



Unsere Verpflichtungen zum Schutz der persönlichen Daten unserer Nutzer:innen

Wir bei Doctolib sind der Meinung, dass persönliche Daten und Gesundheitsinformationen besonders schützenswert sind. Als europäisches Unternehmen, das Online-Services sowohl für Ärzt:innen und Gesundheitsfachkräfte als auch für Patient:innen anbietet, fühlen wir uns dem Schutz der Daten und der Privatsphäre unserer Nutzer:innen zutiefst verpflichtet. Aus diesem Grund haben wir seit unserer Gründung im Jahr 2013 eine Vielzahl von Sicherheitsmaßnahmen ergriffen und erforschen fortlaufend neue Technologien.

WIR VERPFLICHTEN UNS, DATEN UNSERER ZU SCHÜTZEN

1° Wir setzen eine breite Palette von Schutzmaßnahmen ein und entwickeln laufend neue Sicherheitstechnologien.

- Wir schützen die Konten unserer Nutzer durch: Standardmäßige 2-Faktor-Authentifizierung sowohl für die Accounts von Patienten als auch von Gesundheitsfachkräften, Komplexitätsanforderungen an Passwörter und kryptografische Speicherung, Rollenbasierte Zugriffskontrolle.
- Wir entwickeln unsere Software in Übereinstimmung mit den Best Practices des Open Web Application Security Project (OWASP), einer anerkannten gemeinnützigen Stiftung, die sich für die Verbesserung der Sicherheit von Software einsetzt. Dies beinhaltet.
- Unsere Infrastruktur wird geschützt durch: Moderne Cloud-Firewalls, Härtung aller IT-Systeme, Systeme zur Abwehr von unbefugtem Zugriff (Intrusion Detection and Prevention Systems), Zugangskontrollsysteme, 24/7 Sicherheitszentrale (Security Operations Center - SOC), DDoS-Abwehr.

2° Unsere Nutzer profitieren von modernsten Verschlüsselungsverfahren.

- Alle Daten bei Doctolib sind verschlüsselt, sowohl im Ruhezustand als auch bei der Übertragung.
- Darüber hinaus haben wir zusätzliche Sicherheitsmaßnahmen getroffen:
 - Für die Verschlüsselung von Daten im Ruhezustand werden darüber hinaus Master-Schlüssel beim Anbieter ATOS gespeichert, wodurch eine zusätzliche Schutzebene geschaffen wird, die den Zugriff selbst durch unseren eigenen Hosting-Lösungsanbieter verhindert.
 - Für die Verschlüsselung der Daten während der Übertragung setzen wir eine TLS-Verschlüsselung (Transport Layer Security) ein, ein kryptografisches Protokoll, das für die Sicherheit von Kommunikation über Computernetzwerke entwickelt wurde. Der Verschlüsselungskanal wird immer in Europa abgeschlossen und durch unsere Web-Application-Firewall (Cloudflare) von Schadddaten gesäubert. Die TLS-Zertifikate von Doctolib werden dank der Keyless-Handshake-Methode niemals an Cloudflare weitergegeben.
- Wir greifen zudem auf fortschrittliche Verschlüsselungstechnologien wie die Ende-zu-Ende-Verschlüsselung oder die serverseitige Verschlüsselung zurück und werden auch in Zukunft neue technologische Möglichkeiten untersuchen und selbst weiterentwickeln.

3° Die Daten unserer Nutzer sind an einem sicheren Ort.

- Wir haben uns für AWS (Amazon Web Services) als Datenhosting-Lösung entschieden, da es sich um eine der fortschrittlichsten und sichersten Lösungen auf dem Markt handelt.
- AWS ist nach den wichtigsten internationalen Normen, einschließlich ISO/IEC 27001, zertifiziert und wird regelmäßig auditiert.
- In Deutschland hat AWS das vom Bundesamt für Sicherheit in der Informationstechnik (BSI) ausgestellte C5-Zertifikat erhalten.
- Die AWS-Rechenzentren sind rund um die Uhr physisch gesichert.

4° Wir unterziehen uns regelmäßig Zertifizierungen, externen Audits und behördlichen Kontrollen.

- Doctolib ist in Deutschland und Frankreich nach ISO/IEC 27001 und in Frankreich nach HDS ("Healthcare Data Storage") von der BSI Group, einer führenden internationalen Zertifizierungsstelle, zertifiziert worden: Dies zeigt, dass wir die erforderlichen Prozesse (auf der Basis von Risikomanagement) und die besten Verfahren implementiert haben, und ist ein Ausdruck unseres langfristigen Engagements für den Datenschutz. Die Zertifizierungen beinhalten jährliche Kontrollprüfungen und Erneuerungsaudits alle 3 Jahre.
- In Deutschland ist das Doctolib-Patientenportal auch nach "TÜV Geprüfter Datenschutz" durch den TÜV Saarland und die Doctolib-Videosprechstunde nach "Trusted Site Data Privacy und Trusted Site Video Consultation" durch TÜViT zertifiziert. Beide Zertifizierungen werden jährlich durch ein Überwachungsaudit bestätigt und alle 2 ("TÜV Geprüfter Datenschutz") bzw. 3 Jahre ("Trusted Site Data Privacy und Trusted Site Video Consultation") durch ein vollständiges Zertifizierungsaudit erneuert.

5° Der Stellenwert von Sicherheitsbelangen spiegelt sich in unseren langfristigen Investitionen wider.

- Seit der Gründung von Doctolib im Jahr 2013 haben wir erheblich in den Datenschutz investiert.
- Wir haben ein großes Team von technischen und juristischen Experten für Sicherheit und Datenschutz in Paris und Berlin.

WIR FOLGEN STRENGEN DATENSCHUTZSTANDARDS

6° Wir verkaufen keine Daten unserer Nutzer.

- Das Geschäftsmodell von Doctolib basiert hauptsächlich auf einem Abonnement, das von Angehörigen der Gesundheitsberufe und Gesundheitseinrichtungen für die Nutzung unserer Softwarelösungen bezahlt wird.

7° Alle Daten werden in Europa gespeichert.

- Die Daten werden in Frankreich (Paris) und in Deutschland (Frankfurt) bei einem anerkannten Hosting-Anbieter gespeichert: AWS (Amazon Web Services).

8° Datenschutz steht bei der Entwicklung unserer Dienste im Mittelpunkt.

- Unsere Sicherheits- und Rechtsexperten arbeiten Hand in Hand mit den Tech- und Produktteams, um die Entwicklung neuer Dienste von ihrer Konzeption bis zu ihrer Markteinführung zu begleiten.

9° Unsere Dienste sind so konzipiert, dass sie den nationalen und europäischen Datenschutzbestimmungen entsprechen.

- Seit unserer Gründung steht die Einhaltung aller Vorschriften zum Schutz personenbezogener Gesundheitsdaten im Vordergrund unseres Handelns: die europäische

Datenschutzgrundverordnung (GDPR), die Datenschutzrichtlinie für elektronische Kommunikation (ePrivacy) und lokale Datenschutzgesetze: Loi Informatique et Libertés (LIL) in Frankreich, Bundesdatenschutzgesetz (BDSG) und Datenschutz-Grundverordnung (DSGVO) in Deutschland und der Codice in materia di protezione dei dati personali in Italien.

10° Unsere Kunden können ihre Datenschutzeinstellungen jederzeit selbst anpassen.

- 2-Faktor-Authentifizierung bei der Verbindung mit ihrem Account auf einem neuen Gerät.
- Ein zusätzlicher 4-stelliger Code, um den Zugang zu ihrer mobilen Anwendung zu begrenzen.
- Entsperrung ihrer mobilen App über Face ID / Touch ID (iOS-Geräte) oder über Fingerabdruck (Android).

Stanislas Niox-Chateau
Geschäftsführer & Mitgründer von Doctolib



Nikolay Kolév
Geschäftsführer von Doctolib Deutschland

