit: 29.03.2022 – 29.03.2025

Essen, 19.07.2022

Dr. Christoph Sutter
Leiter Zertifizierungsstelle

TÜV Informationstechnik GmbH
TÜV NORD GROUP
Am TÜV 1
45307 Essen
www.tuvit.de

ZUM ZERTIFIKAT

Zertifikat

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH bescheinigt hiermit dem Unternehmen

Doctolib GmbH
Mehringdamm 51
10961 Berlin

für technische Verfahren zur Videosprechstunde

Doctolib Videosprechstunde

die Erfüllung aller Anforderungen der Kriterien

Trusted Site Video Consultation, Version 2.1

der TÜV Informationstechnik GmbH. Die Anforderungen sind in der Anlage zum Zertifikat zusammenfassend aufgelistet.

Die Anlage ist Bestandteil des Zertifikats und besteht aus 5 Seiten. Dieses Zertifikat gilt nur in Verbindung mit dem Evaluierungsbericht.

Video Consultation TÜVIT 2022 Trusted Site

Certificate ID: 5704.22

© TÜVIT – TÜV NORD GROUP – www.tuvit.de

Zertifikatsgültigkeit: 29.03.2022 – 29.03.2025

Essen, 19.07.2022

Dr. Christoph Sutter
Leiter Zertifizierungsstelle

TÜV Informationstechnik GmbH
TÜV NORD GROUP
Am TÜV 1
45307 Essen
www.tuvit.de

ZUM ZERTIFIKAT

Die Videosprechstunde von Doctolib ist vom Zertifizierer TÜV Informationstechnik GmbH (TÜVIT) zertifiziert:

- **nach Art. 42, 43 DSGVO mit dem Prüfzeichen TÜVIT Trusted Site Data Privacy und**
- **mit dem Prüfzeichen TÜVIT Trusted Site Video Consultation.**

› Die Doctolib-Videosprechstunde ist damit auf der Liste der zertifizierten Videodienstanbieter der KBV zu finden und entspricht den geltenden Bestimmungen.

› Die Zertifizierung erfolgt gemäß den Voraussetzungen von Anlage 31b BMV-Ä (Bundesmantelvertrag-Ärzte).

Fokus Datenschutz

Rechtsgrundlagen und Einwilligungs-management

Doctolib als Auftragsverarbeiter – keine Einwilligung der Patient:innen erforderlich für den Einsatz von Doctolib

Die Verarbeitung von personenbezogenen Daten, inklusive Gesundheitsdaten, durch Doctolib ist ohne Einwilligung erlaubt, da sich die Datenverarbeitung auf eine zulässige Auftragsverarbeitung stützt.

Wird durch die Gesundheitseinrichtung ein Auftragsverarbeiter (wie Doctolib) eingesetzt und mit der Verarbeitung personenbezogener Daten der Patient:innen beauftragt, müssen Patient:innen nicht in diese Beauftragung und die Verarbeitung ihrer Daten einwilligen. Ärzt:innen steht es frei, ihre Auftragsverarbeiter auszusuchen und zu beauftragen.

Beachten Sie:

Die Verarbeitung von personenbezogenen Gesundheitsdaten ist daher ohne Einwilligung der Patient:innen zulässig. Patient:innen müssen jedoch über den Einsatz von Doctolib informiert werden. Doctolib stellt in seinem Hilfebereich ein **Muster** zur Verfügung.

Für die Datenverarbeitung, die an den Auftragsverarbeiter delegiert wird, muss die Gesundheitseinrichtung selbst eine Rechtsgrundlage haben. Folgendes kann herangezogen werden:

- Laut Art. 9 Abs. 2 h) DSGVO ist die Verarbeitung von Gesundheitsdaten für die Zwecke der Gesundheitsvorsorge erlaubt. Zur Gesundheitsvorsorge gehört nicht nur die medizinische Versorgung, sondern auch die Terminverwaltung und das Management der Patientenbeziehung.
- Laut Art. 6 Abs. 1 b) DSGVO ist die Verarbeitung von Daten erlaubt, wenn dies für die Erfüllung eines Vertrags erforderlich ist, hier: Behandlungsvertrag Ärzt:in – Patient:in. Ohne die Vereinbarung eines Termins und die Aufnahme der Patientendaten ist keine Behandlung möglich.

Die Gesundheitseinrichtung als Verantwortlicher der Datenverarbeitung darf eine Datenverarbeitung, zu der sie selbst berechtigt ist, gemäß Art. 28 DSGVO an einen Auftragsverarbeiter delegieren. Die Auftragsverarbeitung ist auch im Bereich der Gesundheitsvorsorge zulässig. Es muss ein Auftragsverarbeitungsvertrag nach Art. 28 DSGVO abgeschlossen werden und der Auftragsverarbeiter muss ausreichende technische und organisatorische Maßnahmen (TOM) eingesetzt haben.

- Die Gesundheitseinrichtung erteilt Doctolib den Auftrag zur Datenverarbeitung für präzise festgelegte Verarbeitungstätigkeiten. Doctolib ist streng weisungsgebunden, wie im Auftragsverarbeitungsvertrag festgelegt.
- Ärzt:innen können laut § 203 StGB Dienstleister in ihre Tätigkeit einbinden, wenn sie diese auf die Schweigepflicht verpflichten. Doctolib wirkt an der Tätigkeit der Gesundheitsvorsorge (Terminverwaltung, Verwaltung der Patientenbeziehung) der Ärzt:innen mit und wird vertraglich auf die Schweigepflicht verpflichtet. Doctolib gibt die Schweigepflicht an Mitarbeitende und Unterauftragsverarbeiter weiter. Eine Entbindung von der Schweigepflicht erfolgt somit nicht.
- Die für die Anwendung von Doctolib erforderlichen Daten werden ausschließlich bei besonders für das Hosting von Gesundheitsdaten zertifizierten Hostern gespeichert (sog. Health Data Hosting). Sämtliche TOM sind als Anhang des Auftragsverarbeitungsvertrags aufgelistet.

Import von Daten von Bestandspatient:innen

Der Import bestehender Patientendaten (beschränkt auf die für die Terminverwaltung erforderlichen Daten) und relevanter Termindaten ist ebenfalls ohne Einwilligung möglich.

- Damit in das Doctolib-System relevante Patienten- und Termindaten nicht händisch neu eingetragen werden müssen, können sie durch einen Datenimport in das Doctolib-System übertragen werden.
- Die Verfügbarkeit der Patientenbasis in Doctolib ermöglicht die Online-Buchung in Echtzeit: Um Termine in Echtzeit in den Arztkalender buchen zu können, ist ein Abgleich der Patientenidentität in Echtzeit erforderlich. Darüber hinaus bieten zahlreiche Kliniken bestimmte Besuchsgründe z. B. nur für Bestandspatient:innen an – oder fürPatient:innen, die zum letzten Mal vor einer bestimmten Zeit in der Klinik waren. Um diesen Abgleich des/der den Termin buchenden Patient:in mit dem Patientenstamm der Klinik zuverlässig in Echtzeit und ohne Anlegung von Doppelidentitäten leisten zu können, werden die Patientenstammdaten sowie für die zukünftige Buchung relevante Termindaten in das Doctolib-Terminmanagementsystem übertragen.
- Die Entscheidung, welche Patientendaten in das Doctolib-System übertragen werden, obliegt der Gesundheitseinrichtung als dem für die Datenverarbeitung Verantwortlichen.
- Bezüglich der Termindaten entscheidet ebenso die Gesundheitseinrichtung, welche Termine in das Doctolib-System übertragen werden sollen. Legt die Gesundheitseinrichtung etwa fest, dass die Termine der vergangenen 2 Jahre für die zukünftige Buchung im Terminmanagementsystem erforderlich sind, werden alle administrativen Daten, die mit Terminen zusammenhängen, die älter als 2 Jahre sind, nicht mit übernommen. Ohne Konkretisierung der Gesundheitseinrichtung werden die Termindaten des letzten zurückliegenden Jahres importiert.
- Der Import kann über eine Schnittstelle erfolgen. Wird eine Schnittstelle genutzt, werden Patientendaten, die neu im KIS angelegt werden, auch in Doctolib übertragen. Termine, die in Doctolib angelegt werden, werden ins KIS übertragen. So ist sichergestellt, dass die Daten stets richtig und aktuell sind. Ein fehleranfälliger händischer Übertrag von einem System zum anderen wird vermieden.

Terminerinnerungen an Patient:innen

Erinnerungsnachrichten sind ein Mittel der Terminverwaltung: Sie verhindern die Desorganisation durch No-Shows und ermöglichen die Neuterminierung für frei werdende Slots im Fall von Stornierungen oder Verschiebungen.

Erinnerungsnachrichten sind jedoch – nach Auffassung der deutschen Datenschutzbehörden – für die Terminverwaltung nicht unbedingt erforderlich. Daher kommt als Rechtsgrundlage nur die Einwilligung der Patient:innen in Betracht.

- Patient:innen, die ein Doctolib-Nutzerkonto angelegt haben und online einen Termin buchen, haben die Allgemeinen Nutzungsbedingungen und damit die Terminerinnerungen als Teil des Service von Doctolib akzeptiert.
- Für telefonisch oder vor Ort buchende Patient:innen sind Terminerinnerungen per Voreinstellung deaktiviert. Die Patient:innen sollten bei telefonischer Buchung zunächst mündlich einwilligen, Terminerinnerungen über das Terminsystem Doctolib zu erhalten. Die Erinnerungsfunktion kann daraufhin durch die Fachkraft aktiviert werden. Erscheinen die Patient:innen zum Termin, sollten sie ihre Auswahl zu Nachweiszwecken nochmals schriftlich bestätigen. Doctolib stellt ein Muster der Einwilligungserklärung zur Verfügung.

Die Einstellung kann auf der Patientenkarte jederzeit angepasst werden. Doctolib weist auf das Einwilligungserfordernis auch im Online- Hilfebereich hin.

Online-Buchung des Arzttermins über ein Doctolib-Nutzerkonto

- Doctolib ermöglicht, dass Patient:innen ihre Termine selbst online in Zeiträume im Arztkalender buchen, die die Gesundheitseinrichtung zur Online-Buchung freigegeben hat. Eine Online-Terminbuchung über die Website von Doctolib erfordert das Anlegen eines Nutzerkontos. Dies ist ein gesicherter Bereich, in dem Patient:innen Termine einsehen, stornieren und verschieben können. Sie müssen beim Anlegen des Nutzerkontos eine Zwei-Faktor-Authentifizierung durchlaufen.
- Für das Anlegen des Nutzerkontos ist Doctolib Verantwortlicher der Datenverarbeitung. Die Patient:innen stimmen beim Anlegen des Nutzerkontos den Allgemeinen Nutzungsbedingungen von Doctolib zu. Patient:innen, die wünschen, dass auch ihre vergangenen Termine im Nutzerkonto angezeigt werden, müssen dafür ihre Einwilligung erteilen.
- Für die verbindliche Terminbuchung ist Doctolib Auftragsverarbeiter. Die Terminbuchung ist als Leistung im Auftragsverarbeitungsvertrag genannt. Doctolib hat keine Einsicht in Termine von Patient:innen.
- Patient:innen können ihr Nutzerkonto jederzeit löschen. Termine, für die Doctolib Auftragsverarbeiter der Gesundheitseinrichtung ist, werden durch ein Löschen des Nutzerkontos nicht berührt und bleiben im Kalender des Arztes oder der Ärztin erhalten.

Auftrags-verarbeitungsvertrag

Datenverarbeitung durch Doctolib auf der Grundlage eines Auftragsverarbeitungsvertrags

- Der Vertrag über die Auftragsverarbeitung muss vor der ersten Datenverarbeitungstätigkeit von Doctolib abgeschlossen werden.
- Schon z. B. Systemprüfungen durch Doctolib bei Ärzt:innen oder Schulungen des Personals erfordern den beidseitig unterzeichneten Auftragsdaten-verarbeitungsvertrag. Hintergrund: Es handelt sich um eine Pflicht von Ärzt:innen laut Art. 28 Abs. 3 DSGVO: „Die Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines Vertrags [...]."
- Der von Doctolib vorgeschlagene Auftragsverarbeitungsvertrag enthält sämtliche DSGVO-Pflichtangaben. In einem ersten Anhang zum Vertrag werden die Datenverarbeitungen präzise beschrieben (insbesondere Zwecke der Datenverarbeitung, Rechtsgrundlage, verarbeitete Daten, Speicherdauer). Weitere Anhänge beschreiben die technischen und organisatorischen Maßnahmen, inklusive der Maßnahmen, die bei einem Schnittstelleneinsatz relevant sind. Die Verwendung der von Doctolib vorbereiteten Anhänge ist wichtig, da auf diese Weise sowohl für Doctolib als auch für die Gesundheitseinrichtung sichergestellt ist, dass die Beauftragung genau beschrieben ist.

Aufbewahrungsfristen und Datenlöschung

Löschung von Daten

Aus Art. 17, 30 DSGVO folgt die Pflicht für Unternehmen, personenbezogene Daten nach einer bestimmten Dauer zu löschen.

- Doctolib hat intern eine Data Retention Policy, die für jede Verarbeitungstätigkeit die Speicherdauer und die Löschaktion präzisiert. Danach erfolgt die Datenlöschung durch Anonymisierung oder Löschung. Die Anonymisierung steht gemäß der DSGVO der Löschung gleich, wenn jeglicher Personenbezug irreversibel entfernt wird.
- Vor dem irreversiblen Löschen von Daten wird sichergestellt, dass die Kund:innen ihre Daten in einem gängigen Format (Excel oder CSV) wiedererlangen.
- Doctolib setzt individuelle Löschanweisungen des Auftraggebers um und bestätigt die Auftragslöschung.
- Anfragen von Patient:innen auf Löschung aus dem Doctolib-Kalender kann Doctolib nicht nachkommen, da Doctolib als Auftragsverarbeiter nicht auf Verlangen von Patient:innen deren Daten aus dem Terminkalender eines Arztes bzw. einer Ärztin löschen darf.

Aufbewahrungsfristen

Art	Dauer	Erklärung
Termindaten	Per Default 5 Jahre, einstellbar durch den/die Kund:in zwischen 1 und 20 Jahre	Jede Gesundheitseinrichtung muss prüfen, welche vergangenen Termine auch für die zukünftige Terminierung relevant sind. Dies kann von Fachrichtung zu Fachrichtung unterschiedlich sein. Die Übersicht über die Terminhistorie vermittelt in der Regel behandlungsrelevante Informationen. Doctolib ist allerdings nicht das System, um langfristig Termine aufzubewahren. Im Patienten-Nutzerkonto können Patient:innen die Terminhistorie sehen (wenn sie die Funktion aktiviert haben), die auch im Doctolib-Kalender auf Arztseite sichtbar ist.
Patientendaten	Je nach Weisung des Verantwortlichen	Der Verantwortliche kann Speicherdauer bestimmen.
Im Nutzerkonto hinterlegte Daten von Arzt/Ärztin bzw. Fachkraft	Für die Dauer des Vertrags oder bei Löschung des Nutzerkontos durch die Gesundheitseinrichtung	Für jede:n Mitarbeiter:in, der Zugang zu Doctolib benötigt, ist die Anlegung eines Nutzerkontos erforderlich (nicht zu verwechseln mit dem Patienten-Nutzerkonto zur Online-Terminbuchung). Verlassen Mitarbeiter:innen die Klinik, sollte die Klinik die Nutzerkonten jeweils löschen. Bei Ende des Vertrags zwischen Doctolib und der Gesundheitseinrichtung werden die Daten der Nutzerkonten gelöscht.
Verbindungsdaten der Videosprechstunde	3 Monate	Vorgabe aus Anlage 31b zum BMV-Ä
Nachrichten und Dokumente im Rahmen des Messaging-Dienstes	6 Monate ab Versand	Der Verantwortliche kann anderweitige Weisungen erteilen.
Dokumente und Formulare im Rahmen der Verarbeitungstätigkeit Dokumentenverwaltung	Je nach Dienst oder bis zur Löschung durch den/die Nutzer:in	Werden Dokumente mit dem/der Patient:in in dessen/deren Patienten-Nutzerkonto geteilt, für das Doctolib als Auftragsverarbeiter handelt, kann der/die Patient:in die Funktionalität aktivieren, diese Dokumente in seinem/ihrem Nutzerkonto dauerhaft zu speichern. Für diese Speicherung bis zur Löschung der Dokumente durch den/die Patient:in ist Doctolib Verantwortlicher der Datenverarbeitung.

Datenspeicherung

Grundsätze des Hostings der Doctolib-Plattform

- Doctolib legt großen Wert auf die Systemverfügbarkeit, die IT-Sicherheit und den Datenschutz. Um die Anforderungen der höchsten Systemverfügbarkeit (über 99,8 % hinaus), performanter Nutzbarkeit, anspruchsvollster IT-Sicherheit und des europäischen Datenschutzes zu erfüllen, wählt Doctolib den Ansatz des externen Hostings bei den von unabhängigen Prüfanstalten zertifizierten und auditierten Datenzentren in Deutschland und Frankreich.
- Doctolib ist eine vollredundante Lösung, die auf hochsicheren und redundanten Rechenclustern operiert, die den Anforderungen für Datenschutz und IT-Sicherheit entsprechen. Des Weiteren erfüllen die Rechenzentren die Anforderungen an die Speicherung der sensiblen Gesundheitsdaten.
- Doctolib ist 100-prozentiger Eigentümer der Technologie, die seit Firmengründung intern von einem heute über 150 Entwickler:innen starken Team in 2 Technologiezentren in Berlin und Paris entwickelt wurde.

Hosting ausschließlich in Deutschland (Frankfurt) und Frankreich (Paris)

- Die Daten werden ausschließlich innerhalb Europas gespeichert. Sie verlassen die EU auch nicht für Wartungs- oder Supportzwecke. Der Auftragsverarbeitungsvertrag mit AWS ist mit der Tochtergesellschaft von AWS mit Sitz in Luxemburg geschlossen.
- Die Zulässigkeit des Einsatzes der Luxemburger Tochtergesellschaft von AWS im Gesundheitsbereich wurde vom OLG Karlsruhe mit Entscheidung vom 7. September 2022 (Aktenzeichen: 15 Verg 8/22) festgestellt. Auch der Conseil d'État, der oberste französische Verwaltungsgerichtshof, hat die Zulässigkeit des Hostings bei AWS durch Doctolib im Einklang mit der DSGVO mit Entscheidung vom 12. März 2021 festgestellt.

Daten werden nur in Rechenzentren gespeichert, die für Health Data Hosting zertifiziert sind

Sämtliche Daten sind bei unserem für Health Data Hosting zertifizierten Hosting-Provider gespeichert.

- Die Patienten- und Termindaten werden in einem Rechenzentrum von AWS in Frankfurt am Main gespeichert und in einem Rechenzentrum desselben Anbieters in Paris gespiegelt. AWS ist für diese Rechenzentren speziell fürs Gesundheitsdaten-Hosting zertifiziert (sog. HDS-Zertifikat, HDS steht für Hébergeurs de Données de Santé).
- Die HDS-Zertifizierung ist ein in Deutschland nicht existierender Schutzstandard speziell fürs Gesundheitsdaten-Hosting. Es handelt sich nicht um ein privates Label, sondern die Vergabe erfolgt durch eine vom französischen Gesundheitsministerium eingesetzte Agentur für Gesundheitsinformationssysteme nach Durchlaufen eines mehrstufigen Zertifizierungsprozesses. Sie beruht auf Gesetzesvorschriften. Die Zertifizierung wird zudem erst nach der Zustimmung des Akkreditierungskomitees des Hosts (CAH) und der französischen Datenschutzbehörde (CNIL) erteilt.
- Das HDS-Zertifikat wird in einem mehrstufigen Verfahren erteilt und geht über die ISO-27001-Anforderungen hinaus (Auditierung nach Dokumentation und On-site-Audit).
- Das Health-Data-Hosting-Zertifikat wird für eine Dauer von 3 Jahren ausgestellt.

Zertifizierungsvoraussetzungen für ein HDS-Zertifikat sind insbesondere:

- Einsatz von qualifiziertem Personal für die Datensicherheit
- Einsatz technischer Schutzmaßnahmen
- Organisations- und Kontrollverfahren zur Gewährleistung von Datenschutz und Datensicherheit sowie der Integrität und Verfügbarkeit bei Datenverarbeitungen
- Festlegung und Umsetzung eines Vertraulichkeits- und Sicherheitskonzepts, insbesondere zur Sicherstellung der Einhaltung der gesetzlichen Anforderungen an die Vertraulichkeit und Geheimhaltung
- Individualisierung der Organisation, der Hosting-Aktivitäten und der dafür verwendeten Mittel sowie Datenmanagement und Datenfluss
- Definition und Implementierung von Informationstools für die Personen, die Daten in die Datenbank eingeben, besonders für den Fall, dass sich erhebliche Änderungen bei den Bedingungen für die Durchführung dieser Aktivität ergeben
- Eindeutige Bestimmung der für die Hosting-Aktivität verantwortlichen Personen

Hébergeurs de Données de Santé
BUREAU VERITAS Certification

Umgang mit dem Data Privacy Framework und Schrems-II-Urteil des EuGH

Im sog. Schrems-II-Urteil hat der Europäische Gerichtshof im Juli 2020 entschieden, dass Unternehmen, die mit Dienstleistern arbeiten, die außerhalb der EU (d. h. in einem sog. Drittland) sitzen oder eine Muttergesellschaft haben, die in einem Drittland sitzt, prüfen müssen, ob sie ausreichende Schutzmaßnahmen eingerichtet haben, um einen Zugriff auf die Daten durch Behörden des Drittlandes zu kontrollieren bzw. zu verhindern.

Der Einsatz von Dienstleistern mit US-Bezug ist durch das sog. Data Privacy Framework vom 10. Juli 2023 wieder erleichtert worden, sofern der Dienstleister unter diesem Framework zertifiziert ist. Für AWS ist dies der Fall. Doctolib behält jedoch die nach dem Schrems-II-Urteil eingerichteten Zusatzmaßnahmen bei.

1. In dem mit AWS abgeschlossenen Auftragsverarbeitungsvertrag verpflichtet sich AWS, dass die Daten ausschließlich in den von Doctolib benannten Rechenzentren (Frankfurt am Main und Paris) gespeichert werden.
2. Die Verschlüsselung der personenbezogenen Patienten- und Termindaten stellt sicher, dass AWS selbst im theoretischen Fall einer Anfrage auf Datenherausgabe nur auf verschlüsselte Daten zugreifen könnte.

Wie genau funktioniert die Verschlüsselung der Daten bei der Speicherung auf AWS?

- Beim Transport von Informationen wird eine Verschlüsselung auf Basis von TLS (Transport Layer Security) verwendet.
- Auf den Servern werden die Daten durch HSM(Hardware-Security-Modul-)-geschützte Schlüssel verschlüsselt, die wiederum durch einen Master-Schlüssel geschützt werden, der im Besitz von Doctolib ist.
- Wir verwenden den AWS KMS (Key Management Service). Dabei sind die KEK (Key Encryption Keys) mit einem Master-Schlüssel geschützt, der ausschließlich Doctolib gehört und von dem französischen Unternehmen Atos bereitgestellt wird. Der AWS Customer Master Key (CMK) wurde von unserem HSM importiert, sodass AWS nicht in der Lage ist, Doctolib-Daten zu entschlüsseln.

Patienteninformation

Müssen Patient:innen über die externalisierte Datenverarbeitung informiert werden?

- **Ja!** Patient:innen sind laut Art. 13 und 14 DSGVO über die Datenverarbeitung zu informieren.
- Ärzt:innen können der Informationspflicht insbesondere nachkommen durch:
  - Aushang oder Flyer
  - Einfügung eines Absatzes in die eigenen Datenschutzbestimmungen auf der Website
  - Telefonansage
  - Doctolib stellt ein Muster zur Verfügung.
  - Am Telefon ist keine ausführliche Information über die Datenverarbeitung erforderlich.
- Bestandspatient:innen, deren Stamm- und Termindaten in Doctolib übertragen werden, müssen nicht gesondert informiert werden. Art. 13 Abs. 1 DSGVO knüpft ausschließlich an den „Zeitpunkt der Erhebung“ an, zu dem den Betroffenen alle verfügbaren Informationen mitgeteilt werden sollen. Da sich der Zweck der Datenverarbeitung nicht ändert, besteht auch keine nachträgliche Informationspflicht nach Art. 13 Abs. 3 DSGVO.
- Die betroffenen Personen haben gegenüber der Gesundheitseinrichtung das Recht, sog. Betroffenenrechte geltend zu machen (Recht auf Auskunft, Berichtigung, Löschung etc.). Eine Löschung von Patientendaten aus Doctolib kann die Gesundheitseinrichtung durch Löschung der Patientenkarte vornehmen.

Datenschutz-Folgenabschätzungen

Doctolib unterstützt bei der Durchführung von Datenschutz-Folgenabschätzungen

Nach der DSGVO muss der Verantwortliche der Datenverarbeitung bei Verarbeitungsvorgängen, die aufgrund ihrer Art, ihres Umfangs, ihrer Umstände und ihrer Zwecke wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringen, eine Datenschutz-Folgenabschätzung durchführen.

Doctolib als Auftragsverarbeiter hilft dem Verantwortlichen bei der Durchführung der Datenschutz-Folgenabschätzung und stellt die erforderlichen Informationen bereit:

- Informationen über die durchgeführten Verarbeitungstätigkeiten und die getroffenen Sicherheitsmaßnahmen werden in unserem Auftragsverarbeitungsvertrag sowie in unseren online verfügbaren Datenschutzhinweisen für Gesundheitsfachkräfte und Patient:innen zur Verfügung gestellt.
- Auf Anfrage stellt Doctolib eine Risikoanalyse in Bezug auf Online-Buchungsservice und Terminverwaltung sowie eine Risikoanalyse bezüglich der Telekonsultation bereit.

Diese Dokumente sind Teil des internen Risikomanagementprogramms von Doctolib. Sie können an Kund:innen übermittelt werden, um ihnen die notwendige Unterstützung bei der Durchführung ihrer Datenschutz-Folgeabschätzung zu geben.

Diese Dokumente sind vertraulich und dürfen nicht an Dritte weitergegeben werden.

Methode zur Durchführung von Datenschutz-Folgenabschätzungen

Für die Erstellung von Datenschutz-Folgenabschätzungen bezüglich Datenverarbeitungen in eigener Verantwortung folgt Doctolib folgenden 4 Schritten:

1. Test der Verarbeitungstätigkeit auf Erforderlichkeit einer Datenschutz-Folgenabschätzung
2. Durchführung: Bewertung der Risiken für die Rechte und Freiheiten der Betroffenen
3. Interne Validierung und Dokumentation
4. Umsetzung ggf. identifizierter Maßnahmen zur Risikominimierung

Bei den Datenschutz-Folgenabschätzungen handelt es sich um eine interne Dokumentation. Diese wird Behörden und Auditoren zur Verfügung gestellt.

Datenschutz-Folgenabschätzungen als Zertifikatsbestandteil

- Datenschutz-Folgenabschätzungen sind grundlegender Bestandteil der Zertifizierungen von Doctolib. Sie werden den Auditoren auf Anfrage vorgelegt.
- Die von Doctolib gehaltenen Zertifikate erfordern eine regelmäßige Erneuerung der Datenschutz-Folgenabschätzungen (in der Regel alle 3 Jahre).

Fokus Datensicherheit

Verschlüsselung

Verschlüsselungsverfahren und -parameter

Verschlüsselung des Datenverkehrs

- Sämtlicher Datenaustausch zwischen den Doctolib-Servern und den Clients ist immer verschlüsselt. Wir unterstützen das TLS-1.3-Protokoll mit modernsten Verschlüsselungstechniken wie z. B. AES-256 GCM und CHACHA20.
- Unsere Zertifikate verwenden einen 4.096-Bit-Schlüssel, ausgestellt von der höchst angesehenen und vertrauenswürdigen Zertifizierungsstelle GeoTrust und signiert durch SHA-256 mit RSA.
- Die Verschlüsselungsstandards sind so implementiert, dass sie den höchsten Grad an Interoperabilität und Sicherheit gewährleisten.

Verschlüsselte Datenspeicher

- Die Doctolib-Datenbanken sind mit dem AES-256-Verschlüsselungsalgorithmus codiert.
- Eine zusätzliche Verschlüsselungsebene wird auf sensible Daten angewendet, um den Zugriff auf die Daten durch die Datenbankadministrator:innen zu verhindern.

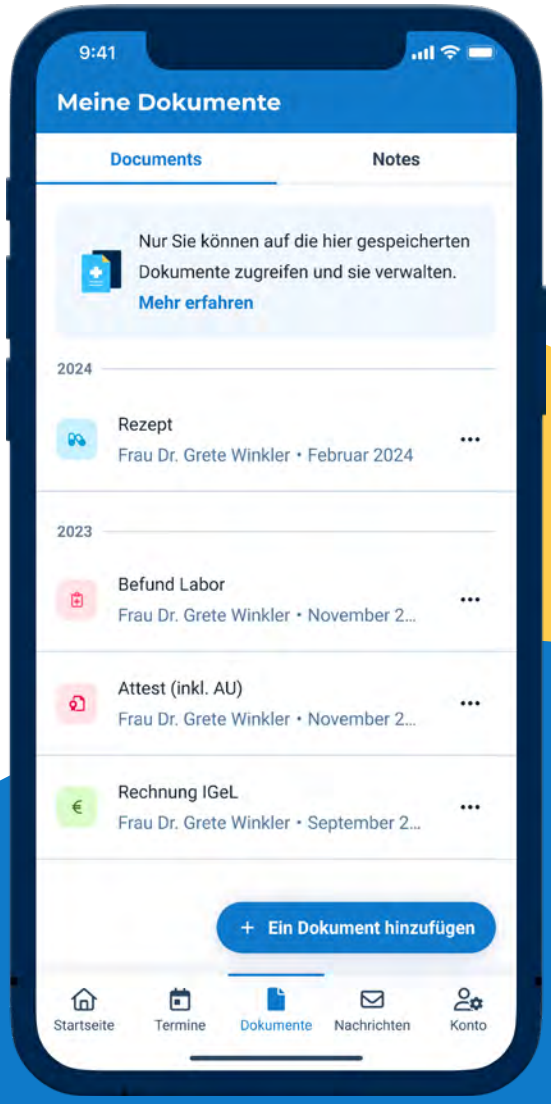
Schlüsselmanagement

- Doctolib nutzt einen hochmodernen KMS-Dienst zur Verschlüsselung sensibler Daten. Es handelt sich um einen sicheren und robusten Dienst, der Hardware-Sicherheitsmodule verwendet.
- Das System ist so konzipiert, dass niemand, einschließlich der Mitarbeitenden unserer Hosting-Einrichtung, Klartextschlüssel vom Dienst abrufen kann.
- Der Dienst verwendet Hardware-Sicherheitsmodule (HSMs), die nach FIPS 140-2 Stufe 2 validiert wurden, einschließlich der physischen Sicherheit zum Schutz der Vertraulichkeit und Integrität von Doctolib-Schlüsseln. Der Dienst wurde ebenfalls nach Common Criteria EAL4+ zertifiziert.
- Doctolib-Klartextschlüssel werden nie auf die Festplatte geschrieben und immer nur in einem flüchtigen Speicher der HSMs für die Zeit verwendet, die zur Durchführung der angeforderten kryptografischen Operation benötigt wird.
- Alle innerhalb der HSMs verwendeten symmetrischen Schlüsselverschlüsselungsbefehle verwenden die Advanced Encryption Standards (AES) im Galois-Zählermodus (GCM) mit 256-Bit-Schlüsseln. Die analogen Aufrufe zur Entschlüsselung nutzen die inverse Funktion.

Document-Sharing-Feature

Mit dem Document-Sharing-Feature können Patient:innen, die ein Doctolib-Nutzerkonto haben, und Ärzt:innen medizinische Dokumente direkt via Doctolib austauschen.

- Um Datensicherheit und Anwendungsflexibilität gleichermaßen zu gewährleisten, kann nur die Person, die ein verschlüsseltes Dokument hochgeladen hat, es jederzeit wieder löschen.
- Auf Anfrage können autorisierte Mitarbeitende von Doctolib das Dokument ebenfalls löschen, jedoch ohne dabei auf den Inhalt zugreifen zu können.
- Um das Persönlichkeitsrecht der Patient:innen zu wahren, werden bei einer Löschung des Nutzerkontos durch die Patient:innen die verschlüsselten Dokumente ebenso gelöscht.



Verschiedene Aspekte der Architektur

Verschlüsselung

- Sichere Verbindungen (HTTPS, TLS, IPsec ...)
- Verschlüsselte Datenbank (Encryption at rest ...)
- Verschlüsselte Speicherung (Harddisk und Partition)
- Patientenstammdaten verwalten

Schutz

- 6 Schutzebenen und Verschlüsselung der Daten
- Zugang: starke Authentifizierung, automatische Abmeldung, granulare Rechte, Nachverfolgbarkeit
- Plattform: gesicherte Datenzentren (HDS, ISO 27001, starke physische Sicherheit, Sicherheitspersonal 24/7), Anti-DDoS-Schutz

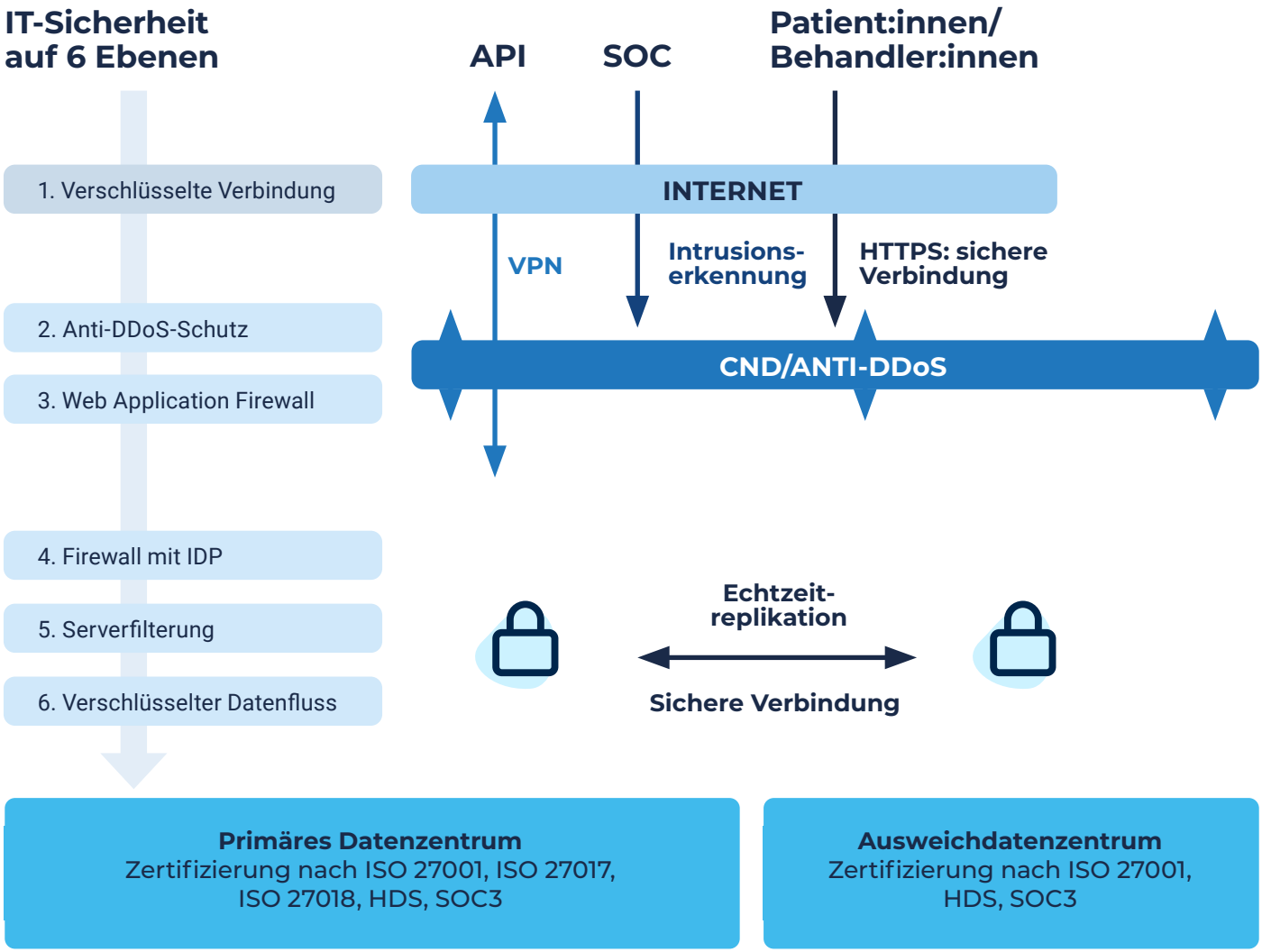
Datentrennung

- Zugriff nur auf ausdrückliche Anweisung durch die Organisation als Auftraggeber
- Trennung der Datenbanken verschiedener Auftraggeber

Mittel

- Security by Design: integriert in den Code mit allen Ent- wickler:innen, die hinsichtl. Sicherheit geschult sind
- Mehr als 20 Mitarbeiter:innen im Security-Team mit ständiger Einsatzbereitschaft
- 90 T€ jährliches Investment, um Schwachstellen zu entdecken (Intrusionstests und Bug Bounty)
- 4 Mio. € jährliches Investment für Sicherheit (Plattform, Produkt, Mitarbeitende)

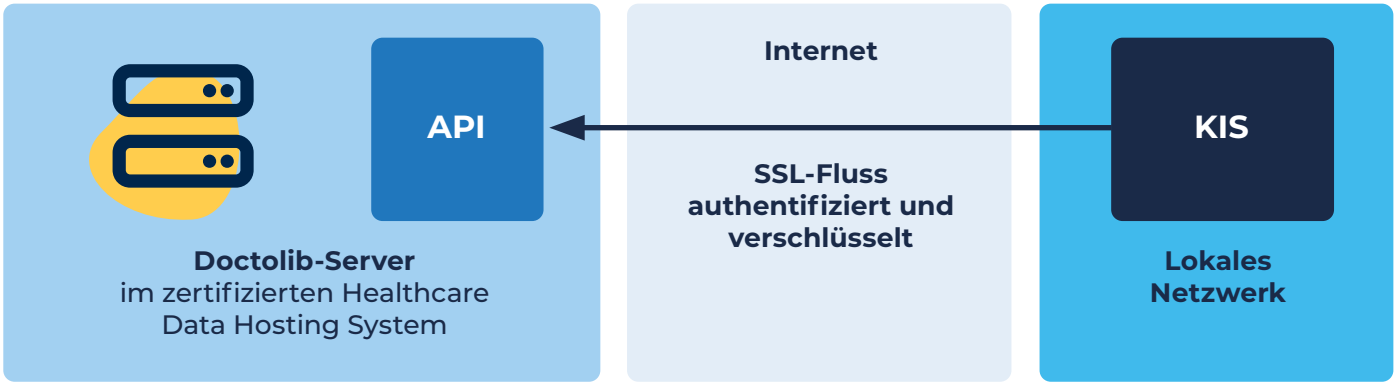
IT-Sicherheit durch verteilte Serverarchitektur



- Schutz und IT-Sicherheit von Datenflüssen auf 6 Ebenen
- Verschlüsselung aller Datenströme
- Hosting im Rechenzentrum in Frankfurt am Main und Spiegelung in Paris
- Alle Rechenzentren sind für die Speicherung von Gesundheitsdaten speziell zertifiziert.
- Mehrfache Datenreplikation, Point-in-time-Back-up in jedem Rechenzentrum
- Vollständig redundante Serviceplattform und Datenspeicher
- Echtzeitüberwachung und Alarmierung

Sichere Datenübertragung zwischen Datenzentren und Einrichtungen

HTTPS- und HMAC-Verschlüsselung (APISync)



- Mit APISync werden alle Meldungen vom KIS gesendet oder empfangen (in Echtzeit oder alle 5 Sekunden). Die Verbindung wird durch HTTPS verschlüsselt und mithilfe von HMAC authentifiziert und vor Verfälschung geschützt.
- Mögliche Formate: HL7 oder Doctolib-formatiertes JSON-Äquivalent

Weitere Sicherheitsmaßnahmen der Doctolib-Rechenzentren

- Das System und die Netzwerkumgebung von Doctolib sind mit einer State-of-the-Art-Firewall-Technologie geschützt.
- Doctolib hat technische Maßnahmen gegen Denial-of-Service(DDoS-)-Angriffe implementiert (z. B. Arbor Networks).
- Die Doctolib-Rechenzentren verfügen über starke physische Sicherheitsstandards im Sinne der Anlage 1 zu § 9 BDSG (u. a. Zäune, Wände, Schranken, Wachen, Tore, elektronische Überwachung, physische Authentifizierungsmechanismen, Empfangsbereiche und Sicherheitspatrouillen).
- Doctolib nutzt strenge Sicherheitskonfigurationen für Server/Infrastruktur der Doctolib-Rechenzentren (z. B. Hypervisoren, Betriebssysteme, Router, DNS-Server).
- Doctolib verwendet eine WAF (Web Application Firewall), um Angriffe auf die Webservices zu blockieren.
- Doctolib beauftragt regelmäßige Pentests.
- Doctolib setzt CIS, OWASP und weitere Best Practices um.

Keine Speicherung von Daten auf den Endgeräten

- Aufgrund der großen Anzahl von Mitarbeitenden, deren Heterogenität und einer großen Fluktuation stellt ein Krankenhaus besondere Herausforderungen an die Einhaltung der notwendigen, höchstmöglichen Datenschutzstandards. Hinzu kommt meist ein Mangel an physischer Sicherheit (Zutritts-, Zugangs- und Weitergabekontrolle).
- Doctolib setzt daher auf eine Lösung, die das Speichern persönlicher Daten auf Endgeräten nicht erfordert und damit Risiken minimiert.
- Doctolib speichert keine personenbezogenen Daten auf Endgeräten wie Smartphones, Tablets oder Desktop-PCs.
- Um Risiken zu minimieren, ist der Zugang zu Patientendaten auf den Zeitraum begrenzt, für den ein:e Nutzer:in autorisiert worden ist. Zu dem Zeitpunkt, an dem diese Autorisierung ausläuft, z. B. aufgrund der Kündigung des Doctolib-Abonnements, kann der Zugang durch Administrator:innen auch aus der Ferne entzogen werden.

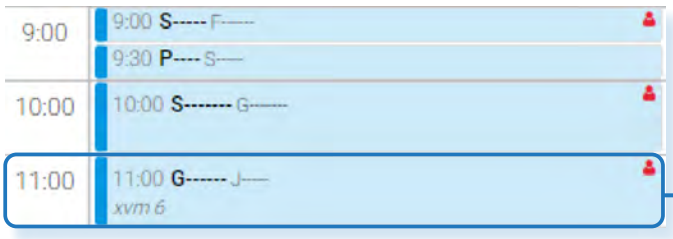
Zugriffsrechte

Zugangsbeschränkung für Doctolib-Mitarbeitende: Pseudonymisierung der Daten

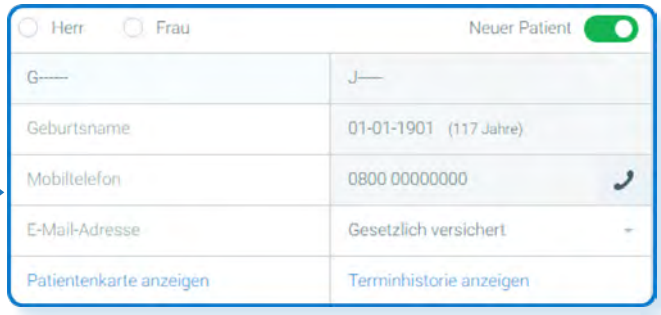
Doctolib-Mitarbeitende haben standardmäßig keine Einsicht in Daten, die in dem Terminkalender eines Arztes oder einer Ärztin eingetragen sind. Alle Stammdaten und Termindaten sind für Doctolib-Mitarbeitende nur pseudonymisiert sichtbar:

- Vor- und Nachname: X------ Y-------
- Geburtstag: 01/01/1901
- Telefonnummer: 080000000000
- Sonstiges: zufällige Buchstaben, Zahlen und Satzzeichen

Kalenderansicht für zugriffsberechtigte Mitarbeitende von Doctolib



Terminansicht/Patientenansicht für zugriffsberechtigte Mitarbeitende von Doctolib



Zugang zu den Daten unter strengen Bedingungen

Für Patient:innen, die online ihren Termin buchen

- Doctolib informiert die Patient:innen über die Nutzung ihres Accounts in den Patienten-Nutzungsbedingungen.
- Alle Patient:innen, die Doctolib für die Terminbuchung verwenden, müssen die Nutzungsbedingungen akzeptieren und können die Datenschutzhinweise von Doctolib einsehen.

Für die Nutzer:innen der Auftraggeber von Doctolib, die über entsprechende Rechte verfügen

- Der Zugang ist beschränkt auf Behandler:innen und deren Personal, die den Kalenderservice nutzen.

Für das Sicherheitsteam von Doctolib

- Das IT-Sicherheitsteam von Doctolib besteht derzeit aus mehr als 20 Personen.
- Dies gewährleistet die Verfügbarkeit, Leistung und Sicherheit der Doctolib-Systeme.
- Der Zugriff auf Kundendatenbanken wird ausschließlich 1. durch das IT-Sicherheitsteam, 2. auf schriftliche Anweisung und Anfrage des/der betreffenden Kund:in oder 3. nach Vereinbarung und unter der Kontrolle des/der Kund:in gewährt.
- Der Zugang wird nur über ein Teilnetz gewährt, das vom lokalen Netz getrennt und vom Internet durch eine Firewall (DMZ) isoliert ist. Jede Verbindung wird nach einem strengen Verfahren protokolliert und überwacht.

Zugriffsrechte – 2 verschiedene Arten von Nutzerkonten

- Doctolib unterscheidet 2 Arten von Nutzer:innen:
  - **„Pro-Account-Nutzer:innen“** mit einem individuellen „professionellen Nutzerkonto“ (Mitarbeitende der Gesundheitseinrichtung)
  - **„Patient:innen“** mit einem individuellen „Patientenkonto“ (Patient:innen, die Termine online gebucht haben)
- Sowohl Patient:innen als auch professionelle Nutzer:innen haben ein individuelles Doctolib-Konto mit spezifischen Rechten, um Daten einzusehen und ggf. zu ändern.
- Jeder Zugang zu einem Nutzerkonto bedarf der Eingabe des Benutzernamens (E-Mail-Adresse, die bei der Registrierung verwendet wurde) und des zugehörigen Passworts, das aus mind. 8 Zeichen bestehen muss.
- Alle Passwörter sind mithilfe einer „bcrypt“-Verschlüsselung in den Doctolib-Datenzentren gesichert.

  Sicherheitsvorkehrungen gegen Brute-Force-Angriffe (Angriffe, bei denen versucht wird, durch Eingabe einer Vielzahl von möglichen Kombinationen aus Buchstaben, Zahlen und Sonderzeichen Zugang zu Daten zu erhalten):
- Pro-Account-Nutzer:innen: bei mind. 10 aufeinanderfolgenden erfolglosen Log-in-Versuchen:
  - automatische Sperrung des Nutzerkontos
  - Benachrichtigung an Kontoinhaber:in, die einen Entsperrungs-Link enthält
- Patientenkonto: bei mind. 10 vergeblichen Log-in-Versuchen innerhalb von 30 Sekunden:
  - Benachrichtigung vom Kontoinhaber:in

Zugriffsrechte auf Patientenkonten

Für Patient:innen, die online ihren Termin buchen

- Wenn Patient:innen Online-Termine via Doctolib buchen, nutzen sie ein Patientenkonto. Dies gilt unabhängig von der Zugriffsart (Zugriff per Link, der in die Websites der Krankenhäuser integriert ist, über die Doctolib-Website oder per App) und unabhängig vom Zugriffsgerät (z. B. Desktop, Handy, Tablet).
- Patient:innen können von jedem Gerät mit einer Internetverbindung (z. B. Desktop, Handy, Tablet) per Browser auf ihre persönlichen Daten unter der folgenden Adresse zugreifen: www.doctolib.de
- Patient:innen können darüber hinaus via iPhone- und Android-App auf ihre persönlichen Daten zugreifen.
- Bei der erstmaligen Registrierung von Patient:innen verlangt Doctolib eine Zwei-Faktor-Authentifizierung, d. h., wenn Neukund:innen ein Patientenkonto erstellen, müssen sie ihre Registrierung mit der Eingabe eines Codes, den sie zuvor per SMS erhalten haben, bestätigen.

Zugriff auf Pro-Account-Nutzerkonten

- Pro-Account-Nutzer:innen können von jedem Endgerät (z. B. Desktop, Handy, Tablet) mit einer Internetverbindung per Browser unter pro.doctolib.de auf ihre persönlichen Daten zugreifen. Professionelle Nutzer:innen können dies darüber hinaus via iPhone- und Android-App tun.
- Es können verschiedene Zugriffsrechte und -level für einzelne Mitarbeitende vergeben werden. Dabei stehen folgende Optionen zur Auswahl: kein Zugriff; Lesezugriff; Lese- und Bearbeitungszugriff bezüglich der Termine exklusive spezifischer Einstellungen; Bearbeitungszugriff bezüglich der Termine inklusive spezifischer Einstellungen; vollwertiger Administratorenzugriff.
- Doctolib bietet mit einer Zwei-Faktor-Authentifizierung ein wirksames Mittel an, um Datensicherheit zu gewährleisten: Wenn professionelle Nutzer:innen sich auf einem neuen Gerät mittels E-Mail-Adresse und Passwort anmelden, müssen sie die Anmeldung durch Eingabe eines 6-stelligen Codes bestätigen, dieser wird per SMS an die jeweilige Mobilnummer geschickt. Das Gerät wird dann für dieses Nutzerkonto als „bekannt“ hinterlegt.
- Die Doctolib-„Zugriffszone“ schützt vor unautorisierten Zugriffen auf professionelle Nutzerkonten von Orten, die nicht zuvor von dem/der Kund:in als solche spezifiziert worden sind:
  - Der/die Kund:in kann für seine/ihre professionellen Nutzerkonten spezifische IP-Adressen definieren, die zu bestimmten Orten gehören. Dann können Nutzer:innen nur von diesen Orten mit dem professionellen Nutzerkonto auf die Daten zugreifen. Dieses Feature verhindert Zugriffe auf die nutzerspezifischen Daten von außerhalb des Krankenhauses, selbst wenn Dritte sowohl die E-Mail-Adresse als auch das Passwort des/der professionellen Nutzer:in erlangt haben sollten.
- Doctolib erstellt eine Historie der letzten 20 Verbindungen inklusive IP-Adresse, Zugriffsort, Geräteart, Datum und Zeit der Verbindung. Diese können professionelle Nutzer:innen in ihrem persönlichen Bereich einsehen.

Berechtigungs- und Zugriffskonzept für Pro-Account-Nutzerkonten

Registrierung und Deregistrierung von Benutzer:innen

Neue Nutzerkonten können entweder von Administrator:innen oder von Doctolib-Customer-Success-Manager:innen angelegt und mit entsprechenden Berechtigungen versehen werden.

Im Laufe des Projekts schulen die Doctolib-Projektmanager:innen die Administrator:innen und legen die benötigten Benutzerkonten an.

Die Konten können von den gesundheitseinrichtungsinternen Administrator:innen oder dem Doctolib-Customer-Success-Team jederzeit bei Bedarf gelöscht werden.

Zuteilung und Änderung von Benutzerzugängen sowie Überprüfung von Benutzerzugangsrechten

Die Berechtigungen der einzelnen Benutzer:innen können jederzeit bearbeitet bzw. mit sofortiger Wirkung entzogen werden.

Die gesundheitseinrichtungsinternen Administrator:innen haben Einsicht in die Liste der Benutzerkonten mit den jeweiligen Berechtigungen.

Die Administrator:innen können die Benutzerkonten den Krankenhauseinheiten hinzufügen, um Zugangsrechte für Gruppen von gleichberechtigten Nutzer:innen zu verwalten.

Bei Passwortänderung oder Sperrung eines Benutzerkontos werden die Administrator:innen per E-Mail darüber informiert.

Verwaltung privilegierter Zugangsrechte

Benutzer:innen mit Administratorrechten haben wichtige Verwaltungsberechtigungen. Sie dürfen das Webprofil der Gesundheitseinrichtung bearbeiten, neue Terminkalender anlegen und anderen Benutzer:innen Administratorrechte verleihen.

Die Administrator:innen haben außerdem sämtliche Berechtigungen eines normalen Benutzerkontos, inklusive:

- Kalender erstellen
- Sprechzeiten erstellen
- Patientenstammdaten verwalten

Verwaltung geheimer Authentifizierungsinformationen von Benutzer:innen

Benutzer:innen benötigen einen **Benutzernamen** und ein Passwort zum Anmelden in der Doctolib-Software.

Alle Passwörter sind mithilfe der **modernsten „bcrypt"-Verschlüsselung** in den Doctolib-Datenzentren gesichert.

Der Informationsfluss zwischen der Browseranwendung und dem Doctolib-Server ist mit einem TLS-Zertifikat signiert und stets verschlüsselt, sodass die Passwörter nicht abgehört werden können.

Bei 10 aufeinanderfolgenden erfolglosen Log-in-Versuchen wird das Nutzerkonto automatisch gesperrt und der/die Kontoinhaber:in hierüber per E-Mail an das entsprechende Konto informiert. Damit bleibt das Konto gegen Brute-Force-Angriffe geschützt und die Authentifi-zierungsinformationen bleiben ebenso geschützt.

Zugangsrechte der normalen Nutzer:innen

Die Zugangsrechte bestimmen, welche Aktionen Nutzer:innen in einem Terminkalender durchführen dürfen. Haben Nutzer:innen Zugriff auf mehrere Terminkalender, können ihre Zugangsrechte für jeden Terminkalender individuell definiert werden.

Termin-, Abwesenheits- und Sprechzeitenverwaltung (vollständiger Zugang)

- Sprechzeiten und Abwesenheiten erstellen/löschen/verändern
- Termine innerhalb und außerhalb der eingestellten Sprechzeiten erstellen/löschen/verändern/duplizieren

Terminverwaltung und Abwesenheitsmanagement

- Abwesenheiten erstellen/löschen/verändern
- Termine innerhalb und außerhalb der eingestellten Sprechzeiten erstellen/löschen/verändern/duplizieren

Terminverwaltung

- Termine innerhalb und außerhalb der eingestellten Sprechzeiten erstellen/löschen/verändern/duplizieren

Terminverwaltung nur innerhalb der Sprechzeiten

- Termine innerhalb der eingestellten Sprechzeiten erstellen/löschen/verändern/duplizieren

Nur Leserecht

- Nutzer:innen haben nur Lesezugriff auf den Terminkalender und können keinerlei Änderungen vornehmen.
- Unmöglich, Termine, Abwesenheiten und Sprechzeiten zu bearbeiten
- Unmöglich, Patient:innen zusammenzuführen, kein Zugang zur Patientenbasis
- Sobald Nutzer:innen Zugriff auf einen Terminkalender haben, können sie auch automatisch die gesamte Patientenbasis der Einrichtung aufrufen bzw. Patient:innen über die Suchleiste finden und sie über Termine informieren.

Erweiterte Zugangsrechte

Krankenhauseinheit

Um ein effektives Verwalten der Nutzerrechte in großen Organisationen wie Unikliniken zu ermöglichen, bietet Doctolib an, Nutzer:innen einer Fachabteilung bzw. einer Klinik zu einer Krankenhauseinheit zusammenzufassen. Die Berechtigungen können für alle Nutzer:innen einer Krankenhauseinheit zentral verwaltet werden. Damit entfällt die Notwendigkeit, jedes Benutzerkonto einzeln zu verwalten. Die Möglichkeit, bei Bedarf Nutzerberechtigungen auf der individuellen Ebene einzelner Benutzer:innen zu verwalten, besteht weiterhin.

Administrator:innen

Administrator:innen haben zusätzlich zu den Berechtigungen der normalen Nutzer:innen folgende Rechte:

- das Webprofil des Krankenhauses zu editieren,
- andere Nutzerkonten zu administrieren,
- Einsicht in die Parameter der Schnittstelle zu haben,
- Benachrichtigungen über kritische Aktionen mit der Doctolib-Software (z. B. Export von Patientenstammdaten, Passwortänderungen) zu erhalten u. v. m.

Verfügbarkeit

Systemverfügbarkeit

- Durch die Verteilung der Doctolib-Serveranwendung auf geografisch getrennte und unabhängige Rechenzentren kann Doctolib eine sehr hohe Verfügbarkeit garantieren. Die Echtzeitreplikation von Daten ermöglicht es, die Doctolib-Anwendung bei einem Serverausfall auf das Ausweichrechenzentrum ohne jeglichen Datenverlust umzuleiten.
- Wir garantieren eine Verfügbarkeit von 99,8 %. In den letzten 12 Monaten konnte Doctolib eine Verfügbarkeit von 99,99 % exklusive/99,90 % inklusive geplanter Wartungen sicherstellen.
- Eine Echtzeitüberwachung aller Komponenten der Systemarchitektur unter dem Einsatz von führender Server-Monitoring-Software, sofortige Fehlererkennung und schnelle Problemlösungsfähigkeiten helfen dabei, Systemfehler zu vermeiden bzw. schnell zu reagieren, bevor es zu Ausfällen kommt.
- Neben permanenten Failover-Tests wird ein komplettes Failover-Verfahren (simulierter Serverausfall) alle 3 Monate durchgeführt, um den Maßnahmenplan zu validieren.
- Im absoluten Katastrophenfall gibt der Disaster-Recovery-Plan die Liste der Maßnahmen vor, mit denen die Doctolib-Anwendung spätestens nach 10 Minuten wieder erreichbar ist.

Anwendungsverfügbarkeit

- Doctolib verfügt über mehrere unabhängige Test- und Qualifizierungsumgebungen, um sämtliche Entwicklungen zu validieren, ohne dabei die Verfügbarkeit des Service in der Liveumgebung zu gefährden.
- Außerdem nutzt Doctolib ein sog. Hot-Deployment-System. Dadurch wird vermieden, dass der Service während eines Updates unterbrochen werden muss. Um die Implementierung ohne Einschränkung der Leistung zu gewährleisten, hat Doctolib einen leistungsstarken und automatisierten Deployment-Prozess implementiert.
- Jede Änderung am Code oder System wird durch das 4-Augen-Prinzip von mind. einem/einer anderen als dem/der ursprünglichen Entwickler:in gegengelesen. Nachdem die Änderung abgezeichnet wurde, durchläuft sie über 14.000 automatisierte Tests, die sämtliche Funktionalitäten der Doctolib-Software in einer Testumgebung prüfen.
- Nachdem die Änderung alle automatischen Tests bestanden hat, wird sie auf die Testumgebung von Doctolib aufgespielt, wo sie vom Doctor-&-Hospital-Supportteam sowie vom Produktteam manuell getestet wird.
- Jeder in der Entwicklung durch manuelle Tests festgestellte Fehler, wird protokolliert, auf Ursachen analysiert und es wird ein Handlungsplan entwickelt, der sicherstellt, dass die gleiche Art von Fehlern nicht wiederholt wird.
- Schlussendlich wird die Änderung in die Liveumgebung eingespielt („deployed“) und es wird ein Logfile der Einspielung gesichert.

Überwachung und Anomaliebehandlung

Audits und Intrusionstests

- Doctolib lässt sein IT-Informationssystem regelmäßig auditieren, um sich vom Sicherheitsniveau zu überzeugen.
- Eine Cybersecurity-Überwachung erfolgt durch ein CSIRT (Computer Security Incident Response Team) für das gesamte Einsatzgebiet von Doctolib.
- Das Sicherheitsteam führt regelmäßig interne Intrusionstests für den gesamten Anwendungsbereich des Informationssystems durch.
- Ein Bug-Bounty-Programm ermöglicht es unabhängigen Personen, Schwachstellen anzuzeigen.

Schutz

- Seit September 2017 werden Sicherheitsthemen durch einen Head of IT Security und dessen Team behandelt.
- Der Prozess besteht darin, dass die Beteiligten (CTO, Infrastruktur-Team, IT, Sicherheitsteam), nachdem der Sicherheitsvorfall definiert ist, diesen und alle damit verbundenen Informationen erfassen, sortieren und klassifizieren und dann die für seine Lösung erforderlichen Maßnahmen priorisieren. Sobald diese Maßnahmen abgeschlossen und verifiziert sind, führen die Beteiligten eine dokumentierte Post-mortem-Analyse durch, um sicherzustellen, dass sich der Vorfall nicht wiederholt.

Verfügbarkeit: Organisation einer ständigen Bereitschaft

Im Hinblick auf die Tätigkeit von Doctolib werden Bereitschaftsdienste für Funktionen eingerichtet, die für die Gewährleistung der Kontinuität des Dienstes, der Wartung, der Sicherheit und der IT für das System wesentlich sind. Die Bereitschaftspolitik von Doctolib ist auf verschiedenen Ebenen strukturiert:

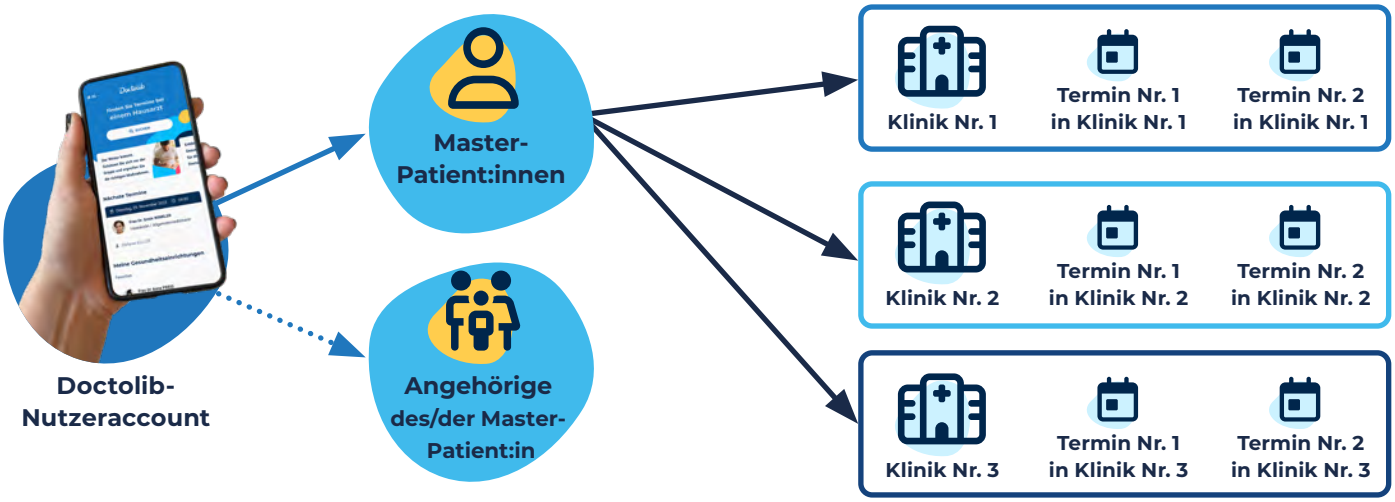
1. Der Bereitschaftsdienst der Ebene 1 wird 7 Tage in der Woche, 24 Stunden am Tag und an jedem Tag des Jahres nach einem rotierenden Zeitplan innerhalb der Tech-Teams zugewiesen. Der Bereitschaftsdienst der Ebene 1 ist für die erste Phase der Analyse und die Lösung des Problems zuständig, wenn dies in seinen Zuständigkeitsbereich fällt.
2. Wenn die Frage komplexer ist, ist der Bereitschaftsdienst der Ebene 1 für die Kontaktaufnahme mit dem Bereitschaftsdienst der Ebene 2 zuständig. Falls Letzterer nicht in der Lage ist, das Problem zu lösen, verfügt er über ein Verzeichnis mit den Telefonnummern der verschiedenen technischen und funktionellen Expert:innen von Doctolib und der verschiedenen Partner von Doctolib, die bei der Verfügbarkeit eine Rolle spielen können (Host, Schnittstellen-Software-Editoren, Anbieter von SMS-Versanddiensten usw.).

Doctolib ist mit Systemen ausgestattet, die den korrekten Betrieb der Plattform permanent überprüfen. Im Fall eines Problems alarmieren diese Systeme den Bereitschaftsdienst der Stufe 1 per SMS/E-Mail und per Telefonanruf.

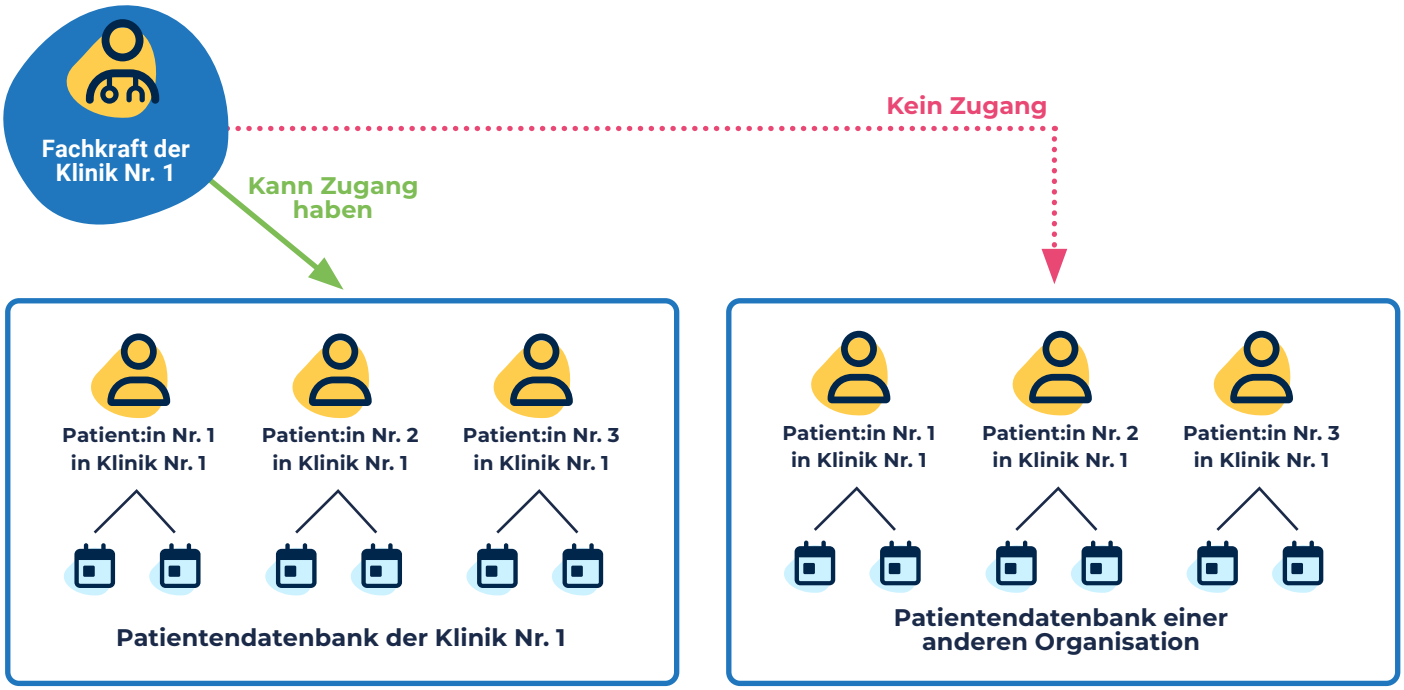
Patiententrennung

Logische Trennung der Patientenbasen

Wenn Patient:innen einen Termin via Doctolib buchen, werden die ihnen zugewiesenen Termine unabhängig voneinander erfasst.



Die Fachkräfte haben nur Zugang zu den Daten ihrer eigenen Patient:innen.



Doctolib

Doctolib ist ein etablierter Partner für Gesundheitseinrichtungen auf dem europäischen Markt und einer der führenden E-Health-Service-Anbieter in Europa.

Doctolib ist ein europäisches E-Health-Unternehmen und trägt mit digitalen Lösungen für Praxen und Krankenhäuser, speziell im Patienten- und Terminmanagement, dazu bei, das tägliche Leben von Gesundheitsfachkräften zu erleichtern. Gleichzeitig bietet Doctolib Patient:innen einen schnellen, unkomplizierten Zugang zu digitalen Services für sämtliche Behandlungsphasen. Bereits über 900.000 Ärzt:innen und Gesundheitsfachkräfte in Deutschland, Frankreich und Italien vertrauen Doctolib. Mehr als 80 Mio. Patient:innen in Deutschland, Frankreich und Italien nutzen Doctolib für ihr Gesundheitsmanagement.

Mehr über Doctolib erfahren:

info.doctolib.de

Mehr über den Datenschutz bei Doctolib erfahren:

about.doctolib.de/privatsphaere

Doctolib GmbH, Mehringdamm 51, 10961 Berlin, Amtsgericht Charlottenburg (Berlin) HRB 175963 B. Geschäftsführer: Nikolay Kolev, Stanislas Niox-Château.
Stand: Januar 2024.