Doctolib

Datenschutz und Datensicherheit bei Doctolib

November 2022

Inhaltsverzeichnis

Grundlagen


?
DSGVO
Doctolib
Doctolib
TÜVIT
2022
Trusted Site
Certificate ID: 5604.22

Zertifikate

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 Zwei-Jahres-Rhythmus zu durchlaufenden Rezertifizierung werden folgende Aspekte geprüft:

- Grundanforderungen an die **Datenschutzorganisation** (DPO, Datengeheimnis, Meldepflichten, Verfahrensverzeichnis, Vorabkontrolle)
- **Technische und organisatorische Maßnahmen** (Zutritt, Zugang, Zugriff, Verfügbarkeit bis hin zur Datentrennung)
- 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

Zwischen den Rezertifizierungen absolviert Doctolib jährlich einen Überwachungsaudit.

TÜV SAARLAND Geprüfter Datenschutz Systemprüfung
tuev-saar.de/TK44448

Doctolib hat das ISO-9001-Zertifikat erhalten

BUREAU VERITAS
Certification

Zertifikat

DOCTOLIB
54 Quai Charles Pasqua
92300 Levallois Perret
Frankreich

Bureau Veritas Certification bestätigt, dass das Management-System der oben genannten Organisation bezüglich und die in den folgenden Normen und Regelwerken festgelegten Anforderungen erfüllt.

Normen / Regelwerk

DIN EN ISO 9001:2015

Geltungsbereich

Entwicklung, Verkauf, Marketing, Bereitstellung eines Pre- und After-Sales Service von Management- und Unterstützungssoftware für die Organisation von Arztpraxen für medizinisches Fachpersonal.

Start Zertifizierungszyklus: 16. Oktober 2020
Vorausgesetzt, dass während der Gültigkeitsdauer dieses Zertifikates alle Anforderungen der Normen kontinuierlich erfüllt sind, ist das Zertifikat gültig bis: 15. Oktober 2023
Rezertifizierung durch Bureau Veritas: 16. Oktober 2020
Zertifikats-Nr.: FR058339-1 Datum: 20. Oktober 2020

Laurent Cangemann (Président)

Seite: 1 von 2

ISO 9001 ist die internationale Norm für Qualitätsmanagementsysteme (QMS) und wurde von der ISO (International Organization for Standardization) entwickelt. Das Qualitätsmanagementsystem, oft kurz als QMS bezeichnet, ist eine Sammlung von Richtlinien, Prozessen, dokumentierten Verfahren und Aufzeichnungen. Diese Sammlung von Dokumentationen definiert ein Set von internen Regeln, die bestimmen, wie ein Unternehmen Produkte oder Dienstleistungen produziert und an die Kunden liefert.

- Starke Kundenorientierung, um den Anforderungen der Gesundheitsfachkräfte nachzukommen
- Internes Wissensmanagement, das alle Mitarbeitenden dazu befähigt, die beste Arbeit zu leisten
- Reaktionsfähigkeit und professionelles Risikomanagement
- Firmenweite Zusammenarbeit auf höchstem Niveau

Doctolib hat das ISO-27001-Zertifikat erhalten

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

ISO 27001 ist die international führende Norm für Informationssicherheits-Managementsysteme (ISMS) 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

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.™

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

BSI (EMEA) Headquarters: 389 Chiswick High Road, London, W4 4AL, United Kingdom
A Member of the BSI Group of Companies.

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

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

Doctolib ist zertifizierter Videosprechstundenanbieter

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.**

Certificate

The certification body of TÜV Informationstechnik GmbH hereby awards this certificate to the company

Doctolib GmbH
Mehringdamm 51
10961 Berlin, Germany

to confirm that its technical procedures for video consultation

Doctolib Videosprechstunde

fulfils all requirements of criteria

Trusted Site Video Consultation, version 2.1

of TÜV Informationstechnik GmbH. The requirements are summarized in the appendix to the certificate.

The appendix is part of the certificate and consists of 5 pages.

The certificate is valid only in conjunction with the evaluation report.

Video Consultation TÜViT 2022 Trusted Site

Certificate validity: 2022-03-29 – 2025-03-29

Certificate ID: 5704.22

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

Essen, 2022-03-29

Dr. Christoph Sutter
Head of Certification Body

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

TO CERTIFICATE

- 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).

DSGVO –

allgemeiner Überblick

Doctolib erfüllt die Anforderungen der DSGVO

Wir beachten die deutschen und europäischen Bestimmungen zum Schutz personenbezogener Gesundheitsdaten, insbesondere die DSGVO und das BDSG.

- Doctolib hat auf Gruppenebene Frau Justine Bourdeu als **Datenschutzbeauftragte** bestellt (Art. 37 Abs. 1 lit. c DSGVO). Frau Bourdeu ist bei der federführenden Aufsichtsbehörde CNIL gemeldet. Sie wird durch ein derzeit 7-köpfiges Datenschutzteam unterstützt, darunter eine Person in Deutschland. Das Datenschutzteam ist in die Rechtsabteilung eingegliedert.
- Doctolib handelt für die Terminverwaltung als **Auftragsverarbeiter** und verarbeitet die Patienten- und Termindaten allein für die im Auftragsverarbeitungsvertrag festgelegten Zwecke und nur im erforderlichen Ausmaß.
- Doctolib wird mittels seiner AGB auf die **Schweigepflicht (§§ 203, 204 StGB)** verpflichtet. Doctolib gibt diese Verpflichtung an die eigenen Mitarbeitenden und an die Auftragsverarbeiter weiter. Eine Entbindung von der Schweigepflicht findet nicht statt.
- Doctolib führt ein ständig aktuelles **Verzeichnis der Verarbeitungstätigkeiten** (Art. 30, § 2) und hat Prozesse für die Sicherstellung von Datenschutz und Datensicherheit eingesetzt. Doctolib hat **Datenschutzfolgeabschätzungen** für den Kalenderservice und den Telekonsultationsservice durchgeführt. Das Ergebnis lautet: akzeptables Restrisiko für die informationelle Selbstbestimmung der betroffenen Personen.
- Doctolib **informiert seine Kund:innen transparent über die Datenverarbeitungen** mittels der Datenschutzhinweise für Gesundheitsfachkräfte sowie durch die Verträge, die Kunden zur Verfügung gestellt werden.
- Doctolib wird jährlich **durch externe Auditoren geprüft** (TÜV Saarland, TÜV IT, ISO 27001, Kundenaudits). Doctolib kann eigene sowie die Zertifikate der Auftragsverarbeiter vorlegen.

Rechtlicher Fokus: Datenschutz

Datenschutz-folgeabschätzungen

DSFA – Zertifikatsbestandteil

- Die durchgeführten DSFA sind regelmäßiger **Prüfgegenstand im Rahmen der TÜV-Zertifizierung** des Patientenbuchungsportals von Doctolib (www.doctolib.de), wobei insbesondere das Datenschutzmanagement, organisatorische und technische Anforderungen überprüft werden.
- Prüfgrundlagen sind u. a. das Bundesdatenschutzgesetz (BDSG), ausgewählte Aspekte des BSI-Grundschutzes, relevante Elemente der ISO 27001, TÜV-spezifische Anforderungen sowie branchenspezifische Gesetze und vertragliche Regelungen.
- Weiterhin ist die DSFA bzgl. der **Zertifizierung der Videosprechstunde** an die unabhängige und von der KBV anerkannte Zertifizierungsstelle des TÜV IT übermittelt und durch diese geprüft worden.
- Die Schwerpunkte dieser Überprüfung liegen auf den Bereichen Datenschutz, Datensicherheit und Verbraucherschutz.

DSFA – Risiken und Maßnahmen

Die Risiken wurden wie folgt bewertet:

Für den Doctolib-Terminkalender

- Unberechtigter Zugang: begrenzt (Zugriff unberechtigter Mitarbeitender des Arztes bzw. der Ärztin)
- Unerwünschte Änderung: begrenzt (z. B. Löschen von Termindaten durch Mitarbeitende des Arztes bzw. der Ärztin)
- Verlust von Daten: vernachlässigbar (ausreichende Schutz- und Überwachungsmaßnahmen)

Für die Doctolib-Telekonsultation

- Unberechtigter Zugang: begrenzt (wie für Terminkalender)
- Unerwünschte Änderung: begrenzt (wie für Terminkalender)
- Verlust von Daten: vernachlässigbar (wie für Terminkalender)

Zur Risikobehandlung identifizierte und schon umgesetzte Maßnahmen

- Einsatz von Verschüsselungstechnologien beim Dokumentenaustausch: umgesetzt
- Dezidiertes Rechtemanagement in der Anwendung: umgesetzt
- Zeitliche Beschränkung der Terminspeicherung: per default Dauer 5 Jahre (Empfehlung der federführenden Aufsichtsbehörde CNIL). Jede Organisation muss bei der Einrichtung von Doctolib die Speicherdauer wählen: 5 Jahre per default beibehalten oder zwischen 1 und 20 Jahren wählen.

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. Die Größe dieses Teams wird sich in den nächsten 2 Jahren verdoppeln.

Art und Dauer der Datenspeicherung im Kalender

Art	Dauer	Erklärung
Termindaten	Per default 5 Jahre, einstellbar durch den Kunden zwischen 1 und 20 Jahre	Verantwortlicher kann Speicherdauer bestimmen
Patientendaten	Je nach Weisung des Verantwortlichen	Verantwortlicher kann Speicherdauer bestimmen
Im Nutzerkonto hinterlegte Daten des bzw. der Ärzt:in/Fachkraft	Bis 3 Monate nach Vertrags-beendigung	Sicherstellung vollständiger Rückerlangung der Daten
IP-Adresse	1 Jahr ab dem Ztp. der Registrierung	Verbesserung der Produktqualität und Sicherheit der Anwendung
Verbindungsdaten der Videosprechstunde	3 Jahre (allg. Verjährungsfrist)	
Antworten auf fakultative Umfragen	1 Monat nach Zusendung	

Löschkonzept

Wir beachten die deutschen und europäischen Bestimmungen zum Schutz personenbezogener Gesundheitsdaten, insbesondere die DSGVO und das BDSG.

EU GDPR COMPLIANT

- 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 vollständige 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.

Hosting auf den europäischen Servern von Amazon Web Service mit Sitz in Luxemburg (AWS)

- Doctolib arbeitet mit AWS als sog. Hosting Provider, d.h., die Daten werden in Rechenzentren der europäischen Tochtergesellschaft von AWS mit Sitz in Luxemburg gespeichert. Konkret beschränkt sich die Speicherung auf Server in der EU (Frankfurt am Main und Paris).
- Die Zulässigkeit des Einsatzes der Luxemburger Tochtergesellschaft von AWS im Gesundheitsbereich wurde zuletzt auch 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.

Schutzmaßnahmen gegen einen Zugriff aus Drittstaaten (Schrems-II-Urteil des EuGH von Juli 2020)

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.

Doctolib arbeitet mit AWS als sog. Hosting Provider, d.h., die Daten werden in Rechenzentren von AWS gespeichert. Wie setzt Doctolib das Schrems-II-Urteil um?

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 (s. Details dazu auf den weiteren Seiten).
3. Doctolib nimmt eine einzelfallbezogene Prüfung der Voraussetzungen einer Datenübermittlung vor und prüft gemäß den Empfehlungen des Europäischen Datenschutzausschusses (EDSA) und der deutschen Datenschutzbehörden, ob und welche Zusatzmaßnahmen zusätzlich zur Verschlüsselung noch sinnvoll sind.

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

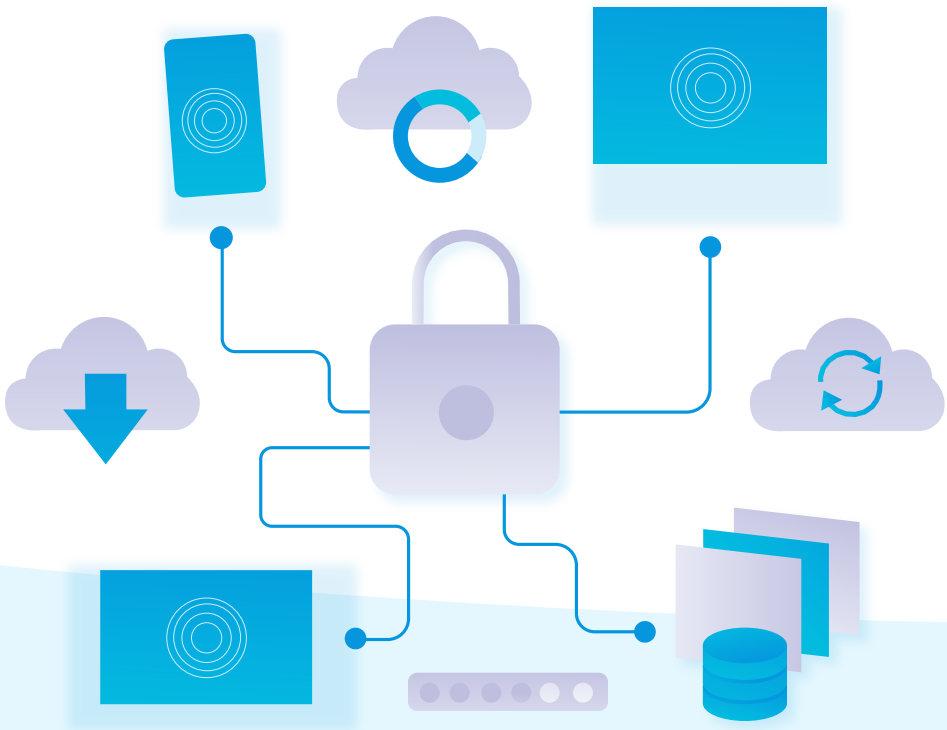
- Beim Transport von Informationen wird eine Verschlüsselung auf Basis von TLS (Transport Layer Security) verwendet.
- Auf den Servern werden die Daten durch **HSM-(Hardware-Security-Modul-)geschützte Schlüssel** verschlüsselt, die wiederum durch einen **Master-Schlüssel** geschützt werden, der im Besitz 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**.

Zusätzlich zu Verschlüsselungslösungen prüfen wir in Form einer einzelfallbezogenen Risikoanalyse, welche Schutzmaßnahmen für die Zusammenarbeit von Doctolib mit Dienstleistern, die in Drittländern ansässig sind oder eine Muttergesellschaft in einem Drittland haben, angemessen sind.

Dabei setzt Doctolib die Empfehlungen des Europäischen Datenschutzausschusses um:

- Auflistung aller geplanten internationalen Transfers
- Prüfung der **Übermittlungsinstrumente** (z. B. SCCs)
- Prüfung des (gesetzgeberischen) Schutzniveaus des Bestimmungsdrittlandes
- Vorbereitung von **zusätzlichen Sicherheitsmaßnahmen**, um ein mit dem der EU gleichwertiges Schutzniveau herzustellen (Prüfbögen, vertraglichen Klauseln etc.)

Mit allen Unterauftragsverarbeitern, die Daten zur Erbringung ihrer Dienstleistung in ein Drittland übertragen oder einer Herausgabepflicht gegenüber staatlichen Behörden unterliegen, werden die neuen SCC verhandelt und technische Zusatzmaßnahmen geprüft. Der genaue Stand der Anpassungen kann auf Anfrage mitgeteilt werden.



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 für Gesundheitsdatenhosting zertifiziert (sog. HDS-Zertifikat, HDS steht für Hébergeurs de Données de Santé).
- Die HDS-Zertifizierung ist ein in Deutschland nicht existierender Schutzstandard speziell für Gesundheitsdatenhosting. 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

aws

Rechtsgrundlage und Einwilligung

Patient:innen buchen über ihr Doctolib-Konto einen Arzttermin. Ist das datenschutzrechtlich zulässig?

- 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 Webseite von Doctolib erfordert das Anlegen eines Nutzerkontos. Dies ist ein gesicherter Bereich, in dem Patient:innen Termine einsehen, stornieren, verschieben können. Sie müssen beim Anlegen des Nutzerkontos eine 2-Faktor-Authentisierung 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. Rechtsgrundlage ist Art. 28 DSGVO in Verbindung mit Art. 6 Abs. 1 b) und Art. 9 Abs. 2 h) DSGVO. Doctolib hat keine Einsicht in Termine von Patient:innen.

Müssen Patient:innen ohne Doctolib-Account in die Verarbeitung ihrer Daten zwecks Terminbuchung einwilligen?

Die Verarbeitung von Patienten- und Termindaten zwecks Terminverwaltung ist ohne Einwilligung zulässig, da sich die Datenverarbeitung auf eine zulässige Auftragsverarbeitung stützt.

Die Gesundheitseinrichtung selbst hat eine Rechtsgrundlage zur Verarbeitung von Patienten- und Termindaten:

- 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. Terminvereinbarungen und -änderungen stellen typische Tätigkeiten von Ärzt:innen und Krankenhäusern dar.
- Laut Art. 6 Abs. 1 b) DSGVO ist die Verarbeitung von Daten erlaubt, wenn dies für die Erfüllung eines Vertrages 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.

Art. 28 DSGVO: Es muss ein Auftragsverarbeitungsvertrag nach Art. 28 DSGVO abgeschlossen werden und der Auftragsverarbeiter muss ausreichende TOMs eingesetzt haben.

- Der Arzt bzw. die Ärztin erteilt Doctolib den Auftrag zur Datenverarbeitung zu einem festgelegten Zweck, nämlich der Terminverwaltung. Doctolib ist streng weisungsgebunden, wie im Auftragsverarbeitungsvertrag festgelegt.
- Die Reform des § 203 StGB aus dem Jahr 2017 ermöglicht, dass ohne Verstoß gegen die ärztliche Schweigepflicht Patientendaten an Doctolib übermittelt werden. Doctolib wirkt an der Tätigkeit der Gesundheitsvorsorge (Terminverwaltung) der Ärzt:innen mit und wird vertraglich auf die Schweigepflicht verpflichtet. Doctolib gibt die Schweigepflicht an Mitarbeitende und Unterauftragsverarbeiter weiter.
- Die für die Anwendung von Doctolib erforderlichen Daten werden ausschließlich bei besonders für das Hosting von **Gesundheitsdaten zertifizierten Hostern** gehostet (sog. Health Data Hosting). Sämtliche TOMs sind als Anhang des Auftragsverarbeitungsvertrages aufgelistet.

Die Verarbeitung von Patienten- und Termindaten ist daher ohne Einwilligung der Patient:innen zulässig. **Patient:innen müssen jedoch über den Einsatz von Doctolib als Auftragsverarbeiter informiert werden. Doctolib stellt gerne ein Muster zur Verfügung.**

Ist der Import von Daten von Bestandspatient:innen zwecks Terminverwaltung zulässig?

Der Import der bestehenden Patientendaten (beschränkt auf die für die Terminverwaltung erforderlichen Daten) ist ebenfalls ohne Einwilligung möglich.

- Die Arbeit mit einem Auftragsverarbeiter erfordert keine Einwilligung der von der Datenverarbeitung betroffenen Personen. Die Auftragsverarbeitung (Art. 28 DSGVO) in Verbindung mit Art. 9 Abs. 2 h) und Art. 6 Abs. 1 b) DSGVO stellt eine wirksame Rechtsgrundlage für die Übertragung von Daten an Doctolib dar.
- Doctolib handelt als Auftragsverarbeiter streng nach Weisung und auf Grundlage eines DSGVO-konformen Auftragsverarbeitungsvertrages.
- Doctolib beachtet das Gebot der Datenminimierung. Jede Gesundheitseinrichtung kann abweichend von der Standardeinstellung (5 Jahre) die Aufbewahrungsdauer der Termine einstellen. Die getroffene Einstellung findet auch auf importierte Daten Anwendung. Wird eine Einstellung z. B. von 2 Jahren gewählt, werden alle administrativen Daten, die mit Terminen zusammenhängen, die älter als 2 Jahre sind, gelöscht.

Ist es zulässig, dass Patient:innen Terminerinnerungen erhalten?

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 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.

Auftrags-verarbeitungsvertrag

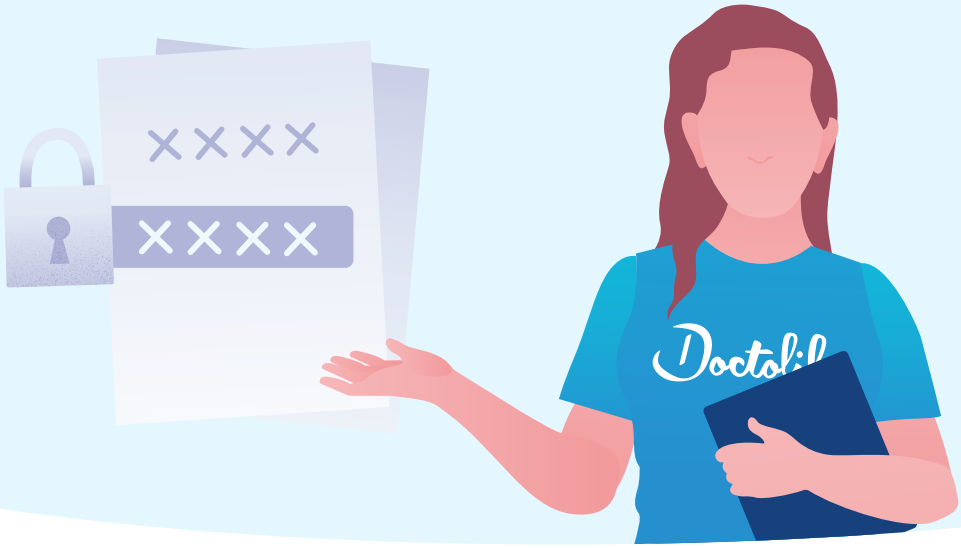
Wann muss der Auftragsdatenverarbeitungsvertrag abgeschlossen werden?

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 Auftragsdatenverarbeitungsvertrag.

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 [...].“*

Patienteninformation und Schweigepflicht

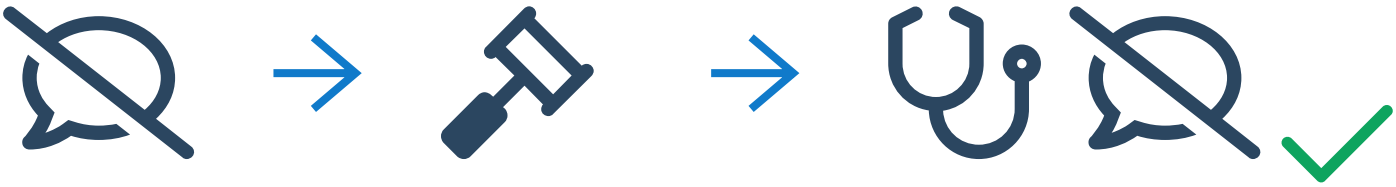


Müssen Patient:innen über die externalisierte Datenverarbeitung informiert werden?

- **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 Webseite
  - 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.

Verpflichtung von Doctolib auf die Schweigepflicht

Schweigepflicht nach § 203 Abs. 1, Abs. 4 S. 1 StGB, § 204 StGB



Reform des § 203 StGB vom 9. November 2017

- Einführung des § 203 Abs. 3 S. 2
- Erlaubt das Offenbaren von fremden Geheimnissen gegenüber Dritten, soweit dies für die Inanspruchnahme der Tätigkeit der mitwirkenden Personen erforderlich ist

Doctolib wird über die AGB und den Auftragsverarbeitungsvertrag auf die Schweigepflicht nach §§ 203, 204 StGB verpflichtet und über die Strafbarkeit belehrt.

Doctolib gibt die Verpflichtung auf die Schweigepflicht an die Mitarbeitenden und an die Unterauftragnehmer weiter.

Eine Entbindung von der Schweigepflicht ist nicht erforderlich und nicht relevant.

Technischer 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 **4096-Bit-Schlüssel**, ausgestellt vom höchst angesehenen und vertrauenswürdigen Aussteller **GeoTrust** und signiert durch **SHA-256** mit **RSA**.
- Darüber hinaus bieten wir, wo erforderlich, einen **IPsec-VPN-Tunnel** zur vollständigen Verschlüsselung der Datenverbindung an.
- 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 **verschlüsselt**.
- Eine **zusätzliche Verschlüsselungsebene** wird auf **sensible Daten** angewendet, um den Zugriff auf die Daten durch die Datenbankadministrator:innen zu verhindern.

Schlüsselmanagement

- Doctolib verwendet 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 verwenden 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 ebenfalls 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 24x7), Anti-DDoS-Schutz

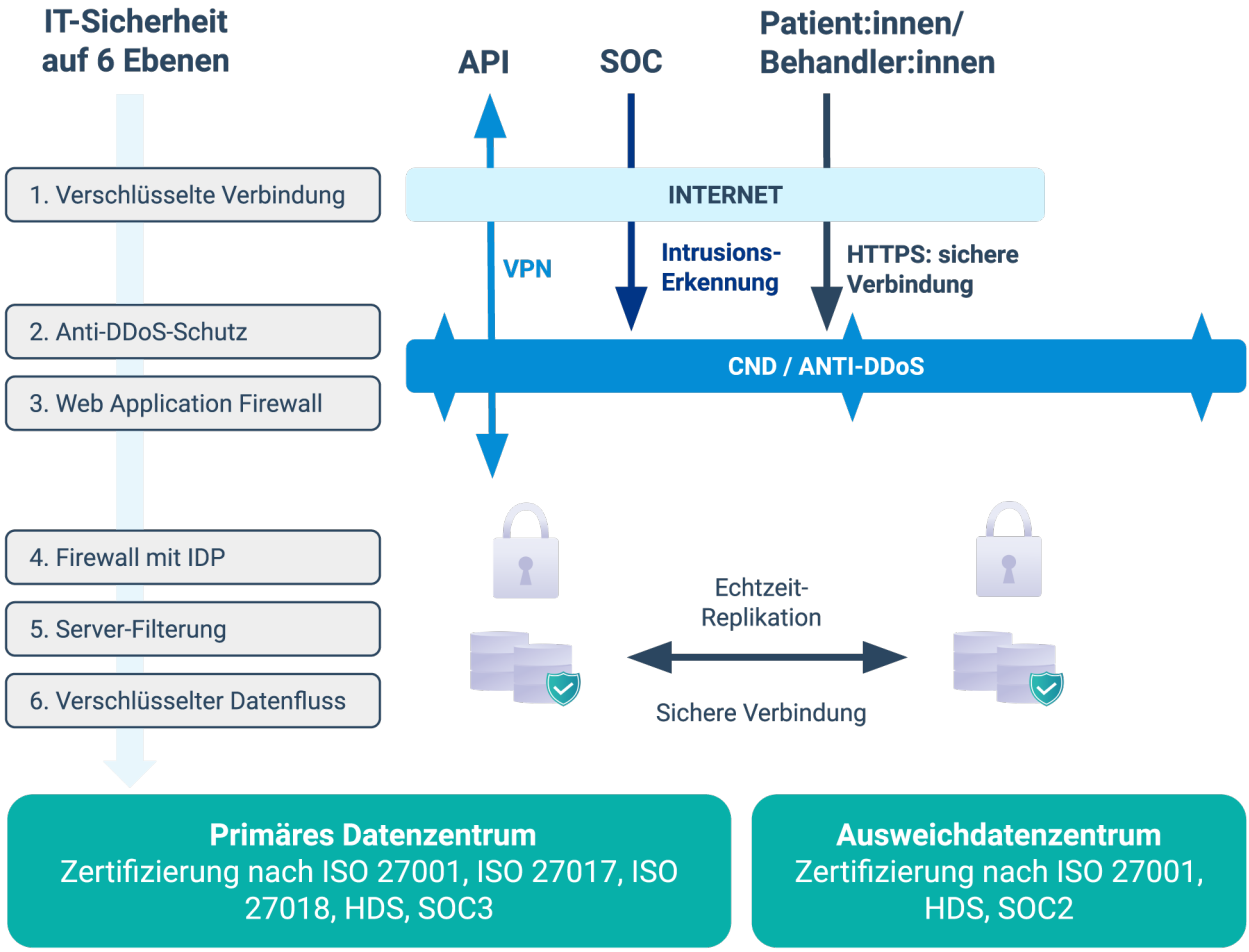
Datentrennung

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

Mittel

- Security by Design: integriert im Code mit allen Entwickler: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)

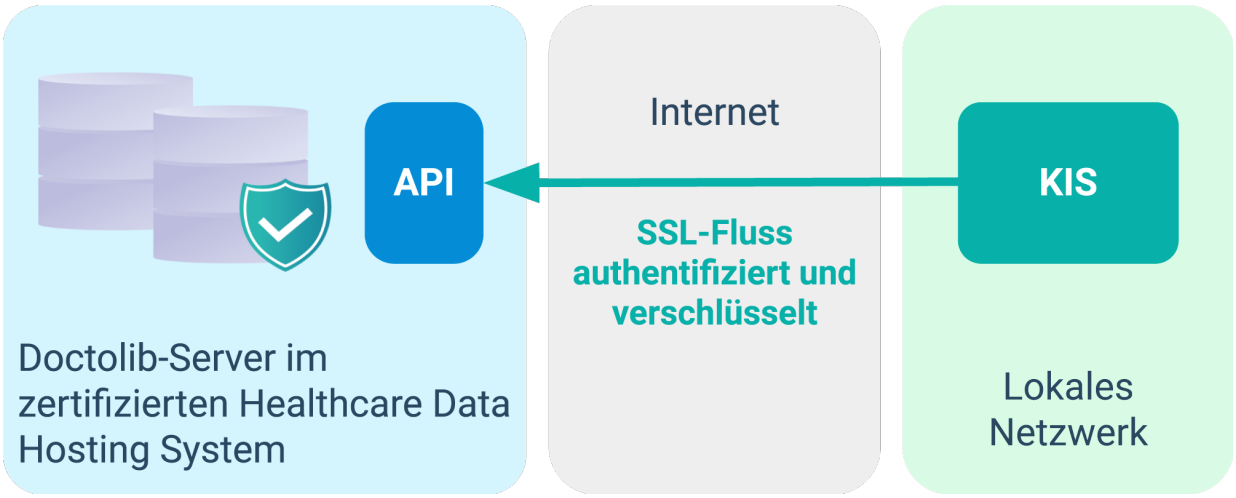
IT-Sicherheit durch verteilte Server-Architektur



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

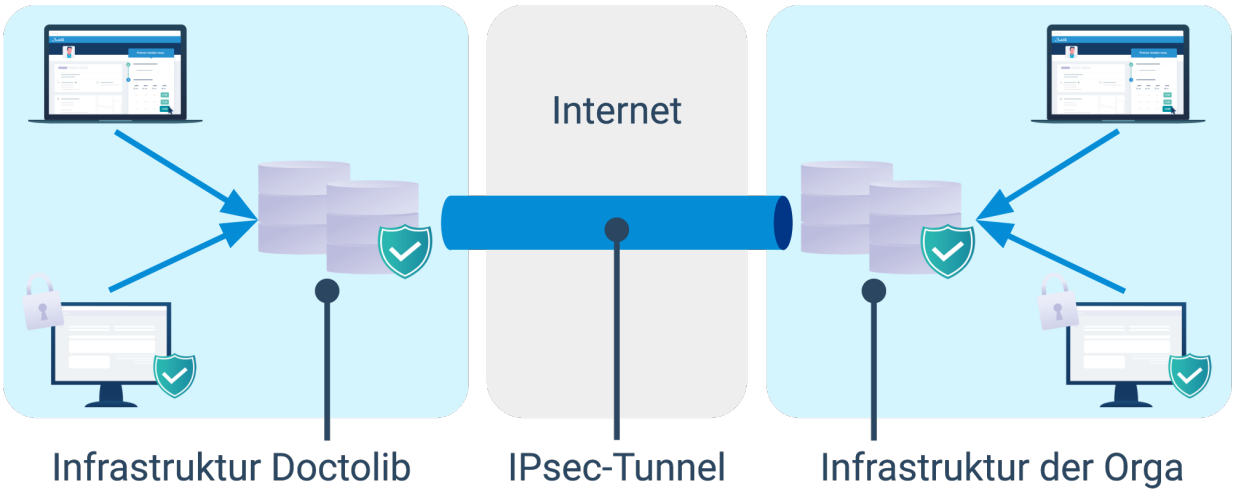
Sichere Datenübertragung zwischen Datenzentren und Einrichtungen

Option 1: HTTPS- und HMAC-Verschlüsselung (APISync)



- Mit API Sync 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.

Option 2: Server-to-Server-IPsec-VPN-Tunnel



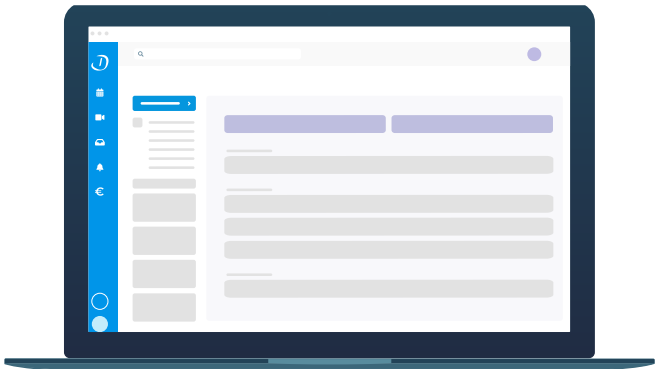
- IPsec-Tunnel: Diese Technologie erlaubt es räumlich getrennten Benutzer:innen, so zu kommunizieren, als ob sie sicher mit demselben lokalen Netzwerk verbunden wären.
- Durch IPsec wird die Vertraulichkeit, Authentizität und Integrität der übertragenen Daten geschützt.
- Quell- und Zieladressen beider Netzwerke werden verschlüsselt.
- Meldungen sind bidirektional in HL7.

Weitere Sicherheitsmaßnahmen der Doctolib-Rechenzentren

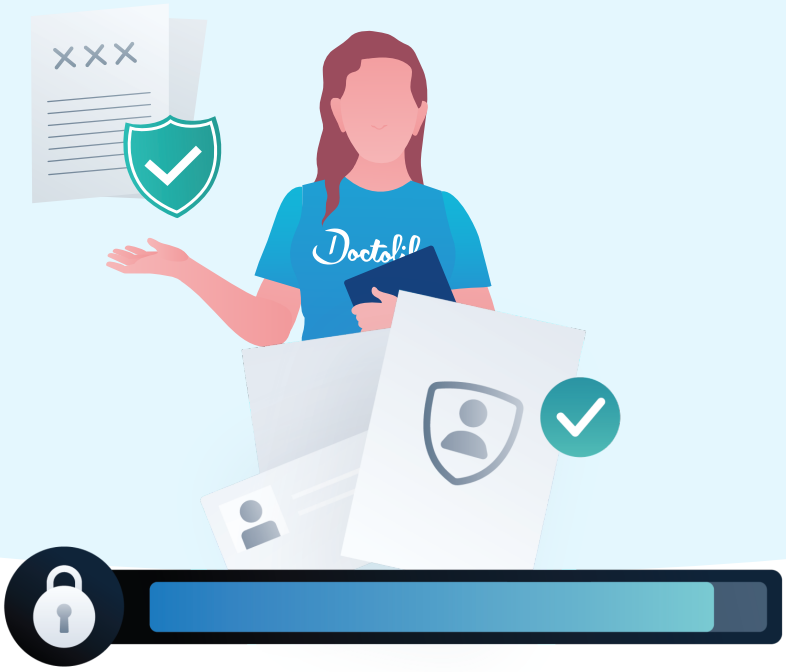
- Das System und die Netzwerkumgebung von Doctolib sind mit einer State-of-the-Art-Firewall-Technologie geschützt.
- Doctolib hat technische Maßnahmen gegen Denial-of-Service-(DDos-)Angriffe implementiert (z. B. Arbor Networks).
- Die Doctolib-RZ verfügen über starke physische Sicherheitsstandards im 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-RZ (z. B. Hypervisoren, Betriebssysteme, Router, DNS-Server).
- Doctolib benutzt eine WAF (Web Application Firewall), um Angriffe auf die Web-Services 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.
- 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, zu 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

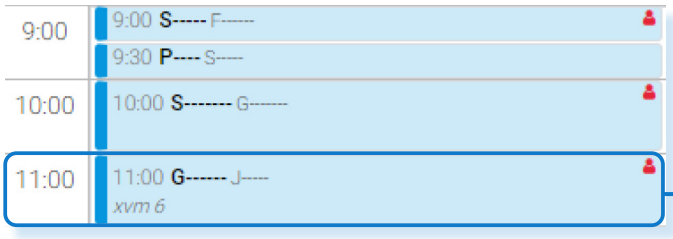


Zugangsbeschränkung für Doctolib-Mitarbeitende: Pseudonymisierung der Daten

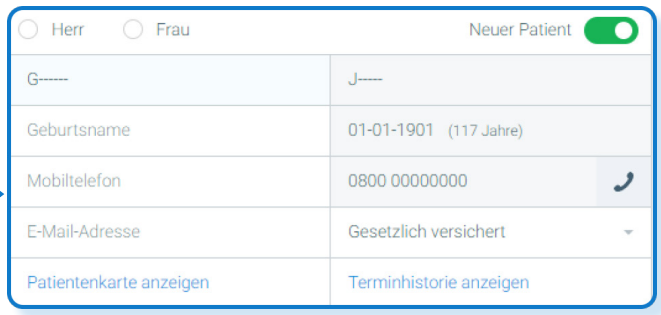
Doctolib-Mitarbeitende haben standardmäßig keine Einsicht in Daten, die in einem Terminkalender eines Arztes oder einer Ärztin eingetragen sind. Alle Stammdaten und Termindaten sind für Doctolib-Mitarbeitende nur pseudonymisiert sichtbar:

- 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

- Zugang 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 betreffenden Kunden oder 3) nach Vereinbarung und unter der Kontrolle des Kunden 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 min. 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 min. 10 aufeinanderfolgenden, erfolglosen Log-in-Versuchen:
    - Automatische Sperrung des Nutzerkontos
    - Benachrichtigung des/der Kontoinhaber:in, der/die einen Entsperrungs-Link enthält
  - Patientenkonto: bei min. 10 vergeblichen Log-in-Versuchen innerhalb von 30 Sekunden:
    - Benachrichtigung des/der 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 auf den Webseiten der Krankenhäuser integriert ist, über die Doctolib-Webseite 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 2-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:innenkönnen von jedem Endgerät (z. B. Desktop, Handy, Tablet) mit einer Internet-verbindung per Browser unter pro.doctolib.de auf ihre persönlichen Daten zugreifen. Professionelle Nutzer:innen können darüber hinaus via iPhone- und Android-App auf ihre persönlichen Daten zugreifen.
- Es können verschiedene Zugriffsrechte und -level für einzelne Mitarbeitende vergeben werden; dabei stehen folgende Optionen zur Auswahl: kein Zugriff; Lesezugriff; Lese- und Bearbeitungszugriff bzgl. der Termine exklusive spezifischer Einstellungen; Bearbeitungszugriff bzgl. der Termine inkl. spezifischer Einstellungen; vollwertiger Administratorenzugriff.
- Doctolib bietet mit einer 2-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 vom Kunden als solche spezifiziert worden sind:
  - Der Kunde kann für seine 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 sollte.
- Doctolib erstellt eine Historie der letzten 20 Verbindungen inkl. 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

1. 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-Prokejtmanager: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.

2. 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.

3. 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 vergeben.

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

- Kalender erstellen
- Sprechzeiten erstellen
- Patientenstammdaten verwalten

4. Verwaltung geheimer Authentifizierungsinformation 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 Authentifizierungsinformationen bleiben 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.

1. Termin-, Abwesenheits- und Sprechzeitenverwaltung (= vollständiger Zugang)

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

2. Terminverwaltung und Abwesenheitsmanagement

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

3. Terminverwaltung

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

4. Terminverwaltung nur innerhalb der Sprechzeiten

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

5. Nur Leserecht

- Nutzer:innen haben nur einen Lesezugriff auf den Terminkalender und können keinerlei Änderungen vornehmen
- Unmöglich, Termine, Abwesenheiten und Sprechzeiten zu bearbeiten
- Unmöglich, Patient:innen zusammenzuführen. Kein Zugang auf die 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 der 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 Echtzeit-Replikation von Daten ermöglicht es, die Doctolib-Anwendung im Falle eines Serverausfalls 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 % exkl./99,90 % inkl. 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 anderen als dem ursprünglichen Entwickler gegengelesen. Nachdem die Änderung abgezeichnet wurde, durchläuft sie über **14.000 automatisierte** Tests, die sämtliche Funktionalitäten der Doctolib-Software in einer Testumgebung prüft.
- Nachdem die Änderung alle automatischen Tests bestanden hat, wird sie auf die **Testumgebung** von Doctolib aufgespielt, wo sie vom Doctor & Hospital Support Team sowie dem Produktteam **manuell getestet wird.**
- Jeder Fehler, der in der Entwicklung durch manuelle Tests festgestellt wird, 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 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, den Vorfall 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 Postmortem-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:

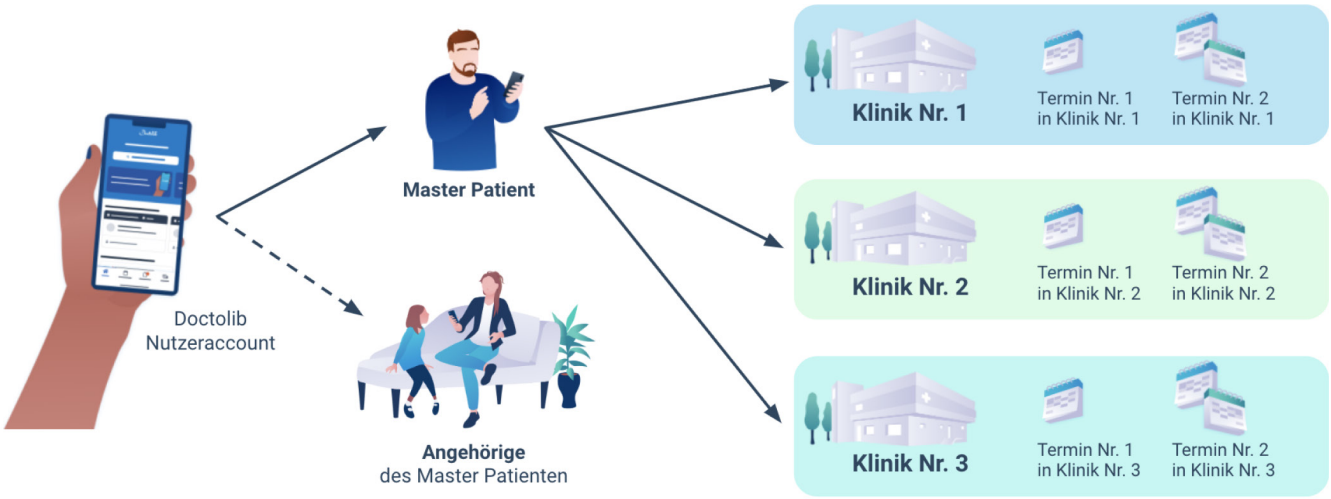
1. **Der Bereitschaftsdienst der Ebene 1 wird 7 Tage in der Woche, 24 Stunden am Tag und an jedem Tag des Jahres** nach einem rotierenden Zeitplan innerhalb der Tech-Teams zugewiesen. Der Bereitschaftsdienst der ersten Ebene ist für die erste Phase der Analyse und die Lösung des Problems zuständig, wenn 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 Falle eines Problems alarmieren diese Systeme den Bereitschaftsdienst der Stufe 1 per SMS/E-Mail und per Telefonanruf.

Mandantentrennung

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

Doctolib bietet Gesundheitseinrichtungen eine Softwarelösung für die Patienten-, Zuweiser- und Terminverwaltung. Bereits über 320 000 Ärzt:innen und Gesundheitsfachkräfte in Deutschland, Frankreich und Italien vertrauen Doctolib. Mehr als 70 Mio. Patient:innen in Deutschland, Frankreich und Italien nutzen Doctolib zur Buchung und Verwaltung ihrer Arzttermine.

Mehr über Doctolib erfahren:

info.doctolib.de

Mehr zum 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