SICHERHEITS-WHITEPAPER

Wie wir bei Speakap die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen bewahren

Version 4.3 - April 2026

speakap

Inhaltsverzeichnis

Einleitung

Heutzutage ist die Informationssicherheit ein Muss für jedes moderne SAAS-Unternehmen. Bei Speakap haben wir immer die Meinung vertreten, dass unsere Kunden ihre Daten besitzen sollten und deshalb haben wir seit jeher auf Datenschutz geachtet. Wir begrüßen die erhöhte Aufmerksamkeit für diese Themen – sie ist für alle Unternehmen und Konsumenten von Vorteil.

Informationssicherheit war schon immer ein wichtiger Teil all unserer Prozesse bei Speakap, aber mit dem Wachstum unseres Unternehmens und unseres Kundenstocks, ist die Notwendigkeit eines formalen Informationssicherheits-Managementsystems (ISMS) noch mehr in den Vordergrund getreten.

Über die letzten Jahre haben wir Verfahren und Strategien dokumentiert und regelmäßige Kontrollen und Revisionen durchgeführt. Wir haben auch unsere Systeme und Anlagen überprüft und den Eigentümern spezifische, dokumentierte Verantwortungen zugeteilt. Zu guter Letzt haben wir ein Risikobeurteilungsverfahren implementiert, das uns hilft unsere Bemühungen zu leiten, wenn es zu der Verbesserung und Einführung von Informationssicherheitskontrollen kommt.

Mit einem ISO 27001 konformen Managementsystem können wir den Bestimmungen von Verordnungen wie der DSGVO entsprechen, aber es versichert auch, dass wir unsere Vertragspflichten gegenüber Kunden und Lieferanten einhalten.

Auf den folgenden Seiten finden Sie eine Zusammenfassung all der betrieblichen und technischen Maßnahmen, die Speakap in Bezug auf Informationssicherheit gesetzt hat.

Unser risikobasierter Ansatz erlaubt uns die Informationssicherheit in den Bereichen, wo sie am wichtigsten ist, ständig zu verbessern.

Bart van Wissen
CTO

Anwendungssicherheit

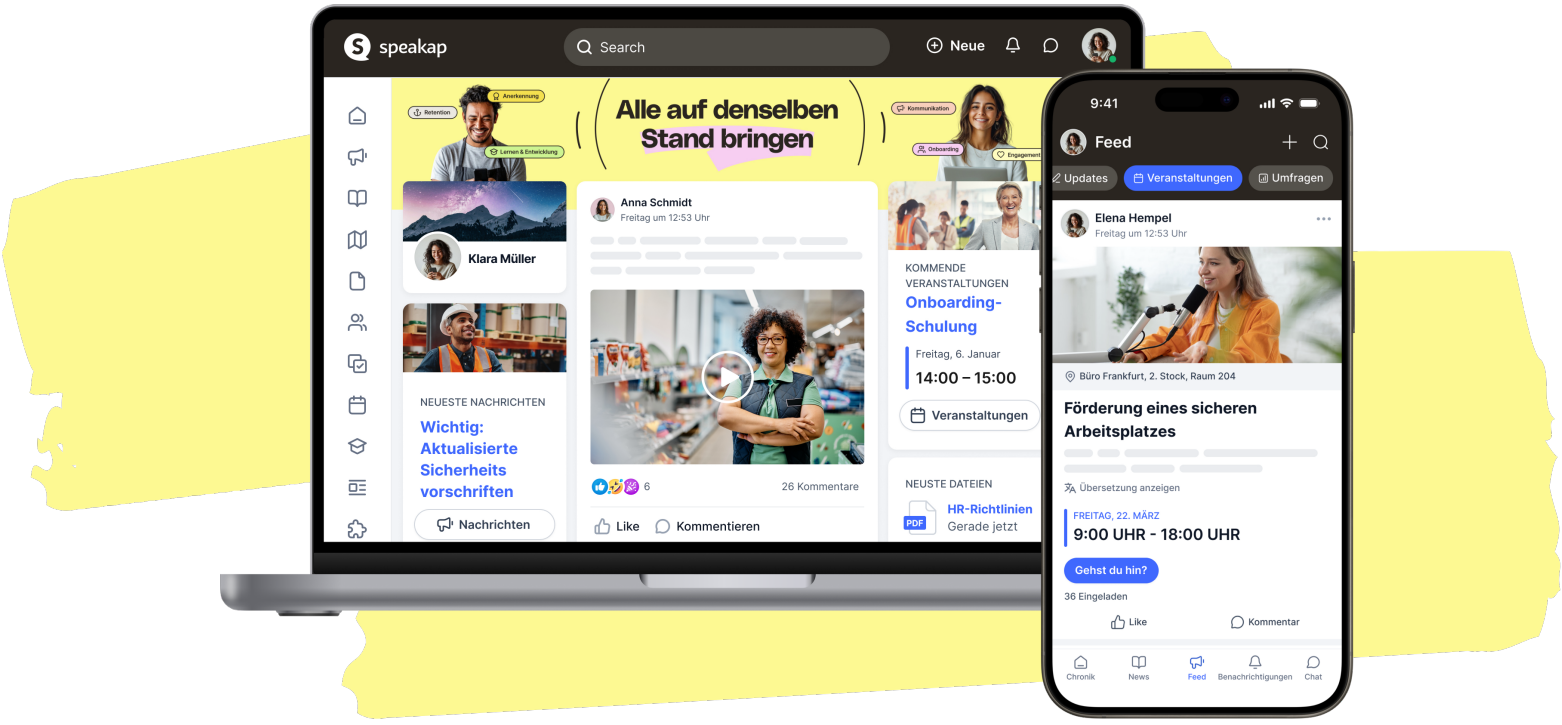
Speakap versichert, dass die Nutzer der Plattform Zugang zu genau den Daten haben, für die sie die Zugriffsberechtigung haben. Das Sicherheitsmodell der Anwendung basiert auf:

- Nutzern: Das sind die Mitglieder Ihrer Organisation, die von ernannten Administratoren innerhalb der Organisation verwaltet werden. Alle Mitglieder der Organisation (des Netzwerks) haben eine Rolle, welche die Nutzerrechte auf der Netzwerkebene bestimmt.

- Nachrichten: Können entweder geschützt in Privatnachrichten gesendet werden, was bedeutet, dass nur der Sender und Empfänger Zugang haben; oder in einer Gruppe oder mit der gesamten Organisation geteilt.

- Chroniken, auf denen die Daten in Form einer Nachricht geteilt werden.

- Gruppen mit Mitgliedschaften, die von bestimmten Administratoren in der Gruppe oder auf Organisationsebene verwaltet werden. Alle Mitglieder einer Gruppe haben in der Gruppe eine Rolle, die ihre Rechte festlegt. Gruppen haben ihre eigenen Chroniken und Inhalte, die in der Gruppe geteilt werden (von Gruppe abhängig) sind nur für Mitglieder der Gruppe zugänglich.



Web-Sicherheit

- Alle Verbindungen zum und vom Backend sind über HTTPS mit mindestens TLS 1.2 gesichert (TLS 1.3 wird bevorzugt). Es werden starke Verschlüsselungsverfahren eingesetzt, darunter AES-256-GCM und ChaCha20-Poly1305 mit ECDHE-Schlüsselaustausch, der Perfect Forward Secrecy bietet.
- Das ältere und schwächere SSL Protokoll wird nicht mehr verwendet.
- Sensible Cookies werden mit sicheren HttpOnly-Flags versehen.
- Der gesamte User Input wird vor der Verarbeitung bestätigt. Es wird besondere Vorsicht darauf gelegt Cross Site Scripting (XSS), Cross Site Request Forgery (CSRF) und SQL-Einschleusung zu vermeiden.

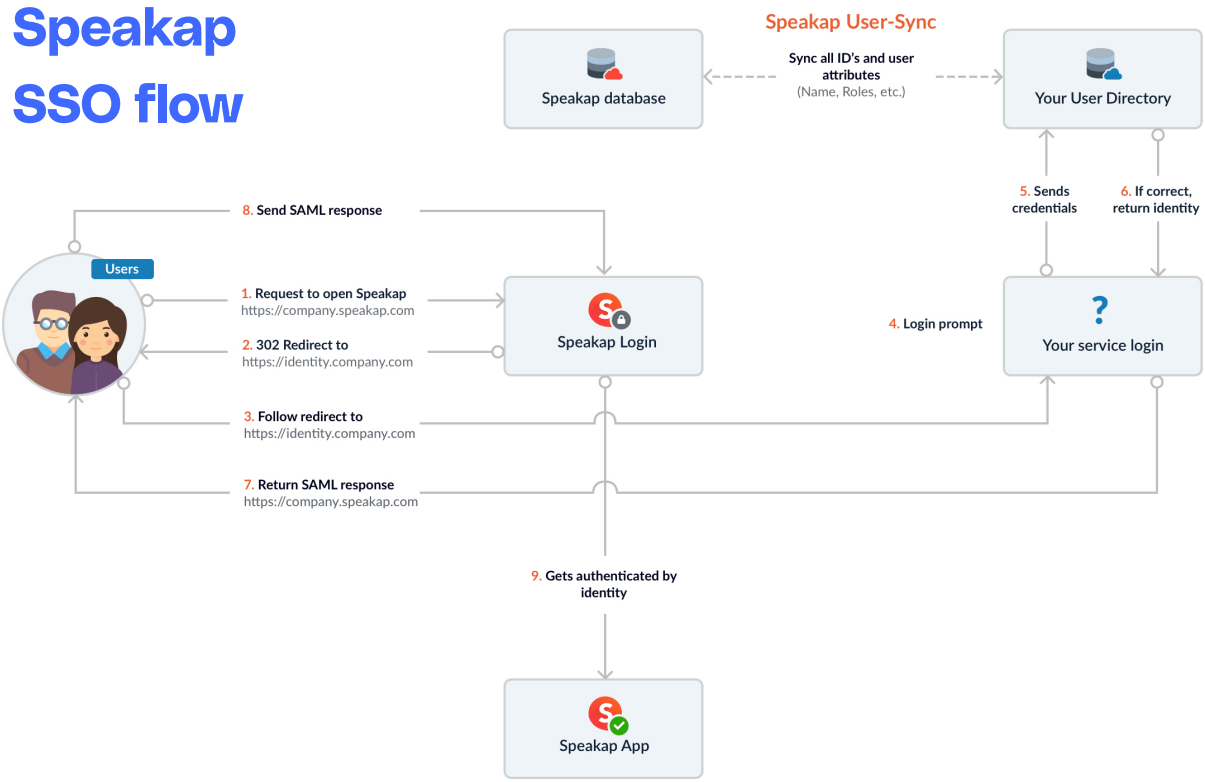
Malware-Schutz

- Vom Nutzer hochgeladene Dateien werden beim Hochladen automatisch auf Malware überprüft und abgelehnt falls Malware entdeckt wird.
- Malware Definitionen werden regelmäßig und automatisch aktualisiert.

Authentifizierung und Passwörter

- Speakap API Authentifizierung basiert auf OAuth 2.0. Zugriffstokens haben eine Länge von 100 Bytes, werden mit einem Pseudozufallszahlengenerator von OpenSSL hergestellt und haben eine Lebensdauer von einer Stunde, danach müssen sie neu geladen werden.
- Alle aktiven Zugangstokens werden zurückgezogen, wenn ein Nutzer sein Passwort ändert.
- Für einen einmaligen Log-In kann SAML 2.0 verwendet werden.
- Das Ausloggen auf einem Gerät funktioniert auch aus der Entfernung.
- Passwörter haben eine Mindestlänge von 10 Zeichen, müssen mindestens einen Kleinbuchstaben, einen Großbuchstaben und ein nicht alphabetisches Zeichen enthalten.

- Passwörter werden als Salt-Hashes, durch den BCrypt Algorithmus verschlüsselt, gespeichert, Speakap hat also keine Kenntnis der eigentlichen Passwörter.
- Um sein Passwort zu ändern, muss der Nutzer immer das alte Passwort angeben.
- Wenn ein Passwort vergessen wurde, kann ein Nutzer die Zurücksetzung anfordern. Ein geheimer Link, um das Passwort zurückzusetzen wird an die primäre E-Mail-Adresse des Nutzers gesandt.
- E-Mail-Adressen müssen mit einem geheimen Token verifiziert werden, bevor sie als primäre E-Mail-Adressen verwendet werden können.
- Passwörter werden nie auf dem Gerät oder Browser des Nutzers gespeichert: stattdessen wird ein OAuth Token sicher gespeichert.
- Der Token wird von den Mobilgeräten gelöscht, wenn der Nutzer sich abmeldet oder die App deinstalliert.
- Authentifizierungstokens laufen automatisch ab, wenn sie längere Zeit nicht verwendet werden.



Datenverschlüsselung

- Alle Daten auf Speichersystemen und im Datenverkehr werden verschlüsselt.
- Alle Verbindungen zum und vom Backend sind über HTTPS mit mindestens TLS 1.2 gesichert (TLS 1.3 wird bevorzugt). Es werden starke Verschlüsselungsverfahren eingesetzt, darunter AES-256-GCM und ChaCha20-Poly1305 mit ECDHE-Schlüsselaustausch, der Perfect Forward Secrecy bietet.
- Das ältere, schwächere SSL Protokoll ist deaktiviert.
- Kundendaten werden in Speichersystemen mit dem AES-256 Algorithmus verschlüsselt.
- Passwörter werden unter Verwendung des hochsicheren BCrypt Algorithmus als Hashes gespeichert.

E-Mail-Schutzmaßnahmen

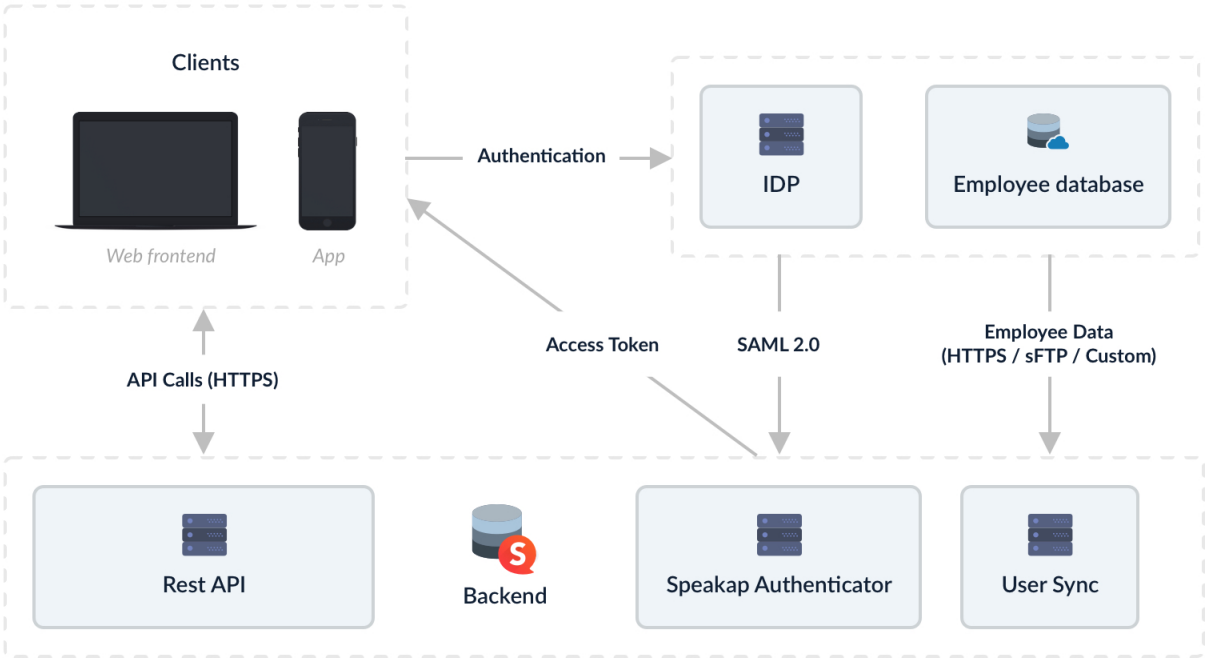
- Ausgehende Transaktions-E-Mails werden über AWS SES versendet und unterliegen umfassenden Authentifizierungsmaßnahmen.
- Bei allen ausgehenden Emails wird eine DKIM-Signatur angewandt.
- Absenderfälschung wird durch SPF verhindert.
- Die DMARC-Richtlinie wird mit einer "Reject"-Aktion für E-Mails durchgesetzt, die die Authentifizierungsprüfungen nicht bestehen, und bietet so umfassenden Schutz vor E-Mail-Spoofing und Phishing-Angriffen.

Schutz der Server und Infrastruktur

- Die Produktionsumgebung ist in mehrere sichere Zonen eingeteilt, der Verkehr zwischen ihnen ist mit Firewall Regeln gesichert.
- Zugang zu der Produktionsumgebung erfordert eine VPN Verbindung mit verpflichtender 2- Faktor Authentifizierung.

- Eine limitierte Gruppe von leitenden Systemingenieuren hat Zugang zu den Servern in der Produktionsumgebung.
- Das Least-Privilege Prinzip wird angewandt.
- Alle Dienste werden von Firewalls gesichert.
- Auf allen Servern werden alle Schnittstellen und Dienste standardmäßig blockiert und erst geöffnet, wenn die Dienste erfordert werden.
- Speakap Server werden über ein zentralisiertes Konfigurationsmanagement System zur Verfügung gestellt, das eine sichere, einheitliche Konfiguration über alle Server sicherstellt. Auf alle Konfigurationsdaten wird eine Versionskontrolle angewandt.
- Sicherheitskritische Patches werden innerhalb von 24h der Verfügbarkeit installiert.
- Speakap Server sind automatisch gegen DDoS Angriffe geschützt.

Speakap Architecture overview



Protokollierung und Überprüfung

- Tätigkeiten, die von Nutzern in der App ausgeführt werden, werden in einem zentralisierten Auditprotokoll aufgezeichnet.
- Server-Protokolle, die für die Sicherheit relevant sind werden auf eine zentralisierte Art gespeichert, werden analysiert und haben ein automatisiertes Warnsystem.
- Rund-um-die-Uhr-Überwachung und ein automatisiertes Warnsystem stellen sicher, dass die Speakap-Systemingenieure schnell handeln können im Falle einer Servicestörung.

Katastrophenwiederherstellung, Backup und Redundanz

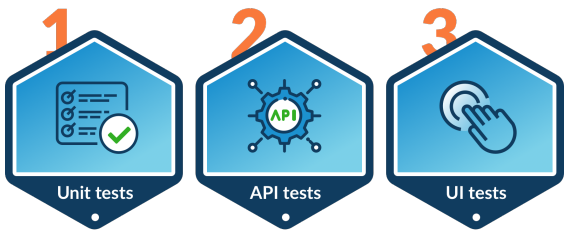
- Speakap garantiert 99,8% Betriebszeit, mit Ausnahme von geplanten Wartungszeiten.
- Alle wesentlichen Services werden redundant aufgesetzt, um eine hohe Verfügbarkeit zu versichern, in den meisten Fällen mit einer automatischen Ausfallsicherung.
- Die Kundendaten werden mehrere Male am Tag gesichert und einen Monat lang gespeichert, so dass im Notfall Daten wiederhergestellt werden können.
- Verschlüsselte Backups werden über mehrere AWS Availability Zones innerhalb derselben Region (EU oder USA) verteilt gespeichert und bieten so geographische Trennung und Redundanz bei gleichzeitiger Einhaltung der Anforderungen an die Datenlokalisierung.
- Speakaps Katastrophenwiederherstellungsplan hilft im Notfall alle Dienste schnell wiederherzustellen.

Datenzentren

- Die Datenzentren, in denen Speakap untergebracht ist, sind ISO 27001:2013 zertifiziert.
- Die Backend-Systeme von Speakap werden bei Amazon Web Services gehostet, wobei sich die Rechenzentren für europäische Kunden in Europa und für US-Kunden in den Vereinigten Staaten befinden.
- Die Kundendaten befinden sich entweder im EU-Rechenzentrum oder im US-Rechenzentrum. Es findet keine Datenübertragung zwischen diesen Standorten statt und der Kunde hat die volle Kontrolle über den geografischen Standort der Daten.
- Physischer Zugang zu den Datenzentren und Servern wird nur befugtem Datenzentrum-Personal gewährt.

Sicherheit bei der Entwicklung

- Speakap Entwicklungsumgebungen sind von der Test- und Produktionsumgebung getrennt.
- Produktionsdaten werden nie für Testzwecke verwendet.
- Produktionsdaten werden nie von der Produktionsumgebung zur Testumgebung übertragen.
- Bei jeder Veränderung im Speakap Code werden automatisierte Testreihen durchgeführt und die Änderungen werden erst umgesetzt, wenn alle Tests bestanden sind. Zusätzlich wird manuell getestet und die Qualitätssicherung in einer isolierten Testumgebung durchgeführt, die für normale Nutzer nicht zugänglich ist.
- Alle Veränderungen im Speakap Code werden einem Peer-Review von leitenden Entwicklern, die ein breites Wissen der Anwendungssicherheit besitzen, unterzogen. Die Anwendung wird mit den Best Practices der Branche entwickelt und es werden Maßnahmen gesetzt, um die in den OWASP Top 10 gelisteten Schwachstellen zu vermeiden.



Sicherheitsprüfungen, Penetrationstests und automatisierte Tests

- Mindestens einmal im Jahr werden von einer externen, unabhängigen Sicherheitsfirma eine Reihe von Penetrationstests durchgeführt.
- Zusätzlich betreiben wir ein Security-Bug-Bounty-Programm, das über eine Ethical-Hacker-Plattform abgewickelt wird.
- Tägliche, automatisierte SSL Server-Tests versichern, dass unsere SSL-Konfiguration immer dem Branchenstandard entspricht.
- Die Zugangskontrolle der Anwendung werden regelmäßigen Tests unterzogen, die bei jeder Veränderung und bei jedem Release gemacht werden.

- Alle Änderungen an der Anwendung werden einer umfangreichen Reihe von API- und Integrationstests sowie Einheitstests und statischen Analysen unterzogen.
- Kunden können auf Anfrage ihre eigenen Penetrationstests durchführen.

Organisation und Verwaltung

- Risikobewertung und die Analyse der Geschäftsauswirkungen werden regelmäßig durchgeführt.
- Die ISMS wird sowohl intern als auch extern jährlich geprüft, so wie es von der ISO 27001:2013 Norm verlangt wird.
- Informationssicherheits-Bewusstseinstrainings garantieren bei der gesamten Belegschaft ein Bewusstsein über die Sicherheitsrisiken und Kontrollen.
- Personal mit Zugang zu Kundendaten wird vor der Einstellung überprüft.
- Entwickler müssen vor der Einstellung ein tiefgehendes Wissen über Sicherheitsthemen vorweisen.
- Um sensible Daten zu schützen, unterzeichnen Speakap Mitarbeiter bei der Einstellung eine Vertraulichkeitsvereinbarung.
- Richtlinien für einen sauberen Arbeitsplatz und Desktop bei Speakap garantieren Vertraulichkeit in unseren Büros.
- Die Arbeitsgeräte der Mitarbeiter müssen starke Passwörter, eine Festplattenverschlüsselung und eine automatische Bildschirmsperre haben.
- Speakaps Passwort-Richtlinie erfordert, dass die Mitarbeiter bei allen Systemen starke, einzigartige Passwörter verwenden und dass wenn möglich zusätzliche Maßnahmen wie Zwei-Faktor Authentifizierung gesetzt werden.
- Richtlinien zur Informationsklassifikation, zusammen mit dokumentierter Information und Asset-Handling Verfahren garantieren Vertraulichkeit, Integrität und Verfügbarkeit von sensibler Information.
- Alle Richtlinien haben zugewiesene Besitzer und werden regelmäßig überprüft.
- Zugangsverwaltungsverfahren versichern, dass den Mitarbeitern der Zugang zu Systemen gegeben und genommen werden kann, wenn Änderungen eintreten, so wie beim Onboarding, dem Beenden eines Arbeitsverhältnisses oder einer Änderung in der Funktion innerhalb des Unternehmens.

Vorfallsreaktion

- Speakap hat ein dokumentiertes Informationssicherheitsvorfall-Reaktionsverfahren, um sicherzustellen, dass alle Verantwortlichkeiten klar definiert sind und im Fall eines sicherheitsrelevanten Ereignisses die richtigen Maßnahmen ergriffen werden.

- Speakap hat ein dokumentiertes Verfahren für die Meldung von Verletzungen personenbezogener Daten, das sicherstellt, dass entsprechend den DSGVO-Artikeln 33 und 34 die richtigen Personen benachrichtigt werden.

Compliance

- Speakap hat ein Informationssicherheitsmanagementsystem und ist ISO 27001:2013 zertifiziert.

- Speakap ist DSGVO-konform.

- Speakap wurde von einem unabhängigen Prüfer einer erfolgreichen Prüfung nach SOC 2 Typ II hinsichtlich des Designs, der Implementierung und der operativen Effektivität der internen Kontrollmaßnahmen unterzogen.

- Speakap ist HIPAA-konform und erfüllt die Anforderungen der HIPAA-Sicherheitskontrollen.

- Wir haben mit allen Unterauftragsverarbeitern Datenverarbeitungsübereinkommen erstellt.

- Speakap hat einen zugewiesenen Datenschutzbeauftragten.

- Speakap wird Anfragen zur Strafverfolgung an den Kunden weiterleiten (außer wenn rechtlich nicht erlaubt) so dass der Kunde entscheiden kann, ob er die angefragte Information preisgeben, oder die Anfrage ablehnen will.

www.speakap.de