Datenschutz-Folgeabschätzung

Version 2.4

Autor: Joost Bruggeman, Arvind Rao, Paul Willems, Jordi van Duyne, Sassan Sangsari
Publikum: Patienten und deren Angehörige, medizinisches Fachpersonal, IT-Fachleute, Datenschützer und Behörden, Siilo-Anwender, Siilo-Kunden
Stichwörter: DSGVO, General Data Protection Regulation, DSFA, Datenschutz-Folgenabschätzung, sensible Informationen, Sicherheit, Privatsphäre, Transparenz
Zweck: Dieses Dokument erklärt, wie Siilo die Daten von Benutzern und Nachrichten, die von unseren Benutzern gesendet werden, schützt. Dieses Dokument kann als Input für Datenschutz-Folgenabschätzungen (Data Protection Impact Assessments, DPIAs) unserer Kunden und Nutzer verwendet werden.
Abstrakt: Die wichtigste Determinante zum Schutz von Privatsphäre und Sicherheit in Software-Plattformen wie dem Siilo Messenger ist die Unternehmenskultur. Zum Beispiel, wie gut nimmt ein Unternehmen das Feedback von Nutzern, Datenschutz- und Sicherheits-Communities an, wie wird dieses Feedback eingeladen und wie transparent ist ein Unternehmen über dieses Feedback. Dieses Dokument soll dies aufzeigen und beschreibt, welche (persönlichen) Daten auf/von Siilo geteilt und gesammelt werden, welche Datenschutz- und Sicherheitsrisiken damit verbunden sind und was getan werden kann, um diese Daten zu schützen.
Unsere Bitte an Sie, unseren Leser: möchten wir Sie einladen, uns Ihre Meinung darüber mitzuteilen, was wir sammeln, wie wir es sammeln, und wie wir die Informationen aus diesen Quellen verarbeiten und schützen. Wir hoffen auch, dass die Sprache und die Erklärungen, die in diesem Dokument angeboten werden, für jeden mit Interesse an unserem DSFA-Dokument zugänglich sind. Wenn dies nicht der Fall ist oder Sie andere Fragen oder Feedback für uns haben, senden Sie uns bitte eine E-Mail an privacy@siilo.com und geben Sie in der Betreffzeile bitte "DFSA" an.
Wichtiger Hinweis: dies ist ein "lebendes" Dokument. Es wird ständig bearbeitet und aktualisiert, genau wie Wikipedia-Artikel.

Revisionshistorie

Revision	Datum	Initiator	Art der Änderung
1.0	10-12-2018	-	Ausgangsversion
1.1	13-03-2020	Paul Willems & Jordi van Duyne	Aktualisierung des Kapitels 3: Siilo Sub-Prozessoren
2.0	22-04-2020	Jasper Aarts & Jordi van Duyne	Detaillierte Übersicht der Subprozessoren hinzugefügt
2.1	06-07-2020	Jordi van Duyne	Spezifikationen für Siilo Connect hinzugefügt
2.2	01-09-2020	Jordi van Duyne	Standardvertragsklauseln (SCCs) für Unterauftragsverarbeiter hinzugefügt
2.3	07-01-2021	Jordi van Duyne	Sub-Prozessoren hinzugefügt
2.4	25-02-2021	Jordi van Duyne & Jasper Aarts	Metadaten hinzugefügt

Inhalt

1.0 Einführung

Diese Datenschutz-Folgenabschätzung (DSFA) ist Teil der Verpflichtung von Siilo gegenüber unseren Nutzern und deren Patienten sowie den (zukünftigen) Kunden von Siilo, um ihnen zu helfen, zu verstehen, wie Siilo mit personenbezogenen Daten in Bezug auf den allgemeinen Datenschutz (DSGVO) umgeht.

Die DSGVO betrachtet gesundheitsbezogene Daten als besonders privat. Gemäß der DSGVO müssen Angehörige der Gesundheitsberufe ihre Gewohnheiten beim Teilen von Patientendaten ernsthaft überdenken. Dies umfasst nicht nur die Art der Programme, die sie auf ihren Smartphones verwenden, sondern auch ihr Verhalten in Bezug auf die Weitergabe von Patientendaten.

Der Druck auf das klinische Personal nimmt zu, und die Qualität ihrer Entscheidungsfindung hängt von der Qualität und Effizienz der Informationen ab, die zwischen den Teams im Gesundheitswesen fließen. Heutzutage aggregieren medizinische Fachkräfte auf der ganzen Welt Patienteninformationen auf ihren mobilen Geräten, um Patienten die bestmögliche Versorgung zukommen zu lassen. Tatsächlich haben mehrere von Ärzten geleitete Studien gezeigt, dass die klinische Entscheidungsfindung schneller, effizienter und von höherer Qualität sein kann, wenn Messenger-Apps auf Smartphones in der klinischen Kommunikation eingesetzt werden. Das Konzept der Privatsphäre ist in der Tat eine starke Überlegung in den Köpfen der medizinischen Fachkräfte, aber es kann manchmal durch das Streben nach einer optimalen Patientenversorgung überschattet werden.

In diesem Dokument nehmen wir eine detaillierte Analyse vor, wie Siilo personenbezogene Daten verarbeitet, welche Risiken damit verbunden sind und wie wir sicherstellen, dass diese Risiken vermieden, minimiert und angemessen verwaltet werden. Für die technischen Details zu unserer Kryptographie und anderen Sicherheitsmaßnahmen lesen Sie bitte unsere Sicherheits-Whitepapers. Für die medizinisch-rechtlichen Details, wie Messenger-Apps im Gesundheitswesen eingesetzt werden sollten, lesen Sie bitte unsere rechtlichen White Papers, die Ihnen im Ressourcen-Bereich unserer Website www.siilo.com zur Verfügung stehen.

1.1 Verantwortung und Gesetzgebung

Bevor sie Inhalte mit Kollegen über ihr Smartphone teilen, ist der übliche Schritt von medizinischem Fachpersonal die vollständige Anonymisierung von Patientendaten. Obwohl dies als logischer und standardisierter Ansatz erscheinen mag, kann es in der Tat mit bestimmten medizinischen Gesetzen in Konflikt geraten, die in erster Linie auf den Schutz der Patienten abzielen. Wenn z. B. unvollständige Patienteninformationen zu Verwirrung im Pflegeteam und unsachgemäßer Behandlung führen, könnte die Patientenversorgung und -sicherheit gefährdet sein. Daher sollten im Interesse der Patientensicherheit der Informationsaustausch und professionelle Diagnosen innerhalb von Pflegeteams niemals anonym erfolgen. Abhängig vom Zustand des Patienten und seiner Behandlungsbeziehung zu seinem Arzt sollte ein unterschriebenes Dokument der informierten Zustimmung zur Weitergabe von Informationen in Erwägung gezogen werden; die teilende Fachkraft muss diese Beziehung als Leitfaden nutzen, wenn es um Fragen der Patienteneinwilligung geht. Siilo hat mehrere juristische White Papers auf der Website veröffentlicht, um Fachleute bei diesem Entscheidungsprozess zu unterstützen. Der Inhalt dieser Papiere befasst sich damit, wie Fachleute das Konzept der DSGVO unter Berücksichtigung ihrer länderspezifischen medizinischen Gesetzgebung angehen sollten, wenn sie klinische Kommunikations-Messenger-Anwendungen verwenden. Es liegt jedoch immer in der Verantwortung der einzelnen medizinischen Fachkräfte, ihren eigenen persönlichen Verhaltenskodex sowie die internen Richtlinien ihrer Organisation zu befolgen.

Als Anbieter einer App, die sensible Patientendaten enthält, weiß Siilo, wie wichtig der Schutz und die Verarbeitung von Informationen im Auftrag seiner Nutzer ist. Um einen sicheren Datenschutz zu gewährleisten, sollte der Umgang mit sensiblen Daten in einer Auftragsverarbeiter-Vereinbarung klar definiert werden, die von jedem Nutzer der App unterzeichnet wird. In dieser Vereinbarung sollte der Anbieter der App als "Verarbeiter" und der Nutzer als

"Verantwortlicher" der Patientendaten definiert werden. Im Fall von Siilo ist die Siilo Holding B.V. der Verarbeiter der Nachrichtendaten, die sich unsere Nutzer gegenseitig senden.

1.2 Meldungsdaten vs. Nutzdaten

Siilo unterscheidet zwischen zwei Arten von Daten:

- Meldungsdaten: dies bezieht sich auf Daten, die von unseren Nutzern aneinander gesendet werden. Da medizinisches Fachpersonal die Hauptnutzer der Siilo App sind, ist es größtenteils zu erwarten, dass unsere Nutzer sensible Informationen und persönliche Daten über die Gesundheit von Patienten (betroffenen Personen) übertragen. Vereinfacht ausgedrückt, ist Siilo ein Verarbeiter von Nachrichtendaten; unsere Nutzer sind die Controller der Nachrichtendaten.
- Nutzdaten: dies bezieht sich auf die personenbezogenen Daten der Nutzer, die Siilo erheben muss, um einen sicheren und konformen Betrieb der Siilo App zu gewährleisten. Siilo ist ein Controller für Nutzerdaten; unsere Nutzer sind die Datensubjekte.

Wie jede Organisation verarbeitet auch Siilo Informationen über seine Kunden, Mitarbeiter, Lieferanten und Partner. Diese Informationsquellen fallen jedoch nicht in den Geltungsbereich dieses Dokuments, können aber per E-Mail unter privacy@siilo.com abgerufen werden.

1.3 Siilos Netzwerk-Funktionen

Die Gesundheitsversorgung ist viel zu komplex geworden, als dass siloartige medizinische Netzwerke existieren könnten; ein alternder und multimorbider Patient wird wahrscheinlich von mehreren Spezialisten aus mehreren Organisationen über mehrere Versorgungslinien hinweg behandelt. Zu den weiteren Entwicklungen gehört, dass hochvolumige und wenig komplexe Behandlungen zunehmend aus den Krankenhäusern heraus verlagert und näher am Wohnort der Patienten erbracht werden. Entwicklungen wie diese verdeutlichen die Tatsache, dass siloartige professionelle Strukturen potenziell kontraproduktiv sein können. Siilo hat erkannt, dass das 21. Jahrhundert die neue Ära der "Netzwerkmedizin" ist, in der Patienten schließlich in der Lage sein werden, ihr eigenes medizinisches Netzwerk zu definieren und zu kontrollieren. Diese neue Ära sieht eine Entwicklung von Consumer-Networking-Tools vor, die es den Nutzern ermöglichen, Verbindungen zu knüpfen, während sie gleichzeitig ihre Privatsphäre und professionelle Distanz wahren. Um diesen Übergang bei der Bereitstellung einer effizienten interdisziplinären, transmuralen Versorgung zu unterstützen, erleichtert Siilo die DSGVO-konforme Vernetzung von medizinischem Fachpersonal (d.h. das "Herstellen von Verbindungen") zum Nutzen der Patientenversorgung. Auf Siilo können Sie haben:

- **Verbindungen 1. Grades;**
- **Verbindungen 2. Grades;**
- **Siilo Network-Verbindungen, und;**
- **Organisationsverzeichnis-Verbindungen.**

Verbindungen 1. Grades sind Verbindungen aufgrund von Telefonnummernübereinstimmung, Verbindungen aufgrund eines gemeinsamen Gruppenchats und Verbindungen aus akzeptierten Chat- und Verbindungsanfragen. Benutzer können ihre Kontakte 1. Grades auf der Registerkarte "Chats" finden. Alle Benutzer auf Siilo können auf ihre Kontakte 1. Grades zugreifen, es sei denn, sie haben die Verifizierung nicht bestanden.

Verbindungen 2. Grades sind die Kollegen, die mit den Verbindungen 1. Grades eines Benutzers verbunden sind. Nur verifizierte Benutzer können Verbindungen 2. Grades in der Funktion "Personen, die Sie vielleicht kennen" auf der Registerkarte "Spaces" unter "Meine Netzwerke" [Symbol] "Siilo Network" aufgelistet finden. Die Liste der Verbindungen 2. Grades ist auf 8 Fachleute beschränkt und diese wurden danach ausgewählt, wie oft eine Verbindung mit einer Verbindung 1. Grades verbunden war.

Siilo Network-Verbindungen sind alle Kollegen auf Siilo, die als medizinischer Fachmann verifiziert wurden und sich nicht abgemeldet haben, um im Siilo-Verzeichnis zu sein. Benutzer finden das "Siilo Network" auf der Registerkarte "Spaces" unter "My Networks". Die Suchfunktion auf dieser Registerkarte kann genutzt werden, um sich mit anderen verifizierten medizinischen Fachkräften zu verbinden. Nur verifizierte medizinische Fachkräfte können das Siilo Network durchsuchen, es sei denn, sie beantragen ein Opt-Out über den Siilo Service Desk Chat. Wenn sie sich abmelden, können sie weder das Netzwerk der verifizierten Fachkräfte auf Siilo durchsuchen, noch können sie von anderen verifizierten Kollegen auf Siilo gefunden werden.

Organisationsverzeichnis-Verbindungen sind alle Teil der gleichen Organisation, wie sie von einem Siilo Connect Kunden definiert wurde. Unabhängig vom Verifizierungsstatus können Benutzer ihre Organisationsverzeichnis-Verbindungen suchen und kontaktieren. Das Organisationsverzeichnis finden Sie auf der Registerkarte "Spaces" unter "Meine Netzwerke" [Symbol] "Organisationsname." Die Organisation kuratiert die Organisationsverzeichnisverbindungen über einen manuellen Prozess oder einen automatisierten Prozess (z.B. Verbindung über eine Integration mit ihrem lokalen Verzeichniszugangsprotokoll).

1.4 Lesen

In den folgenden Kapiteln erläutern wir umfassend unsere Datenverarbeitungsprozesse, beschreiben dann die Risiken, die mit der Verarbeitung dieser Informationen verbunden sind, und unsere Methoden, um Lösungen für solche Probleme zu finden, im Kontext einer sich ständig verändernden Welt voller Sicherheitsrisiken.

2.0 Erfasste (persönliche) Daten

2.1 Meldungsdaten

Es ist von äußerster Wichtigkeit und kann nicht stark genug betont werden: Nachrichtendaten, die in Gesundheitsteams ausgetauscht werden, sollten niemals jemandem zugänglich gemacht werden, der nicht direkt an der optimalen Versorgung des jeweiligen Patienten beteiligt ist.

Aufgrund der Natur von Siilos Verschlüsselungsprotokollen sind Mitarbeiter - oder irgendjemand anderes - niemals in der Lage zu verstehen, welche Informationen geteilt werden, noch warum sie geteilt werden. Daher konzentriert sich Siilo nur auf den Prozess des Teilens und entwickelt die App so, dass dieses Teilen so sicher wie möglich erfolgt, ohne dem Nutzer Reibungsverluste aufzuerlegen.

Nachrichtendaten gelangen in Siilo auf die Smartphones von medizinischem Fachpersonal über:

- die Kamera-App des Telefons,
- eine andere Kommunikations-App auf dem Telefon (Messenger-Apps, E-Mail-Apps);
- die Web-Anwendung von Siilo auf einem Tablet, Laptop oder Desktop;
- eine Nachricht von einem anderen Siilo-Benutzer, oder;
- Siilos dedizierte Kamera-App (Android) oder Langdruck-Funktionalität (iOS).

Sobald die Informationen in der Siilo-App sind, sind die wichtigsten Standardeinstellungen:

- Informationen werden niemals automatisch mit anderen Apps (z. B. landen Fotos niemals in einer Kamerarolle) und Servern (z. B. iCloud, Google Cloud oder Dropbox) geteilt;
- alle Informationen werden ausdrücklich von automatischen iCloud/Android-Backups ausgeschlossen
- Nachrichten werden nach 30 Tagen automatisch gelöscht.

Eine Abweichung von diesen Standardeinstellungen kann nur durch den Benutzer bewusst herbeigeführt werden.
Zum Beispiel kann ein Benutzer wählen, Nachrichten aus der Web-App auf einen Computer herunterzuladen oder Nachrichten/Konversationen auszuwählen, die länger als 30 Tage aufbewahrt werden sollen. Ein anderes Beispiel wäre, wenn eine Gesundheitsorganisation eine Integration des Siilo Messengers mit ihrer elektronischen Patientenakte erwirbt; eine Fachkraft kann dann Nachrichten auswählen, die in die Patientenakte zur Aufbewahrung exportiert werden sollen. Informationen können über die folgenden Wege aus der App heraus gelangen:

- über die Download-Funktionalität in der Web-App von Siilo;
- über die Exportfunktionalität in Siilos mobiler App;
- über eine sichere, kundenspezifische Integration mit On Premise Servern von Gesundheitseinrichtungen; oder
- über die Aufnahme von Screenshots oder Fotos von Telefonen, die die App geöffnet haben.

2.2 Benutzerdaten

Das berechtigte Interesse an der Erhebung und Verarbeitung der personenbezogenen Daten ist für die Erfüllung und Einhaltung des Vertrages notwendig. Bevor ein Nutzer die Siilo-App auf seinem Smartphone installiert, stimmt er der Lizenzvereinbarung, die auch die Datenschutzvereinbarung enthält, durch Anklicken des Links zu, der ihm bei der Registrierung für die App an seine E-Mail-Adresse gesendet wird.

Ein entscheidendes Element zur Absicherung des Austauschs von Patientendaten in einem professionellen Umfeld ist es, sicherzustellen, dass der vorgesehene Empfänger der Informationen tatsächlich derjenige ist, mit dem Sie die Informationen teilen wollen. Denn wenn sich eine medizinische Fachkraft auf einer Messenger-Plattform anmeldet, um über tatsächliche Patienten zu sprechen, und sich als "ZDoggMD" bezeichnet, wie kann man dann sicher sein, dass die Person hinter diesem Namen tatsächlich Dr. Zoe Domani ist?

Siilo ist der Meinung, dass die Identitäten seiner Nutzer gründlich geprüft und verifiziert werden sollten. Dies stellt sicher, dass andere Nutzer auf der Plattform beruhigt sein können, wenn sie Informationen miteinander teilen. Um Fachleuten diesen Seelenfrieden zu geben, können sie den Verifizierungsstatus ihrer Kontakte auf ihrem Avatar deutlich sehen. Die 4 Stati sind:

1. nicht verifiziert;
2. verifizierte Identität;
3. verifizierter registrierter Mediziner, und;
4. Verifizierung fehlgeschlagen.

Die Benutzer werden in der Lage sein, den Verifizierungsstatus ihrer Kollegen auf Siilo mit den folgenden Badges schnell zu sehen:

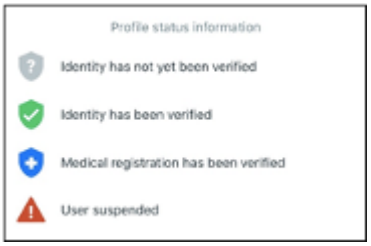

Abbildung 1 *Verifizierungsabzeichen, die auf den Avataren und Profilen der Benutzer sichtbar sind.*

Um verifiziert zu werden, werden Siilo-Nutzer aufgefordert, persönliche Daten während des Registrierungsprozesses, sowie durch den Service Desk Chat in der App anzugeben. Diese persönlichen Daten werden dann sicher über die mobile App an die Server von Siilo gesendet. In der folgenden Tabelle finden Sie alle persönlichen Daten, nach denen ein Siilo-Nutzer gefragt wird:

Informationen	Grund für die Bearbeitung	Vorratsspeicherung
Namen (Vorname, Nachname)	Relevant für die Verifizierung, Aufbau von gegenseitigem Vertrauen	Sofortige Löschung nach Beendigung der Lizenzvereinbarung.
Rufnummer	Relevant für den Aufbau von Verbindungen auf der Siilo-Plattform und relevant für die Kontaktaufnahme mit Nutzern zur weiteren Produktverbesserung.	Sofortige Löschung nach Beendigung der Lizenzvereinbarung.
E-Mail Adresse(n)	Relevant, um die Verknüpfung mit Endbenutzer- und Prozessorvereinbarungen zu senden, relevant für einen Teil des Verifizierungsprozesses, relevant, um Benutzer als Teil der Organisation eines Kunden zu identifizieren, relevant, um Benutzer für weitere Produktverbesserungen zu kontaktieren.	Sofortige Löschung nach Beendigung der Lizenzvereinbarung.
Medizinische Registrierungsnummer	Relevant für die Verifizierung, Aufbau von gegenseitigem Vertrauen (optional)	Sofortige Löschung nach Beendigung der Lizenzvereinbarung.

Avatar-Bild	Relevant für Peer-to-Peer-Vertrauen (optional)	Sofortige Löschung nach Beendigung der Lizenzvereinbarung.
Medizinischer Beruf	Relevant für die Verifizierung, Aufbau von gegenseitigem Vertrauen (mandatory)	Sofortige Löschung nach Beendigung der Lizenzvereinbarung.
Titel(s)	Relevant für Peer-to-Peer-Vertrauen (optional)	Sofortige Löschung nach Beendigung der Lizenzvereinbarung.
Spezialisierung(en)	Relevant für Peer-to-Peer-Vertrauen (optional)	Sofortige Löschung nach Beendigung der Lizenzvereinbarung.
Interesse(n)	Relevant für Peer-to-Peer-Vertrauen (optional)	Sofortige Löschung nach Beendigung der Lizenzvereinbarung.
Organisation/Verband	Relevant für Peer-to-Peer-Vertrauen (optional)	Sofortige Löschung nach Beendigung der Lizenzvereinbarung.
Telefonkontakte Telefonnummern	Relevant für den sofortigen Verbindungsaufbau auf der Siilo-Plattform (optional)	Sofortige Löschung nach Beendigung der Lizenzvereinbarung.
Auffindbarer Gruppenname, Gruppenbeschreibung	Relevant für den Verbindungsaufbau auf der Siilo-Plattform (optional)	Sofortige Löschung nach Beendigung der Lizenzvereinbarung.
Kopie des Arztausweises, Führerscheins oder Reisepasses	Relevant für die Verifizierung, Peer-Vertrauen herstellen (optional)	Immediate deletion after verification.
Organisationsspezifische Profilfelder	Relevant für die Mitglieder einer bestimmten Organisation auf Siilo	Sofortige Löschung nach Beendigung der Lizenzvereinbarung.

Tabelle 1 Persönliche Daten, die Siilo-Nutzer im Rahmen der Registrierung bewusst ausfüllen, ihr berufliches Profil ausfüllen oder eine öffentliche, auffindbare Gruppe auf Siilo einrichten.

Aufgrund der Natur der Messaging-Software sammelt Siilo die folgenden persönlichen Daten, die in der folgenden Tabelle aufgeführt sind, oder muss diese sammeln. Diese Daten sind für das ordnungsgemäße Funktionieren der Siilo App unerlässlich:

Informationen	Grund für die Bearbeitung	Vorratsspeicherung
Anzahl der Verbindungen auf Siilo	Relevant, um Informationen zu erhalten, wie Sie mit Siilo loslegen können.	Sofortige Löschung nach Beendigung der Lizenzvereinbarung.
Geräteinformationen: Benutzer-IP-Adresse Typ des mobilen Geräts Betriebssystem Version der App Sprache des Geräts Push-Ziel Touch-ID aktiviert Face-ID aktiviert	Relevant für den Entwicklungsprozess, und Verständnis für Fehler in der Software und deren Behebung.	Sofortige Löschung nach Beendigung der Lizenzvereinbarung.

WhatsApp installiert **Adobe Acrobat installiert**	Relevant für bestimmte Funktionalitäten in Siilo wie z. B. Einladungen über WhatsApp und das Betrachten von PDF-Dateien auf dem mobilen Gerät.	Sofortige Löschung nach Beendigung der Lizenzvereinbarung.
Anzahl der Gruppen	Relevant, um den Grad des Engagements auf Siilo für Siilo-Kunden zu verstehen	Sofortige Löschung nach Beendigung der Lizenzvereinbarung.
Organisatorische Rolle	Relevant für Berechtigungen in der Siilo Connect Umgebung	Sofortige Löschung nach Beendigung der Lizenzvereinbarung.
Wie viele Nachrichten gesendet/empfangen	Relevant, um den Grad des Engagements auf Siilo für Siilo-Kunden zu verstehen	Sofortige Löschung nach Beendigung der Lizenzvereinbarung.
Wie viele und welche Tage online (letzte 30 d)	Relevant, um den Grad des Engagements auf Siilo für Siilo-Kunden zu verstehen	Sofortige Löschung nach Beendigung der Lizenzvereinbarung.
Web-App-Aktivierung und aktuelle Sitzungen	Relevant, um den Grad des Engagements auf Siilo für Siilo-Kunden zu verstehen	Sofortige Löschung nach Beendigung der Lizenzvereinbarung.

Tabelle 2 *Personenbezogene Daten über Siilo-Nutzer, die von Nutzern durch die Nutzung der App erhoben werden*

2.3 Meta-Daten

Um das Siilo-Produkt zu verbessern und zu verstehen, sowie eine größere Siilo-Benutzererfahrung zu bieten, müssen Siilo-Mitarbeiter möglicherweise auf automatisierte Metadaten zugreifen und diese verarbeiten, was auch als Benutzer-'Profiling' bezeichnet wird. Siilo stellt sicher, dass die Erstellung von Nutzerprofilen ausschließlich als notwendige Voraussetzung für die Verbesserung des Betriebs durchgeführt wird. Dies spiegelt sich in der Art und Weise wider, wie auf Metadaten zugegriffen wird; derzeit müssen Siilo-Entwickler entweder Code schreiben, um die Kopplung zwischen einem realen Nutzer und seinen Metadaten herzustellen, oder Mitglieder des Siilo-Verifizierungs- und Managementteams müssen eine "break the glass-Prozedur" durchlaufen, um auf de-anonymisierte Metadaten zuzugreifen, die unten aufgeführt sind.
Nur Mitarbeiter mit einem gültigen Need-to-know haben Zugriff auf dieses Verfahren. Alle Metadaten werden auf Basis der User-ID pseudonymisiert. Siilo verarbeitet die folgenden Arten von Metadaten:

- Nachrichten-Ereignisse
- Aktivitätsereignisse
- Registrierungsfortschritt-Ereignisse
- Allgemeine analytische Ereignisse

Um die aggregierten Metadaten zu analysieren und zu visualisieren, verwendet Siilo Looker.

Für die Metadaten wird keine Aufbewahrungsfrist angewendet. Alle personenbezogenen Daten werden nach Beendigung des Lizenzvertrages gelöscht. Das bedeutet, dass die Metadaten nicht mehr auf den Benutzer zurückgeführt werden können.

2.3.1 Nachrichten-Ereignisse

Informationen	Grund für die Bearbeitung
Art der Nachricht (Textnachricht, Voice Anruf, Video Anruf)	Wir sammeln diese Informationen, um die Leistung unserer Anwendung über verschiedene Versionen und Länder hinweg zu verfolgen.
Zeitstempel	Wir sammeln diese Informationen, um die Leistung unserer Anwendung über verschiedene Versionen und Länder hinweg zu verfolgen.
Nutzer / Installation ID des Senders	Wir sammeln diese Informationen, um die Leistung unserer Anwendung über verschiedene Versionen und Länder hinweg zu verfolgen.
Art der session (webchat oder nicht)	Wir sammeln diese Informationen, um die Leistung unserer Anwendung über verschiedene Versionen und Länder hinweg zu verfolgen.
Client Typ	Wir sammeln diese Informationen, um die Leistung unserer Anwendung über verschiedene Versionen und Länder hinweg zu verfolgen.
Siilo version	Wir sammeln diese Informationen, um die Leistung unserer Anwendung über verschiedene Versionen und Länder hinweg zu verfolgen.
Ort auf Basis der IP Adresse	Wir sammeln diese Informationen, um die Leistung unserer Anwendung über verschiedene Versionen und Länder hinweg zu verfolgen.
Gruppen ID Ziel ***(nur zutreffend bei Gruppenchats)***	Wir sammeln diese Informationen, um Statistiken wie einzigartige aktive Gruppen und einzigartige Empfänger erstellen zu können.
Zielort der Nachricht (Nutzer oder Gruppe)	Wir sammeln diese Informationen, um Statistiken wie einzigartige aktive Gruppen und einzigartige Empfänger erstellen zu können.
Nutzer ID Ziel ***(ur zutreffend bei Einzelchats)***	Wir sammeln diese Informationen, um Statistiken wie einzigartige aktive Gruppen und einzigartige Empfänger erstellen zu können.
Nachrichten ID	Diese Informationen ermöglichen es uns, eindeutige Nachrichten zu zählen.
Fall ID ***(nur zutreffend wenn ein Fall erstellt wird in einer Konversation)***	Diese Informationen werden verwendet, um die Leistung unserer Chat-Fälle-Funktion zu verfolgen.
Envelop Typ (Normale Nachricht oder neuer Fall)	Diese Informationen werden verwendet, um die Leistung bestimmter Funktionen in unseren Anwendungen zu verfolgen.
Zitat (wurde ein Zitat genutzt oder nicht?)	Diese Informationen werden verwendet, um die Leistung bestimmter Funktionen in unseren Anwendungen zu verfolgen.
Länge des (video or voice) Anrufes	Diese Informationen werden auf jeder asynchronen Messenger-Plattform erstellt

2.3.2 Aktivitätsereignisse

Informationen	Grund für die Bearbeitung
Art der Aktivität	Diese Informationen werden verwendet, um Analysen über die Leistung unserer Anwendungen, aufgeteilt nach Versionen, Ländern und Sprachen, etc. zu erstellen.
Nutzer ID	Diese Informationen werden verwendet, um Analysen über die Leistung unserer Anwendungen, aufgeteilt nach Versionen, Ländern und Sprachen, etc. zu erstellen.
Installation ID	Diese Informationen werden verwendet, um Analysen über die Leistung unserer Anwendungen, aufgeteilt nach Versionen, Ländern und Sprachen, etc. zu erstellen.
Web session ID	Diese Informationen werden verwendet, um Analysen über die Leistung unserer Anwendungen, aufgeteilt nach Versionen, Ländern und Sprachen, etc. zu erstellen.
Client Typ	Diese Informationen werden verwendet, um Analysen über die Leistung unserer Anwendungen, aufgeteilt nach Versionen, Ländern und Sprachen, etc. zu erstellen.
Siilo version	Diese Informationen werden verwendet, um Analysen über die Leistung unserer Anwendungen, aufgeteilt nach Versionen, Ländern und Sprachen, etc. zu erstellen.
Ort auf Basis der IP Adresse	Diese Informationen werden verwendet, um Analysen über die Leistung unserer Anwendungen, aufgeteilt nach Versionen, Ländern und Sprachen, etc. zu erstellen.
Verwendete Sprache	Diese Informationen werden verwendet, um Analysen über die Leistung unserer Anwendungen, aufgeteilt nach Versionen, Ländern und Sprachen, etc. zu erstellen.
Nutzer Agent	Diese Informationen werden verwendet, um Analysen über die Leistung unserer Anwendungen, aufgeteilt nach Versionen, Ländern und Sprachen, etc. zu erstellen.

2.3.3 Registrierung Fortschritt Ereignisse

Informationen	Grund für die Bearbeitung
Schritt im Registrierungsprozess	Wir verfolgen die Registrierungsfortschrittsereignisse, um die Leistung unseres Registrierungsflusses zu verfolgen und Probleme in unserem Registrierungsfluss zu identifizieren, indem wir die Abbruchpunkte betrachten.
Status der eingegebenen Daten	Wir verfolgen die Registrierungsfortschrittsereignisse, um die Leistung unseres Registrierungsflusses zu verfolgen und Probleme in unserem Registrierungsfluss zu identifizieren, indem wir die Abbruchpunkte betrachten.
Client Typ	Wir verfolgen die Registrierungsfortschrittsereignisse, um die Leistung unseres Registrierungsflusses zu verfolgen und Probleme in unserem Registrierungsfluss zu identifizieren, indem wir die Abbruchpunkte betrachten.
Siilo version	Wir verfolgen die Registrierungsfortschrittsereignisse, um die Leistung unseres Registrierungsflusses zu verfolgen und Probleme in unserem Registrierungsfluss zu identifizieren, indem wir die Abbruchpunkte betrachten.
Modell des Mobilgerätes	Wir verfolgen die Registrierungsfortschrittsereignisse, um die Leistung unseres Registrierungsflusses zu verfolgen und Probleme in unserem Registrierungsfluss zu identifizieren, indem wir die Abbruchpunkte betrachten.
Ort auf Basis der IP Adresse	Wir verfolgen die Registrierungsfortschrittsereignisse, um die Leistung unseres Registrierungsflusses zu verfolgen und Probleme in unserem Registrierungsfluss zu identifizieren, indem wir die Abbruchpunkte betrachten.
Nutzer ID (wenn Registrierung beendet wurde)	Wir verfolgen die Registrierungsfortschrittsereignisse, um die Leistung unseres Registrierungsflusses zu verfolgen und Probleme in unserem Registrierungsfluss zu identifizieren, indem wir die Abbruchpunkte betrachten.

2.3.4 Allgemeine analytische Ereignisse

Informationen	Grund für die Bearbeitung
Nutzer ID	Wir verfolgen generische analytische Ereignisse, um die Leistung mehrerer Funktionen in unseren Anwendungen in verschiedenen Versionen und über einzelne Benutzer zu verfolgen.
Client Typ	Wir verfolgen generische analytische Ereignisse, um die Leistung mehrerer Funktionen in unseren Anwendungen in verschiedenen Versionen und über einzelne Benutzer zu verfolgen.
Siilo version	Wir verfolgen generische analytische Ereignisse, um die Leistung mehrerer Funktionen in unseren Anwendungen in verschiedenen Versionen und über einzelne Benutzer zu verfolgen.
Art der Aktivität	Wir verfolgen generische analytische Ereignisse, um die Leistung mehrerer Funktionen in unseren Anwendungen in verschiedenen Versionen und über einzelne Benutzer zu verfolgen.

2.3.5 Konto-Ereignisse

Informationen	Grund für die Bearbeitung
Nutzer ID	Kontoereignisse ermöglichen es uns, die Gesamtzahl der Konten in unserem System im Laufe der Zeit zu verfolgen, aufgeteilt nach Plattform und Sprache.
Konto erstellt oder gelöscht	Kontoereignisse ermöglichen es uns, die Gesamtzahl der Konten in unserem System im Laufe der Zeit zu verfolgen, aufgeteilt nach Plattform und Sprache.
Typ des Kontos (Nutzer oder Gruppe)	Kontoereignisse ermöglichen es uns, die Gesamtzahl der Konten in unserem System im Laufe der Zeit zu verfolgen, aufgeteilt nach Plattform und Sprache.
Client-Typ	Kontoereignisse ermöglichen es uns, die Gesamtzahl der Konten in unserem System im Laufe der Zeit zu verfolgen, aufgeteilt nach Plattform und Sprache.
Verwendete Sprache	Kontoereignisse ermöglichen es uns, die Gesamtzahl der Konten in unserem System im Laufe der Zeit zu verfolgen, aufgeteilt nach Plattform und Sprache.

Tabelle 3 *Metadaten, die Siilo verarbeitet, um eine Nachricht von einem Benutzer zu einem anderen senden zu können.*

3.0 Siilo Sub-Prozessoren

Aufgrund des Designs der Siilo-Messenger-Software nutzt Siilo bestimmte Software, die von anderen Anbietern an Siilo lizenziert wird. Diese Anbieter werden als Unterprozessoren bezeichnet, da Teile der Informationen der Siilo Nutzer mit deren Software interagieren. Zum Beispiel: Wenn sich ein Siilo Nutzer für die App anmeldet, wird eine SMS an die Telefonnummer dieses Nutzers gesendet, um diese Telefonnummer zu verifizieren. Siilo hat keinen eigenen SMS-Verifizierungsdienst entwickelt, sondern nutzt dafür die Software eines anderen Anbieters. Somit verarbeitet dieser Anbieter die Telefonnummer eines Siilo-Nutzers im Auftrag von Siilo. Siilo hat mit allen Unterauftragsverarbeitern vertragliche Datenschutzvereinbarungen getroffen. Die Überwachung der Sicherheit und der Leistung von Unterauftragsverarbeitern ist Teil der Richtlinien des Informationssicherheitsmanagementsystems (ISMS) unserer ISO-27001-Zertifizierung.

Sub-Prozessor	Amazon Web Services
Generell	Die Server-Infrastruktur von Siilo wird von Amazon gehostet.
Wo werden die Daten gehostet?	Alle Messaging-bezogenen Aktivitäten finden in den Frankfurter Rechenzentren von Amazon statt. Für Dienste wie die E-Mail-Verifizierung (Amazon Simple Email Service) und die Protokollierung der Sicherheitsrichtlinien für Website-Inhalte (Amazon Lambda) werden diese Dienste nur im Rechenzentrum in Irland angeboten. Zusammenfassend lässt sich sagen, dass alle Daten innerhalb der EU gehostet werden und sich der Großteil davon in Frankfurt befindet. Die mit Siilo-Benutzern ausgetauschten E-Mails laufen jedoch über das irische Rechenzentrum. Amazon Web Services verwendet Standardvertragsklauseln als Mechanismus für die Übermittlung von Daten außerhalb der Europäischen Union, da der Gerichtshof der Europäischen Union dies bestätigt hat.
Welche Daten werden verarbeitet?	Verarbeitet von Amazon AWS: - -Mail-Adressen und E-Mail-Inhalte - Nutzerprofildaten - verschlüsselte Nachrichtendaten - Nachrichten-Metadaten (pseudonomisiert) - Anfrage-Metadaten
Mehr Informationen	https://aws.amazon.com/compliance/gdpr-center/ https://aws.amazon.com/privacy/

Sub-Prozessor	Twilio
Generell	Twilio wird in einigen Fällen zum Senden von SMS-Nachrichten verwendet. Außerdem wird Twilio verwendet, um Siilos In-App VOIP- (Anrufe über das Internet) und Videoanruf-Funktionalität bereitzustellen. Die Inhalte Ihrer Anrufe werden Ende-zu-Ende verschlüsselt (DTLS/SRTP). Wenn es aufgrund von Firewalls notwendig ist, ermittelt Twilio zunächst, welcher ihrer Server am besten zwischen dem Anrufer und dem Empfänger positioniert ist, um über einen als TURN bekannten Mechanismus als Blind Relay zu fungieren.

Wo werden die Daten gehostet?	https://www.twilio.com/docs/video/ip-address-whitelisting
Welche Daten werden verarbeitet?	- Mobilfunknummern - SMS Inhalt - In-app voice/video Anruf Metadaten
Mehr Informationen	https://www.twilio.com/legal/privacy

Sub-Prozessor	CM.com
Generell	Als Teil des Siilo-Registrierungsablaufs werden die Benutzer aufgefordert, ihre Telefonnummer anzugeben. Diese Telefonnummer ist ein wesentlicher Bestandteil der Kontaktfindung für neue Benutzer. Als Teil der Siilo-Richtlinie zur Verifizierung von Informationen verwenden wir CM als SMS-Anbieter, um eine SMS an den Benutzer mit einem Code zu senden, den er eingibt, um zu bestätigen, dass er tatsächlich Zugriff auf das mit dieser Nummer verbundene Gerät hat. Die von CM beauftragten Dienstanbieter sind:, Unbounce, LinkedIn Insights und Google Analytics.
Wo werden die Daten gehostet?	Das Rechenzentrum befindet sich in den Niederlanden.
Welche Daten werden verarbeitet?	- Mobilfunknummern - SMS Inhalt
Mehr Informationen	https://www.cm.com/about-cm/security-compliance/ https://legal.cmtelecom.com/en/cm-online-bv/privacy-policy

Sub-Prozessor	Firebase
Generell	Firebase wird von Siilo für Analytics und Crash-Reporting in den iOS und Android Mobile Anwendungen, Push-Benachrichtigungen für die Android Anwendung und dynamische Links für Nicht-Nutzer verwendet. Die Benutzerdaten werden vollständig anonymisiert gesendet und enthalten keine personenbezogenen Daten wie Telefonnummern, E-Mails, Namen. Benutzer können sich bei der Registrierung der App vom Analysedienst abmelden.
Wo werden die Daten gehostet?	Google datacenters: https://www.google.com/about/datacenters/locations/index.html Firebase verwendet Standardvertragsklauseln für die Übermittlung von Daten außerhalb der Europäischen Union, da der Gerichtshof der Europäischen Union dies bestätigt hat.

Welche Daten werden verarbeitet?	Keine persönlich identifizierbaren Daten Firebase Crash Reporting: - Instance IDs - Crash traces Crashlytics: - Installation UUID - IP Addresses Firebase Cloud Messaging - Instance IDs Firebase Dynamic Links: - Device specs (iOS)
Mehr Informationen	https://firebase.google.com/support/privacy

Sub-Prozessor	ZenDesk
Generell	Siilo ist ein weitgehend benutzerorientiertes Unternehmen, das seine Software vor allem als Reaktion auf Benutzereingaben verbessert. Siilo-Benutzer haben mehrere Möglichkeiten, Benutzer-Feedback zu geben, wie z. B. über die Siilo-Messenger-App, aber natürlich auch entweder über das Siilo-Kontaktformular auf www.siilo.com oder die folgende E-Mail-Adresse: info@siilo.com. Aufgrund des hohen Volumens dieser Interaktionen hat Siilo ein Ticketing-System, das eine Software namens ZenDesk verwendet, um den Austausch zwischen Mitarbeitern und Benutzern zu verfolgen.
Wo werden die Daten gehostet?	Zendesk hat Rechenzentren in drei Hauptregionen - USA, Asien-Pazifik und Europäische Union. Die Servicedaten können in jeder Region gespeichert werden. ZenDesk verwendet Standardvertragsklauseln als Mechanismus für die Übertragung von Daten außerhalb der Europäischen Union, da der Gerichtshof der Europäischen Union dies validiert hat.
Welche Daten werden verarbeitet?	Namen, E-Mail Adressen, Mobilfunknummern
Mehr Informationen	https://www.zendesk.nl/company/customers-partners/privacy-policy/ https://www.zendesk.com/blog/update-privacy-shield-invalidation-european-court-justice/

Sub-Prozessor	Salesforce
Generell	Informationen, die in das Kontaktformular auf der Website eingegeben werden, werden in Salesforce verarbeitet. Wir verwenden Salesforce, um Anfragen von (potenziellen) Kunden korrekt und effizient zu beantworten.
Wo werden die Daten gehostet?	Frankfurt / Paris

Welche Daten werden verarbeitet?	Namen, E-Mail-Adressen, Name der Organisation, Eigenschaften und Bedürfnisse
Mehr Informationen	https://www.salesforce.com/company/privacy/

Sub-Prozessor	Zapier
Generell	Informationen, die in das Kontaktformular auf der Website eingegeben werden, werden von Zapier verarbeitet und an verschiedene Endpunkte weitergeleitet.
Wo werden die Daten gehostet?	Die Rechenzentren von Zapier befinden sich in den Vereinigten Staaten. Zapier verwendet Standardvertragsklauseln als Mechanismus für die Übertragung von Daten außerhalb der Europäischen Union, da der Gerichtshof der Europäischen Union dies validiert hat.
Welche Daten werden verarbeitet?	Namen, E-Mail-Adressen, Name der Organisation, Eigenschaften und Bedürfnisse.
Mehr Informationen	https://zapier.com/privacy https://zapier.com/tos

Sub-Prozessor	Google Analytics
Generell	Google Analytics wird von Siilo eingesetzt, um ein besseres Verständnis der Besucher und Nutzer von https://www.siilo.com und https://web.siilo.com/ zu erlangen. Darüber hinaus ist der Einsatz von Analytics notwendig, um die Besucher- und Nutzererfahrung kontinuierlich zu verbessern. Die an Google gesendeten Daten spiegeln lediglich das Nutzerverhalten wider und enthalten keine personenbezogenen Daten. Google Analytics nutzt Opt-Out durch die Installation eines Browser-Add-Ons. Auf www.siilo.com können Nutzer Opt-In über den Cookie-Einwilligungsdialog nutzen.
Wo werden die Daten gehostet?	Google datacenters: https://www.google.com/about/datacenters/locations/index.html Google Analytics verwendet Standardvertragsklauseln als Mechanismus für die Übertragung von Daten außerhalb der Europäischen Union, da der Gerichtshof der Europäischen Union dies bestätigt hat.
Welche Daten werden verarbeitet?	Keine persönlich identifizierbaren Daten

Mehr Informationen	https://www.google.com/analytics/terms/us.html https://privacy.google.com/businesses/controllerterms/

Sub-Prozessor	Google Optimize
Generell	Google Optimize wird von Siilo genutzt, um A/B-Tests auf der Website durchzuführen. Mit diesen Informationen kann Siilo lernen, was am besten für unsere Besucher funktioniert. Die an Google gesendeten Daten spiegeln nur das Nutzerverhalten wider und enthalten keine personenbezogenen Daten. Google Optimize baut auf Google Analytics auf, daher werden die gleichen Daten verarbeitet.
Wo werden die Daten gehostet?	Google datacenters: https://www.google.com/about/datacenters/locations/index.html Google Optimize verwendet Standardvertragsklauseln als Mechanismus für die Übertragung von Daten außerhalb der Europäischen Union, da der Gerichtshof der Europäischen Union dies bestätigt hat.
Welche Daten werden verarbeitet?	Data from Google Analytics
Mehr Informationen	https://optimize.google.com/optimize/home/#/accounts https://privacy.google.com/businesses/controllerterms/

Sub-Prozessor	HiBob
Generell	HiBob streamlined die Kernprozesse im Personalwesen durch die Automatisierung und Vereinfachung von Genehmigungszyklen mit nur einem Klick im Web oder unserer mobilen App.
Wo werden die Daten gehostet?	Die von HiBob gesammelten Daten werden in der Amazon Cloud in Irland und Frankfurt gehostet, die erweiterte Sicherheitsfunktionen bietet und dem ISO 27001 Standard entspricht.
Welche Daten werden verarbeitet?	Namen, E-Mail-Adressen, Geburtsdatum, Geschlecht, Nationalität, Berufsbezeichnung, Telefonnummer(n), Datum, an dem Sie zum ersten Mal für Ihren Arbeitgeber gearbeitet haben, Abteilung, in der Sie arbeiten, Mitarbeiter-ID/Nationalversicherungsnummer, Adresse, Land, Stadt, Postleitzahl, Familienstand, Name, Geschlecht und Geburtsdatum des Ehepartners und anderer Angehöriger, Ihre Bankverbindung (Bankname, Kontonummer, Kontotyp, SWIFT-Code, IBAN-Code, Bankleitzahl, Adresse der Zweigstelle), Details zu Ihrem Gehalt und Ihrer Arbeit (Lohnperiode, Zahlungsfrequenz, Grundgehalt, Bruttogehalt, Überstunden, Boni, Provisionen, Gehaltsverzicht, gesetzliche Zahlungen wie Krankheit, Mutterschafts-/Vaterschaftsurlaub, Währung der Gehaltszahlung, Bescheinigung über das Recht, in Ihrem Land zu arbeiten, Steuernummer, Eigenkapital, Kontaktdaten für Notfälle (Name, Verwandtschaft, Telefonnummer(n), E-Mail-Adresse(n), Stadt, Land, Postleitzahl), Beendigungsdatum, Beendigungsgrund,

	Datum des Probezeitendes, Status im System und am Arbeitsplatz, IP-Adresse und andere eindeutige Identifikatoren.
Mehr Informationen	https://www.hibob.com/privacy/privacy-policy/

Sub-Prozessor	Lever
Generell	Siilo nutzt Lever, um die strategisch wichtigste Herausforderung für Unternehmen zu bewältigen: das Wachstum ihrer Teams. Lever integriert die Werte - Zusammenarbeit, Transparenz und Menschlichkeit - in seine Software und zeigt auf, wie Unternehmen über Wachstum nachdenken können, wobei Talent und Teamarbeit im Mittelpunkt stehen.
Wo werden die Daten gehostet?	Lever hat seinen Sitz in den Vereinigten Staaten. Lever verwendet Standardvertragsklauseln als Mechanismus für die Übermittlung von Daten außerhalb der Europäischen Union, da der Gerichtshof der Europäischen Union dies bestätigt hat.
Welche Daten werden verarbeitet?	Namen, E-Mail-Adressen, Adresse, Beschäftigungsgeschichte, Standort und andere Informationen, die von einem Kunden angefordert oder von einem Bewerber im Rahmen eines Einstellungsverfahrens übermittelt werden können.
Mehr Informationen	https://www.lever.co/blog/moving-beyond-the-eu-us-privacy-shield/ https://www.lever.co/privacy/ https://help.lever.co/hc/en-us/articles/360028434011-Service-Privacy-Notice

Sub-Prozessor	Verifai
Generell	Siilo nutzt Verifai, um die Identität von Siilo-Nutzern zu überprüfen und ID-Dokumente zu authentifizieren. In der Siilo-App ermöglichen wir es dem Nutzer, seinen Reisepass, Führerschein oder einen anderen Identitätsnachweis zu fotografieren, um seine Identität zu bestätigen.
Wo werden die Daten gehosted?	Verifai hat seinen Sitz in den Niederlanden.
Welche Daten werden verarbeitet?	erifai speichert niemals persönliche Informationen auf den Geräten seiner Kunden und sendet keine persönlichen Informationen an seine eigenen Server. Verifai verarbeitet lediglich statistische Daten, darunter die Anzahl der Scans, Datum und Uhrzeit, Dokumenttypen, das Ausstellungsland der gescannten Dokumente sowie die Anzahl der erfolgreichen und fehlgeschlagenen Scans. Zu Protokollierungs- und Überwachungszwecken werden grundlegende Angaben zu Ihrem Gerät wie Betriebssystem (OS), OS-Version und Gerätetyp erfasst..
Mehr Informationen	https://www.verifai.com/en/privacy/ https://www.verifai.com/en/terms-use/

Sub-Prozessor	Looker
Generell	Siilo nutzt Looker als Plattform für Dashboarding und BI, die sich mit unserem Amazon Redshift Data Warehouse verbinden würde. Während keine Daten dauerhaft bei Looker gespeichert werden, würden sie unsere Daten verarbeiten und visualisieren und benötigen dafür eine laufende Verbindung und einen temporären Cache von unserem Redshift-Warehouse. Alle Daten sind pseudonymisiert (nach userId) und enthalten keine P(H)I (Name, E-Mail, IP-Adresse, aktuelle Nachrichten, etc.).
Wo werden die Daten gehosted?	Looker hat seinen Sitz in den Vereinigten Staaten, aber in der Datenbank von Looker werden keine personenbezogenen Daten gespeichert.
Welche Daten werden verarbeitet?	Eindeutige (Geräte-)Kennungen, Geräteinformationen, Nutzungsdaten, Analysedaten, Lizenznachweise.
Mehr Informationen	https://looker.com/product/security https://looker.com/trust-center/privacy/policy

Sub-Prozessor	Links in the app: Itunes.apple.com (iOS only) Play.google.com (Android only) Youtube.com Map.google.com
Generell	Innerhalb der App werden hilfreiche Links angeboten. Sie werden von Dritten gehostet; ihre Nutzung innerhalb von Siilo liegt jedoch zu 100% im Ermessen des Nutzers. Keine Funktionen der Anwendung hängen von diesen Websites ab oder senden Daten an sie.
Wo werden die Daten gehosted?	Nicht anwendbar
Welche Daten werden verarbeitet?	Keine Anwendungsfunktionen hängen von diesen Websites ab oder senden Daten an diese Websites.
Mehr Informationen	

4.0 Identifikation von Sicherheits- und Datenschutzrisiken

Dieses Kapitel fasst unsere Sicherheits- und Datenschutzrisiken zusammen. Im nächsten Kapitel haben wir beschrieben, wie wir diese Risiken handhaben.

4.1 Meldungsdaten

- Der Lebenszyklus von Nachrichtendaten, die zwischen medizinischen Fachkräften über eine Kommunikations- oder Messenger-App auf Smartphones ausgetauscht werden, wird in zwei Hauptphasen unterteilt. Die geteilten (Patienten-)Informationen können sein:
- im Transit, d. h., wenn die Informationen von einem Gerät zum anderen übertragen werden, und;
- im Ruhezustand, d. h. wenn sich die Informationen nicht in der Übertragung befinden.

Im Gegensatz zu dem, was der Begriff "in Ruhe" suggeriert, sind oft Informationen, die auf einem Telefon empfangen oder erstellt wurden, selten jemals "in Ruhe". Das Standardverhalten heutiger Apps besteht darin, sich mit anderen Apps und Cloud-Diensten zu synchronisieren. Ein Bild, das über WhatsApp geteilt wird, wird beispielsweise automatisch mit der Kamera-App des Benutzers auf dem Gerät synchronisiert, die dann normalerweise mit Cloud-Diensten synchronisiert wird. Das Gleiche gilt für Textnachrichten auf WhatsApp: All diese sensiblen Inhalte werden automatisch in der iCloud oder den Google-Cloud-Diensten gesichert. Da die meisten Verbraucher-Apps diesem Muster folgen, bedeutet dies, dass bei der Verwendung dieser Arten von Messengern persönliche (Patienten-)Daten außerhalb der Kontrolle der Fachkräfte oder der Organisationen, für die sie arbeiten, durchsickern. Darüber hinaus werden die ausgetauschten Informationen standardmäßig nicht gelöscht und sammeln sich daher in unendlichen Mengen über mehrere Standorte und Geräte hinweg an. Dieser Mangel an Kontrolle macht die Verwendung von BYOD-Smartphones und Social-Media-Anwendungen für Verbraucher nicht konform mit Gesetzen und Vorschriften (z. B. DSGVO), da personenbezogene Daten, die sensible medizinische Informationen enthalten, mit Sicherheit zu Dritten durchsickern, die nicht an der Versorgung von Patienten beteiligt sind.
Dieses Kapitel zielt darauf ab, die potenziellen Sicherheitsrisiken in diesen beiden Phasen zu beschreiben, sowie die Risiken für die Privatsphäre, wenn die Sicherheit beeinträchtigt wird. Sie sind in der folgenden Tabelle zusammengefasst:

Informationen	Sicherheitsrisiken	Risiken für den Datenschutz
Daten bei der Übertragung	• Man-in-the-Middle-Angriff • kompromittierte Firmenserver • schurkischer Mitarbeiter • Versehentlicher Fehler in der Software • sozial manipulierter Angriff • Replay-Angriff	• Zugriff auf unstrukturierte, verschlüsselte Daten von Patienten, die von allen Fachleuten auf Siilo behandelt werden und noch nicht vom Server gelöscht wurden • Zugriff auf (un)verschlüsselte Informationen von Patienten auf dem Gerät eines einzelnen Fachmanns (Handy, Tablet, Desktop) • Metadaten von Siilo-Nachrichten: Absender, Empfänger, Zeit, Größe der Nachricht • Informationen, die als Profilinformationen von Siilo-Benutzern gekennzeichnet sind • Zugang zu einem Netzwerk von Fachleuten, die dazu verleitet werden können, Informationen über Patienten zu teilen

Daten im Ruhezustand	• physischer Zugriff auf das Telefon des Mitarbeiters • kompromittierte Firmenserver • Abtrünniger Mitarbeiter • kompromittiertes Benutzertelefon • sozial ausgeführter Angriff • unwissentliche Nutzung der Exportfunktionalitäten von Siilo durch einen Benutzer	

Tabelle 4 *Sicherheits- und Datenschutzrisiken von Nachrichtendaten*

Wenn auf das Telefon einer Person ohne Berechtigung zugegriffen wird, kann ein Angreifer möglicherweise Nachrichten lesen, die mit diesem einzelnen Benutzer verbunden sind. Aufgrund des standardmäßigen Löschvorgangs würde ein solcher Angriff begrenzte, unstrukturierte und kleine Mengen an Informationen liefern. Wenn jedoch ein Konto komplett von einem Angreifer gekapert wird, können spezifische Informationen abgerufen werden, was dadurch verschlimmert wird, dass die Kollegen nicht wissen, dass dieses Konto kompromittiert wurde. Dies wird als Social-Engineered-Angriff oder genauer gesagt als Phishing bezeichnet. Bei einem unbefugten Zugriff auf die Siilo-Server, auf denen Informationen und Metadaten für viele Siilo-Benutzer gespeichert sind, sind diese Informationen durch Verschlüsselung geschützt.

4.2 Benutzerdaten

Benutzerinformationen sind für einen Angreifer aus verschiedenen Gründen wertvoll: Die Informationen könnten für Marketing- oder Werbezwecke verkauft werden oder sogar dazu verwendet werden, sozial konstruierte Angriffe auf andere Systeme, einschließlich Siilo, zu starten. Die folgende Tabelle fasst die Sicherheitsrisiken in Bezug auf Siilo Benutzerinformationen und die damit verbundenen Datenschutzrisiken zusammen:

Informationen	Sicherheitsrisiken	Risiken für den Datenschutz
Benutzerdaten	• kompromittierte Firmenserver • Schurkenhafter Mitarbeiter / Siilo.Connect-Admin • versehentlicher Fehler in der Software • sozial manipulierter Angriff	• dass persönliche Informationen von medizinischem Fachpersonal für Werbezwecke, Marketing usw. erlangt werden • dass persönliche Informationen für einen sozial manipulierten Angriff verwendet werden, um Patientendaten zu erhalten

Tabelle 5 *Sicherheits- und Datenschutzrisiken von Benutzerdaten*

5.0 Beschreibung der Lösungen

In diesem Kapitel beschreiben wir die technischen und organisatorischen Kontrollmaßnahmen, die Siilo implementiert hat, um die potenziellen Risiken, die im vorherigen Kapitel identifiziert wurden, zu minimieren.

5.1 Organisatorische und administrative Richtlinien und Kontrollen

Siilo hat ein Informationssicherheitsmanagementsystem (ISMS) implementiert und ist nach ISO27001 und NEN7510 (niederländischer Standard für das Management der Informationssicherheit im Gesundheitswesen) zertifiziert. Als Teil des ISMS hat Siilo mehrere organisatorische und administrative Richtlinien und Kontrollen implementiert, wie z. B. regelmäßige und standardmäßige Risikobewertungen, interne Audits, eine Informationssicherheitsrichtlinie, eine Least-Privilege-Richtlinie, Mitarbeiterschulungen, ein (Sicherheits-)Vorfallmanagementverfahren und ein Verfahren zur Benachrichtigung bei Datenverletzungen. Das Ziel von Siilos ISMS ist es, eine weitere Verbesserung der Organisation, der Mitarbeiter und der Produkte zu ermöglichen.

Jede Lösung, die Siilo implementiert, durchläuft eine Risikobewertung und eine Datenschutzfolgenabschätzung. Sie folgt einem strengen Prozess, der durch unsere ISMS-Richtlinien abgesichert ist, was durch unsere ISO-27001 und NEN7510 Zertifikate belegt wird. Siilo hat einen unabhängigen Sicherheitsbeauftragten und Datenschutzbeauftragten ernannt, der bei der niederländischen Datenschutzbehörde registriert ist.

Entwicklungsprozess

Der Entwicklungsprozess von Siilo verwendet mehrere Strategien, um sowohl die Qualität als auch die Sicherheit der Daten zu gewährleisten:
(1) Unit-Tests: Für jede Funktion entwickeln wir eine Reihe von Basistests, die diese Funktion isoliert testen;
(2) Peer-Code-Review: Änderungen an der App werden von mindestens zwei Entwicklern überprüft, bevor sie in eine Beta-Version aufgenommen werden. Bei Funktionen, die sich auf sicherheits- oder datenschutzrelevante Aufgaben auswirken, werden diese neuen Zeilen Softwarecode von einem leitenden Entwickler außerhalb des Teams überprüft, und der leitende Entwickler spricht sich mit dem Sicherheitsbeauftragten und dem Datenschutzbeauftragten ab, bevor die neue(n) Funktion(en) für den Messenger freigegeben werden.
(3) Manuelle Tests und begrenzte öffentliche Beta: Vor der Freigabe werden Funktionen intern für manuelle Tests freigegeben und oft auch für einen ausgewählten Pool von "freundlichen Beta-Testern". Dieser Ansatz wird verwendet, um gerätespezifische Funktionen sowie alle Funktionen zu prüfen, die sich erst herauskristallisieren, nachdem sie einer Vielzahl von Arbeitsabläufen ausgesetzt wurden.

Least privilege

Privilegien werden den Siilo-Mitarbeitern auf einer strengen Need-to-have-Basis gewährt. Dies wird jährlich von einem Sicherheitsbeauftragten überwacht und überprüft. Jeder Siilo-Mitarbeiter, der Zugriff auf Informationen außerhalb der ihm zugewiesenen Rolle benötigt, muss die Anfrage zunächst mit unserer Standardvorlage protokollieren.
Diese Anfragen werden protokolliert und vom Datenschutzbeauftragten autorisiert, wenn eine Anfrage als konform mit der General Data Protection Regulation angesehen wird, bevor sie erfüllt wird. Diese Anfragen werden außerdem einmal pro Quartal vom Siilo ISO-27001-Komitee überprüft, das aus dem Datenschutzbeauftragten und dem Chief Executive Officer und/oder dem Chief Financial Officer von Siilo besteht.

5.2 Technische Richtlinien und Kontrollen

Nachrichtendaten - Daten bei der Übertragung

To understand the solutions to mitigate the risks for data in transit, please read our security white paper (https://www.siilo.com/resources/security-white-paper) as it describes in detail our security-by-design approach, the threat model and cryptographic protocols.
In short, Siilo uses end-to-end encryption implemented with LibSodium, a fork of the NaCl crypto library https://nacl.cryp.to/. This means that each message between sender and receiver (Alice and Bob in Figure 2) is protected via a public/private keypair. Only Alice and Bob are able to decrypt and read the messages they exchange, and the authenticity of any message can be empirically verified. Third parties, including Siilo company and its employees are never able to read them.

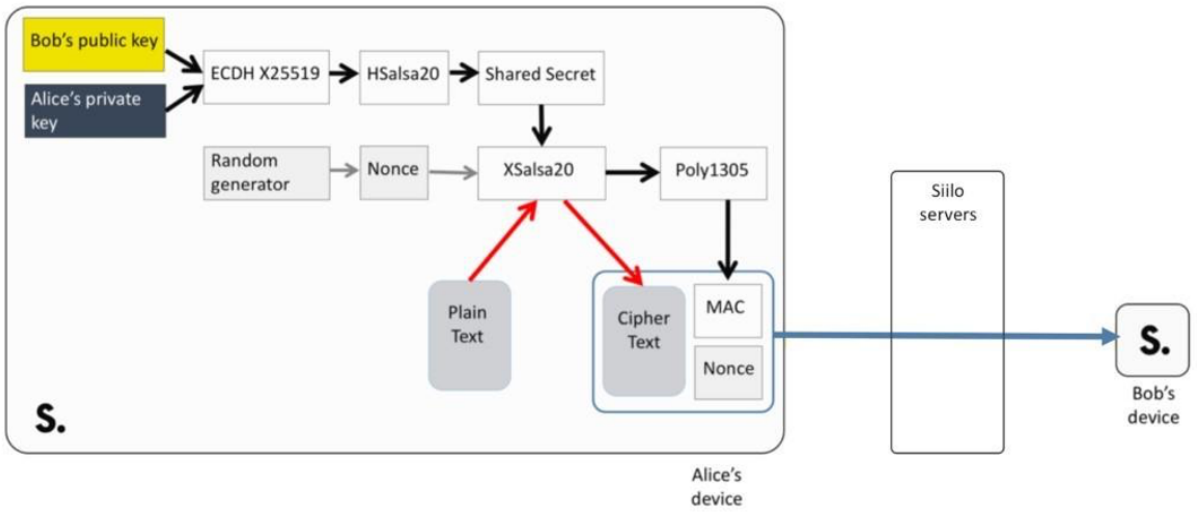

Abbildung 2 Schematische Darstellung des Verschlüsselungsprotokolls zwischen der Siilo-App von Alice und der Siilo-App von Bob.

Siilo verwendet Certificate Pinning, um sogenannte "Man-in-the-Middle"-Angriffe zu verhindern, bei denen Angreifer auf den Datenverkehr zwischen den Telefonen zugreifen und versuchen, in die Kommunikationsleitungen einzubrechen und diese anzuzapfen, um die Nachrichten zu lesen. Die Standard-TLS-v1.2-Kommunikation erfordert ein gültiges SSL-Zertifikat, das von einer vertrauenswürdigen Zertifizierungsstelle ausgestellt und vom Gerät erkannt wurde. Certificate Pinning geht noch weiter und schreibt vor, dass diese Zertifikate nur von einer Vertrauenskette ausgestellt werden dürfen, die auf einen bestimmten Aussteller zurückgeht. Dies schließt eine ganze Reihe von Schwachstellen, die sich aus den Problemen bei der Schlüsselverteilung im Zusammenhang mit der Infrastruktur der Zertifizierungsstellen im Internet ergeben.

Die Verschlüsselung von Siilo erzwingt das Konzept der "Public-Key-Authentifikatoren", ein von Forschern geprägter Begriff. Diese Eigenschaft ermöglicht es der Anwendung, mathematisch zu beweisen, dass die Nachricht von einer der beiden Parteien (Sender/Empfänger) stammt. Dieses Verfahren ist jedoch aufgrund der Art von Social-Engineering-Angriffen, bei denen Personen ähnliche Namen oder Profilfotos verwenden, um sensible Informationen von einer potenziellen Zielperson zu ergaunern, nicht sicher genug. Ein Mechanismus, der diese Art von Angriffen verhindern kann, ist die sogenannte Out-of-Band-Verifikation. Siilo unterstützt diesen Prozess, indem es dem Benutzer erlaubt, zu seinem Profil zu gehen und seine einzigartige ID zu sehen, die "Key Fingerprint" genannt wird. Zwei Benutzer können diese IDs austauschen; idealerweise persönlich, und so sicherstellen, dass sie tatsächlich die sind, die sie vorgeben zu sein.

Siilo verwendet einen Key-Revoke-Mechanismus auf passive Weise: Benutzer sind nicht in der Lage, einen Knopf innerhalb der App zu drücken, um seine Schlüssel zu erneuern. Die Benutzer haben kein Interesse an dieser technischen Verschlüsselung. Um die App einfach zu halten, wurde dieser Button daher weggelassen. Außerdem will Siilo verhindern, dass jemand versehentlich diesen Button aktiviert und alle Daten verliert. Es ist jederzeit möglich, öffentliche Schlüssel über den Fingerabdruck im Profil der App zu vergleichen und zu überprüfen.

Nachrichtendaten - Daten im Ruhezustand auf dem Benutzergerät

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

- Das gesamte "Schlüsselmaterial", auch bekannt als die vom Kryptographen verwendeten Codes, wird in der iOS KeyChain bzw. im Android KeyStore gespeichert;
- Das gesamte "Schlüsselmaterial" wird mit einem "Hauptschlüssel" verschlüsselt, der sich aus dem vom Benutzer gewählten Pin-Code ableitet;
- Die gesamte Datenbank wird mit SQLiteCipher verschlüsselt. Alle Nachrichten, Nachrichten-Metadaten und Kontaktinformationen werden auf diese Weise gespeichert;
- Alle empfangenen Medien werden mit dem symmetrischen Einweg-Schlüssel verschlüsselt gespeichert. Der Zugriff auf diesen Schlüssel erfolgt über die oben genannte Datenbank;
- Ein Pincode-Mechanismus auf Anwendungsebene verhindert den Zugriff durch Menschen, die physischen Zugriff auf das Gerät haben. Dies adressiert die meisten Formen von Social Engineering in Person, wie z. B. die Bitte, das Telefon für einen schnellen Anruf auszuleihen, etc.
- Alle ausgetauschten Informationen in der Siilo App werden automatisch nach 30 Tagen gelöscht. Benutzer können selbst entscheiden, einzelne Nachrichten ad hoc zu löschen, wenn sie 30 Tage für zu lang halten. Wir haben bewusst keine Countdown-Timer und Nachrichtenlaufzeiten wie Sekunden/Stunden eingebaut, da wir glauben, dass dies ein Gefühl der Dringlichkeit erzeugen würde, was zu Screenshots und anderem unerwünschten Verhalten auf der Empfängerseite führen würde;
- Wenn ein Benutzer weiß, dass sein Gerät verloren, gestohlen oder anderweitig kompromittiert wurde, kann er seine Organisation benachrichtigen (dies ist eine Siilo Connect Funktion) und ein Siilo Connect Admin kann die Siilo Daten aus der Ferne von dem Gerät löschen.

Nachrichtendaten - Daten im Ruhezustand auf Siilo-Servern

Für die auf den Siilo-Servern ruhenden Daten gelten die folgenden Sicherheitsvorkehrungen:

- Alle Siilo-Server befinden sich innerhalb der Europäischen Union mit den höchsten Sicherheits- und Compliance-Normen;
- Firewall-Regeln verhindern den Netzwerkzugriff auf die Datenbanken (MySQL und ElasticSearch) und ist auf ein Subnetz mit den Siilo-Servern und ein VPN beschränkt, auf das eine begrenzte Gruppe von Siilo-Mitarbeitern zugreifen kann;
- Die MySQL-Datenbank ist passwortgeschützt und mit dem Industriestandard AES-256 verschlüsselt und speichert Messaging-Daten, Messaging-Metadaten, Siilo Connect Konfigurationsdaten und Benutzerprofildaten;
- ElasticSearch verschlüsselt bestimmte Felder wie E-Mail und Telefonnummern, um einen Abgleich zu ermöglichen. Andere Profilfelder, die in der App als "öffentlich" für Siilo-Mitglieder angezeigt werden, werden im Klartext gespeichert;
- Alle Medien (die über die Anwendung versendet werden und somit als sensibel gelten) werden gespeichert und mit einem symmetrischen Einweg-Schlüssel verschlüsselt. Dieser Schlüssel wird auf keinem Siilo Server gespeichert, außer als Teil der verschlüsselten Nachrichtendaten, die in MySQL gespeichert werden. Die Schlüssel zum Entschlüsseln dieser Daten sind nur auf den Geräten des Senders und des Empfängers verfügbar.

Speicherung von personenbezogenen Daten auf Siilo-Servern

Die Nachrichtendaten werden auf Servern in Frankfurt (Deutschland) gespeichert. Zu Sicherungszwecken werden täglich automatisierte "Snapshots" erstellt, die nicht länger als 7 Tage gespeichert werden. Diese Snapshots sind im Ruhezustand verschlüsselt.

Die Server-Infrastruktur von Siilo wird von Amazon, Inc. gehostet. Siilo hat sich bewusst für Amazon Web Services (AWS) entschieden, da diese die höchsten Sicherheits- und Verschlüsselungsstandards anwenden und mit ihren SOC Level I-II-III, ISO9001, ISO27001, ISO27017 und ISO27018 Zertifizierungen die Einhaltung der (DSGVO) gewährleisten.

Benutzerdaten

Die Benutzerdaten werden auf Servern in Dublin (Irland) gespeichert und werden täglich gesichert und nicht länger als 30 Tage in einem vorkonfigurierten Bucket gespeichert, der im Ruhezustand verschlüsselt ist. Siilo Benutzerdaten werden mit den folgenden Sicherheitsmaßnahmen in Bezug auf die persönlichen Informationen, die wir von unseren Benutzern sammeln, behandelt:

Informationen	Sicherheitsmaßnahmen
Namen (Vorname, Nachname)	Nicht verschlüsselt in der Siilo-Datenbank, gesichert durch ISMS-Richtlinien
Rufnummer	Verschlüsselt in der Siilo-Datenbank und gesichert durch ISMS-Richtlinien
E-Mail Adresse(n)	Verschlüsselt in der Siilo-Datenbank und gesichert durch ISMS-Richtlinien
Medizinische Registrierungsnummer	Verschlüsselt in der Siilo-Datenbank und gesichert durch ISMS-Richtlinien
Avatar-Bild	Nicht verschlüsselt in der Siilo-Datenbank, gesichert durch ISMS-Richtlinien
Medizinischer Beruf	Nicht verschlüsselt in der Siilo-Datenbank, gesichert durch ISMS-Richtlinien
Titel(s)	Nicht verschlüsselt in der Siilo-Datenbank, gesichert durch ISMS-Richtlinien
Spezialisierung(en)	Nicht verschlüsselt in der Siilo-Datenbank, gesichert durch ISMS-Richtlinien
Interesse(n)	Nicht verschlüsselt in der Siilo-Datenbank, gesichert durch ISMS-Richtlinien
Organisation/Verband	Nicht verschlüsselt in der Siilo-Datenbank, gesichert durch ISMS-Richtlinien
Telefonnummern von Kontakten	Verschlüsselt in der Siilo-Datenbank und gesichert durch ISMS-Richtlinien
Auffindbarer Gruppenname, Gruppenbeschreibung	Nicht verschlüsselt in der Siilo-Datenbank, gesichert durch ISMS-Richtlinien
Foto von medizinischem Ausweis, Führerschein oder Reisepass	Verschlüsselt in der Siilo-Datenbank und gesichert durch ISMS-Richtlinien

Tabelle 6 *Sicherheitsmaßnahmen der vom Benutzer bereitgestellten Daten*

Informationen	Sicherheitsmaßnahmen
Anzahl der Kontakte	Nicht verschlüsselt in der Siilo-Datenbank, gesichert durch ISMS-Richtlinien
Geräteinformationen: Benutzer-IP-Adresse Typ des mobilen Geräts Betriebssystem Version der App Sprache des Geräts Push-Ziel WhatsApp installiert Adobe Acrobat installiert Touch-ID aktiviert Face-ID aktiviert	Nicht verschlüsselt in der Siilo-Datenbank, gesichert durch ISMS-Richtlinien
Anzahl der Gruppen	Nicht verschlüsselt in der Siilo-Datenbank, gesichert durch ISMS-Richtlinien
Organisatorische Rolle	Nicht verschlüsselt in der Siilo-Datenbank, gesichert durch ISMS-Richtlinien
Wie viele Nachrichten gesendet/empfangen	Nicht verschlüsselt in der Siilo-Datenbank, gesichert durch ISMS-Richtlinien
Wie viele und welche Tage online (letzte 30 d)	Nicht verschlüsselt in der Siilo-Datenbank, gesichert durch ISMS-Richtlinien
Web-App-Aktivierung und aktuelle Sitzungen	Nicht verschlüsselt in der Siilo-Datenbank, gesichert durch ISMS-Richtlinien

Tabelle 7 Sicherheitsmaßnahmen der von Siilo gesammelten Benutzerdaten

Informationen	Sicherheitsmaßnahmen
Wer chattet mit wem, zu welcher Zeit genau	Nicht verschlüsselt in der Siilo-Datenbank, gesichert durch ISMS-Richtlinien
Zeit und Dauer von VoIP-/Videoanrufen	Nicht verschlüsselt in der Siilo-Datenbank, gesichert durch ISMS-Richtlinien
Größe der Nachricht	Nicht verschlüsselt in der Siilo-Datenbank, gesichert durch ISMS-Richtlinien
Welche Gruppen aktiv sind	Nicht verschlüsselt in der Siilo-Datenbank, gesichert durch ISMS-Richtlinien
Gruppennamen von privaten Gruppen	Nicht verschlüsselt in der Siilo-Datenbank, gesichert durch ISMS-Richtlinien

Zusammensetzung der Gruppen	Nicht verschlüsselt in der Siilo-Datenbank, gesichert durch ISMS-Richtlinien

Tabelle 8 Sicherheitsmaßnahmen der von Siilo erfassten Benutzerdaten, um die Übertragung von Nachrichtendaten zu ermöglichen

Telefonnummernabgleich auf Siilo

Siilo lässt den Benutzer optional andere Siilo-Kontakte durch einen Querverweis mit dem Adressbuch des Telefons entdecken. Wenn der Benutzer dies wählt, werden die folgenden Informationen über eine verschlüsselte TLS-Verbindung zum Server hochgeladen:

(1) Die ersten 64bits des SHA1-Hashes der E.164-normierten Form jeder Telefonnummer, die im Adressbuch des Telefons gefunden wurde

(2) Schlüssel: EEDAAC207FC6BA08727C

(3) Nur die Telefonnummern werden gehasht und mit Querverweisen versehen. Siilo berührt nicht die zugehörigen Namen, E-Mail-Adressen und andere Informationen, die das Adressbuch des Telefons enthält. Der Siilo Server vergleicht dann die Liste der Hashes des Benutzers mit den bekannten Telefon-Hashes der aktuellen Siilo Benutzer. Der Server vergleicht nur mit aktuellen Siilo-Benutzern und verwirft nach der Rückgabe der Übereinstimmungen an den mobilen Client sofort die übermittelten Hashes.

6.0 Sillo Connect

Organisationen des Gesundheitswesens können ihre Mitglieder auf Siilo in einzelnen, manchmal auch mehreren Netzwerken organisieren. Um Organisationen dies zu ermöglichen, hat Siilo ein Tool zur Mitgliederverwaltung entwickelt. Siilo Connect ist der Name des Web-Tools für unsere Kunden. Der Kunde entscheidet, wer dieses Web-Tool bedient (der Siilo Connect Admin).

Mit diesem Produkt können Organisationen ihre Mitglieder über jedes der unterstützten Matching-Kriterien, die ihnen bekannt sind und mit denen sich der Siilo-Benutzer auf der Plattform registriert hat, sicher einbinden, wie z. B;

- gesamte E-Mail-Adresse, z. B. "t.smith@examplehospital.com"
- E-Mail-Domäne, z. B. "@examplehospital.com"
- Telefonnummer
- gängige medizinische Registrierungs-IDs

Organisationen, die diese Art von Informationen nicht kennen, können ihre Mitglieder auch per QR-Code-Scan oder über den Siilo Service Desk Chat einbinden. Bei der letzteren Option müssen die Benutzer eine eindeutige Phrase angeben, die sie von ihrer Organisation erhalten haben. Wenn sie diese Phrase an den Siilo Service Desk senden, werden sie automatisch zu dieser Organisation auf Siilo hinzugefügt.

Siilo Connect Kunden müssen zunächst eine E-Mail-Adresse oder Telefonnummer kennen, mit der ein Siilo Nutzer auf der Plattform registriert ist oder dies in Zukunft tun wird. Dies wird diese Siilo Nutzer mit den Mitgliedern ihrer Organisation abgleichen. Die einzigen Siilo Benutzerinformationen, die sie erhalten werden, sind:

- die Namen der Siilo-Benutzer, die zu ihrer Organisation auf Siilo gehören;
- die E-Mail-Adresse oder Telefonnummer, mit der sich ein Siilo-Benutzer bei der App angemeldet hat (die sie bereits kennen).

Siilo wird niemals die persönlichen Informationen von Siilo Nutzern mit anderen Siilo Kunden teilen. Allerdings kann Siilo Connect Kunden erlauben, Profilfelder zu ihrem organisationsspezifischen Profil auf Siilo hinzuzufügen. Wenn sie sich dafür entscheiden, können sie Profilfelder wie "Telefonnummer", "E-Mail-Adresse" oder "medizinische Lizenznummer" einführen. Es ist die eigene Entscheidung des Siilo Nutzers, dies auszufüllen, da es keine Pflicht ist, etwas auf der Profilseite auszufüllen (Opt-In).

Wenn Sie in einer Organisation sind, können Benutzer das organisationsspezifische Profil der anderen Benutzer sehen. Außenstehende sehen diese Profilinformationen nicht, es sei denn, die Organisation wünscht dies. Eine Organisation kann auch Profilinformationen enthalten, die für alle Benutzer, einschließlich der Organisationsmitglieder selbst, verborgen sind (z. B. Mitgliedskennungen).

Auf organisatorischer Ebene werden Siilo Connect Kunden Zugang zu Nutzungsinformationen haben, insbesondere:

- Anzahl der Mitglieder, die pro Tag online sind;
- Anzahl der Gruppen, die pro Tag online sind;
- Anzahl der gesendeten Nachrichten pro Tag;
- Anzahl der Gesamt(un)registrierungen pro Tag.

Diese Statistiken sind nicht auf einzelne Benutzer rückführbar. Um ein Reverse Engineering dieser Zahlen zu verhindern, indem einzelne oder Gruppen von Benutzern hinzugefügt/entfernt werden, um mehr über sie zu erfahren, werden sie historisch festgelegt. Außerdem erhalten Benutzer, wenn sie zu ihrer Organisation hinzugefügt/entfernt werden, eine Push-Benachrichtigung vom Siilo Service Desk, dass dies geschehen ist.

Innerhalb von Siilo Connect hat der Benutzer die Möglichkeit, Daten selbst anzupassen. Siilo Connect Admins können die folgenden Informationen ändern:

Informationen	Änderbar für Siilo Connect Admin
Name der Organisation	Ja
Logo der Organisation	Ja
Name und Beschreibung einer Organisation Service-Desk-Chat	Ja
Name und Beschreibungen von Organisationsgruppen	Ja
Interner Name des Benutzers zur internen Identifikation	Ja
Organisationsspezifische Profilfelder	Ja
Persönliche Informationen des Benutzers (Tabelle 1)	Nein
Aktivitäten protokollieren	Nein

Tabelle 9 Änderbare Daten durch Siilo Connect Admin

Siilo Connect Admins können den Namen, die Berufsbezeichnung oder andere persönliche Daten nicht ändern. In Tabelle 2 finden Sie eine Übersicht über alle persönlichen Daten, die Siilo Benutzer bewusst als Teil des Registrierungsflusses ausfüllen. Siilo Connect Admins haben keinen Zugriff auf protokollierte Ereignisse.

7.0 Der kontinuierliche Prozess der Sicherheit

Sicherheit wird oft als ein gewünschter Endzustand wahrgenommen, der letztlich durch Verschlüsselung erreicht wird. Aber Sicherheit besteht nicht nur aus Verschlüsselungsprotokollen. Es ist ein kontinuierlicher Prozess, eine Kultur, eine Denkweise. Das Risiko, dass ein Außenstehender die Siilo-Software angreift, ist ein ganz anderes, aber ebenso wichtiges, als die internen Risiken, die entstehen können, und kann nicht einfach durch Verschlüsselung gelöst werden, sondern durch die in der Unternehmenskultur verankerten Werte.

Eine Unternehmenskultur ist die Gesamtheit der Bräuche, Traditionen und Werte der Menschen in dieser Organisation. Die Kultur eines Unternehmens kann an bestimmten Parametern beobachtet werden, wie z.B. der Annahme von Feedback von Benutzer- und Sicherheits-Communities, dem Prozess, wie kritisches Feedback empfangen und verarbeitet wird und wie transparent ein Unternehmen bezüglich seines Feedbacks ist. Siilo glaubt, dass es einen Teil seiner Kultur demonstriert, indem es:

- Kommunikation, wie z. B. dieses Dokument zur Datenschutz-Folgenabschätzung;
- seine ISO27001- und NEN7510-Zertifizierung, über sein Informationssicherheitsmanagement;
- seine (halb)jährlichen Audits und Penetrationstests durch angesehene externe Sicherheitsexperten;
- die regelmäßige Schulung der Mitarbeiter
- die Bereitstellung des Quellcodes von Siilo für Fachleute, die Interesse an der Untersuchung des Codes haben.

Was würden wir uns von Ihnen wünschen?

In diesem Dokument hat Siilo viele organisatorische, administrative und technische Kontrollen implementiert, um potentielle Risiken zu reduzieren und Ihnen einen sicheren Produkt- und Messaging-Service zu bieten.
Wir erwarten von Ihnen, als Nutzer, dass Sie mit persönlichen Daten genauso sorgfältig umgehen wie wir. Wir möchten betonen, wie wichtig es ist, Ihren Siilo-Pin-Code vertraulich zu behandeln und ihn niemals an andere weiterzugeben.

Möchten Sie mehr Informationen über Siilo, seine Sicherheits- oder Datenschutzrichtlinien? Haben Sie Vorschläge zur Verbesserung dieses Dokuments oder unserer App? Bitte kontaktieren Sie uns unter privacy@sillo.com.