October 30, 2019

Rev. 0.9

Technische und organisatorische Maßnahmen (TOM)

Allgemeine Beschreibung zum internen Kontrollsystem von Siilo

Die Geschäftsführung von Siilo ist für die Informationssicherheitspolitik verantwortlich und stellt sicher, dass die die Kriterien für ISO 27001:2013 , NEN 7510:2017 (Niederlande), HIPAA (USA), NHS (UK) sowie relevante Gesetze und Verordnungen in anderen Ländern. Siilo ist nach ISO2700:2013 und NEN7510:2017 (der niederländische Standard für das Management der Informationssicherheit im Gesundheitswesen) zertifiziert. Im Rahmen dieser Standards hat Siilo ein Informationssicherheits-Managementsystem eingerichtet sowie Richtlinien und Verfahren implementiert, die organisatorische, physische und technische Kontrollen in Bezug auf die Informationssicherheit garantieren. Datenschutz ist von wesentlicher Bedeutung für Siilo. Daher führt Siilo jährlich eine Datenschutzfolgenabschätzung der Siilo-App durch.

Siilo unterscheidet zwischen zwei Arten von Daten:

(1) Nachrichtendaten: Dies bezieht sich auf Daten, die von unseren Benutzern untereinander gesendet werden. Da Angehörige der Gesundheitsberufe die Hauptnutzer der Siilo-App sind, wird davon ausgegangen, dass unsere Benutzer sensible Informationen und personenbezogene Daten zur Gesundheit von Patienten (betroffenen Personen) übertragen. Einfach ausgedrückt ist Siilo ein Prozessor für Nachrichtendaten. Unsere Benutzer sind die Kontrolleure der Nachrichtendaten.

(2) Benutzerdaten: Dies sind die persönlichen Daten von Benutzern, die Siilo sammeln muss, um ein sicheres und konformes Funktionieren der Siilo-App zu gewährleisten. Siilo ist ein Controller für Benutzerdaten; Unsere Nutzer sind die betroffenen Personen.

Dies ist von äußerster Wichtigkeit und kann nicht genug betont werden: Nachrichtendaten, die in Gesundheitsteams geteilt werden, sollten niemals für jemanden verfügbar sein, der nicht direkt an der optimalen Versorgung des betreffenden Patienten beteiligt ist.

Aufgrund der Art der Siilo-Verschlüsselungsprotokolle können Mitarbeiter - oder andere - niemals verstehen, welche (persönlichen) Informationen geteilt werden und warum sie geteilt werden. Aus diesem Grund konzentriert sich Siilo nur auf den Prozess der Freigabe und entwickelt die App so, dass diese Freigabe so sicher wie möglich erfolgt, ohne den Benutzer zu belasten.

1. Zutrittskontrolle

Maßnahmen, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten verarbeitet und genutzt werden, zu verwehren:

Siilos Server-Infrastruktur wird von Amazon, Inc in Europa gehostet. Siilo hat gezielt Amazon Web Services (AWS) ausgewählt da somit die höchsten Sicherheits- und Verschlüsselungsstandards (DSGVO-konform) gegeben sind und die Einhaltung der SOC Level III-III, ISO9001, ISO27001, ISO27017- und ISO27018-Zertifizierungen gewährleistet sind. Ein physischer Zugriff auf die persönlichen (Gesundheits-) Informationen ist somit nicht möglich. In den Büros von Siilo werden keine Patientendaten gehostet und die physische Sicherheit der Siilo Büros wird durch die ISO27001 Zertifizierung abgedeckt.

Dies wird unter Zertifizierungen behandelt:
A5 - Informationssicherheitsrichtlinien
A11 - Physische Sicherheit und Umweltsicherheit
A15 - Lieferantenbeziehungen

2. Zugangskontrolle

Maßnahmen, um zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können:

Die Mitarbeiter von Siilo erhalten Zugriff auf Informationen erst wenn dies notwendig für die Erfüllung ihrer Arbeit ist. Unsere Informationssysteme gewähren Benutzern Zugriff nur wenn sich diese im Systemen, mit eindeutigen Kennungen ausweisen können wodurch eine eindeutige Rückverfolgung von Aktivitäten auf die Mitarbeiter möglich ist. Auf diese Weise kann Siilo die Mitarbeiter für Aktivitäten in den Informationssystemen eindeutig verantwortlich machen. Geeignete Sicherheitskontrollen schützen Siilo vor unbefugtem Zugriff auf Daten, die über elektronische Kommunikationsnetze wie das Internet übertragen werden. Unser Sicherheitsteam überprüft die Übermittlungsmethoden und bestimmt geeignete Methoden zum Schutz der übertragenen Daten. Es wird eine Verschlüsselung verwendet um die Vertraulichkeit, Integrität und Verfügbarkeit unserer Daten zu schützen.

Dies wird in den folgenden Abschnitten unserer Zertifizierung behandelt:
A6 - Organisation der Informationssicherheit
A9 - Zugangskontrolle
A10 - Kryptographie
A12 - Betriebssicherheit
A13 - Kommunikationssicherheit

3. Zugriffskontrolle

Maßnahmen, die sicherstellen, dass die Nutzung eines Datenverarbeitungssystems ausschließlich auf die Zugriffsberechtigung unterliegenden Daten zugreifen kann, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

Die Mitarbeiter von Siilo erhalten Zugriff auf Informationen erst wenn dies notwendig für die Erfüllung ihrer Arbeit ist. Unsere Informationssysteme gewähren Benutzern Zugriff nur wenn sich diese im Systemen, mit eindeutigen Kennungen ausweisen können wodurch eine eindeutige Rückverfolgung von Aktivitäten auf die Mitarbeiter möglich ist. Auf diese Weise kann Siilo die Mitarbeiter für Aktivitäten in den Informationssystemen eindeutig verantwortlich machen.
Die Siilo- Verschlüsselungsprotokolle sind so gestaltet, dass Mitarbeiter - oder andere – grundsätzlich nicht nachvollziehen können welche (persönlichen) Informationen geteilt werden und warum sie geteilt werden. Backups werden grundsätzlich verschlüsselt gespeichert.

Dies wird in den folgenden Abschnitten unserer Zertifizierung behandelt:
A6 - Organisation der Informationssicherheit
A9 - Zugangskontrolle
A10 - Kryptographie
A12 - Betriebssicherheit
A18 - Einhaltung

4. Trennungskontrolle

Maßnahmen, die sicherstellen, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:

Die Verarbeitung von Nachrichten- und Nutzerdaten ist logisch getrennt. Wir haben einen strengen Entwicklungsprozess, um sowohl die Qualität als auch die Sicherheit der Daten zu gewährleisten. Produktions-, Test- und Entwicklungsumgebung sind voneinander getrennt, um die Risiken von unberechtigten Zugriffen oder Änderungen der Betriebsumgebung zu reduzieren.

Dies wird in den folgenden Abschnitten unserer Zertifizierung behandelt:
A9 - Zugangskontrolle
A12 - Betriebssicherheit
A13 - Kommunikationssicherheit

5. Weitergabekontrolle

Maßnahmen, die sicherstellen, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist:

Nachrichtendaten:
Die Siilo-Verschlüsselungsprotokolle sind so gestaltet, dass Mitarbeiter - oder andere - niemals verstehen, welche (persönlichen) Informationen geteilt werden und warum sie geteilt werden. Dies gilt auch für die Datenübertragung. Nachrichten werden nach 30 Tagen automatisch gelöscht. Eine Abweichung von diesen Standardeinstellungen muss vom Benutzer gezielt vorgenommen werden.

Benutzerdaten:
Um das Siilo-Produkt zu verstehen und zu verbessern, sind Siilo-Mitarbeiter in der Lage auf automatisierte Meta-Informationen zuzugreifen. Siilo stellt sicher, dass dies nur als notwendige Voraussetzung für die Verbesserung der Abläufe durchgeführt wird, und dies spiegelt sich in der Art und Weise wider, wie auf Metadaten zugegriffen wird. Alle Benutzerdaten werden sofort nach Beendigung der Lizenzvereinbarung gelöscht.

Dies wird unter Zertifizierungen behandelt:
A9 - Zugangskontrolle
A10 - Kryptographie

6. Eingabekontrolle

Maßnahmen, die sicherstellen, dass nachträglich geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt wurden:

Unsere Informationssysteme gewähren dem Benutzer Zugriff über eindeutige Kennungen, die die Mitarbeiter von Siilo identifizieren, und ermöglichen die Rückverfolgung von Aktivitäten in Bezug auf Informationssysteme auf eine bestimmte Person durch Verfolgung ihrer eindeutigen Kennung. Auf diese Weise kann die Organisation Benutzer für Funktionen verantwortlich machen, die in Informationssystemen ausgeführt werden, wenn sie in diesen Systemen angemeldet sind. Wir führen stichprobenartige Überprüfungen der Aktivität in unseren Informationssystemen durch. Die Mitarbeiter von Siilo haben keinen Zugang zu diesen Audits. Wenn anhand dieser Berichte verdächtige Aktivitäten identifiziert werden, werden diese untersucht und die Ergebnisse der Untersuchung als Sicherheitsvorfall dokumentiert und zur Vermeidung künftiger Ereignisse entschärft.

Dies wird in den folgenden Abschnitten unserer Zertifizierung behandelt:
A9 - Zugangskontrolle
A12 - Betriebssicherheit

7. Auftragskontrolle

Maßnahmen, die sicherstellen, dass personenbezogene Daten, nur entsprechend den Weisungen des Auftragsgebers verarbeitet werden können (Auftragskontrolle)

Bestimmte Komponenten der Siilo Messenger-Software werden von Drittanbietern an Siilo lizenziert. Diese Anbieter werden als Subprozessoren bezeichnet, da Teile der Benutzerinformationen von Siilo mit ihrer Software interagieren. Beispiel: Wenn sich ein Siilo-Benutzer für die App anmeldet, wird eine SMS an die Telefonnummer dieses Benutzers gesendet, um seine Telefonnummer zu bestätigen. Siilo hat keinen eigenen SMS-Überprüfungsdienst entwickelt, verwendet dazu jedoch Software eines anderen Anbieters. Daher verarbeitet dieser Anbieter die Telefonnummer eines Siilo-Benutzers im Auftrag von Siilo. Siilo hat vertragliche Datenschutzvereinbarungen mit allen Subprozessoren.

Dies wird in den folgenden Abschnitten unserer Zertifizierung behandelt:
A15 - Lieferantenbeziehungen
A18 - Einhaltung

8. Verfügbarkeitskontrolle

Maßnahmen, die sicherstellen, dass personenbezogene Daten, gegen zufällige Zerstörung oder Verlust geschützt sind:

Siilo verfügt über einen detailliert dokumentierten Notfallplan. Die folgenden Grundsätze wurden beim Entwurf des Notfallwiederherstellungsplans berücksichtigt: Nachrichten zwischen Benutzern sollten immer geschützt sein. Dies gilt für ruhende Daten und Daten auf dem Transportweg. Benutzerprofile sollten immer geschützt sein. Dies gilt für ruhende Daten und Daten auf dem Transportweg. Die Kommunikation über Siilo Messenger kann für den Nutzer und die Erfüllung dessen Arbeit unverzichtbar sein. Die Kontinuität von Siilo hat somit höchste Priorität. Im Notfall ist es wichtig, die Nutzer darüber zu informieren was mit ihren (möglicherweise) vertraulichen Informationen geschehen ist und ab wann der Messenger wieder zur Verfügung steht. Es muss auch klar sein, wie viele Informationen verloren gegangen sind und ob Informationen veröffentlicht wurden oder nicht.

Unser Sicherheitsteam sowie autorisiertes Personal (z.B. Contingency-Team) ist verantwortlich für die Datenrettung und Wiederherstellung von Informationssystemen während eines Notfalls. In regelmäßigen Abständen werden unsere Notfallpläne überprüft. Die Pläne werden erforderlichenfalls überarbeitet, um Probleme oder Lücken zu beheben, die durch den Testprozess festgestellt wurden. In Fällen, in denen Sicherheitsvorfälle auftreten, die eine sofortige Änderung unserer Pläne erfordern, werden wir die erforderlichen Änderungen vornehmen, um das Sicherheitsproblem zu beheben.

Dies wird in den folgenden Abschnitten unserer Zertifizierung behandelt:
A6 - Organisation der Informationssicherheit
A12 - Betriebssicherheit
A15 - Lieferantenbeziehungen
A17 - Geschäftskontinuitätsmanagement

9. Pseudonymisierung

Maßnahmen, die gemäß Art. 32 Abs. 1 lit. ein DS-GVO; Kunst. 25 Abs. 1 DS-GVO gewährleistet, dass verarbeitete Daten ohne zusätzliche Informationen nicht mehr einer bestimmten Person zugeordnet werden können.

Diese Maßnahmen sind für Siilo nicht zutreffend, da wir modernste Verschlüsselungstechniken verwenden und somit die Daten vollständig anonymisieren.

10. Evaluierung

Maßnahmen zur Überprüfung und Bewertung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung. (zB Datenschutz-Management; Inciden t-Response-Management; Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO); Auftragskontrolle)

Unser Sicherheitsteam führt regelmäßig sowohl die nichttechnische Bewertung der Dokumentation von Richtlinien und Verfahren als auch die technische Bewertung unserer Informationssysteme durch. Die Sicherheitsmaßnahmen werden erforderlichenfalls überarbeitet, um Probleme oder Lücken zu beheben, die bei den Bewertungsverfahren festgestellt wurden. Wir werden sicherstellen, dass die Ergebnisse solcher Bewertungen dokumentiert werden . In

Bezug auf unsere Zertifizierungen / Compliance-Anforderungen haben auch (zwei) jährliche Audits und Penetrationstests durch angesehene externe Sicherheitsexperten stattgefunden .

Dies wird in den folgenden Abschnitten unserer Zertifizierung behandelt:
A18 - Einhaltung