Auftragsverarbeiter-Vereinbarung Siilo

Diese Auftragsverarbeiter-Vereinbarung ist eine Vereinbarung zwischen dem/der Nutzer*in der Apps und/oder Dienste (nachfolgend: „**für die Verarbeitung Verantwortliche**“) und der Siilo Holding B.V., einer nach niederländischem Recht gegründeten Gesellschaft mit Sitz in Keizersgracht 585, 1072 DR Amsterdam, Niederlande (nachfolgend: „**Auftragsverarbeiter**“).

ÜBERLEGUNGEN:

Im Rahmen ihrer vertraglichen Beziehungen verpflichten sich der Auftragsverarbeiter und der für die Verarbeitung Verantwortliche (im Folgenden zusammen: „**Parteien**“), die geltenden Datenschutzgesetze und -vorschriften einzuhalten, einschließlich, aber nicht beschränkt auf die Bestimmungen der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016, die ab dem 25. Mai 2018 gilt (im Folgenden die „DSGVO“).

Der Zweck dieser Vereinbarung mit dem Auftragsverarbeiter besteht darin, die Bedingungen festzulegen, unter denen sich der Auftragsverarbeiter verpflichtet, die Verarbeitung der vom für die Verarbeitung Verantwortlichen zur Verfügung gestellten personenbezogenen Daten durchzuführen, um die Dienstleistungen zu erbringen.

VEREINBARUNG:

1. Definitionen

Die Definitionen im Anhang zu dieser Vereinbarung stehen hier zur Verfügung.

2. Inkrafttreten und Dauer

Diese Vereinbarung tritt mit der Unterzeichnung des Vertrags, dem sie beigefügt ist, in Kraft und bleibt für die Dauer der vertraglichen Beziehung zwischen dem Auftragsverarbeiter und dem für die Verarbeitung Verantwortlichen in Kraft.

3. Status der Parteien

Der Auftragsverarbeiter ist von dem für die Verarbeitung Verantwortlichen ermächtigt, im Namen des für die Verarbeitung Verantwortlichen die für die Erbringung der Dienste erforderlichen personenbezogenen Daten, einschließlich Gesundheitsdaten, unter strikter Einhaltung der in dieser Vereinbarung über die Verarbeitung festgelegten Bedingungen zu verarbeiten.

Wenn der für die Verarbeitung Verantwortliche personenbezogene Daten oder Gesundheitsdaten Dritter in die Applikation und/oder die Dienste eingibt oder wenn er die Dienste nutzt, z. B. Daten von Kolleg*innen oder Patient*innen, muss er die Anforderungen der geltenden Datenschutzgesetze und -vorschriften einhalten.

3.1. Pflichten des für die Verarbeitung Verantwortlichen

Der für die Verarbeitung Verantwortliche ist allein verantwortlich für die Führung eines Verzeichnisses der Verarbeitungstätigkeiten gemäß Artikel 30 Absatz 1 DSGVO und gegebenenfalls für die Erfüllung aller Formalitäten, einschließlich, aber nicht beschränkt auf Meldungen, Registrierungen oder Vorabmeldungen, vor der Durchführung der Verarbeitung von personenbezogenen Daten und Gesundheitsdaten bei der zuständigen Aufsichtsbehörde, soweit dies nach den geltenden Datenschutzgesetzen und -vorschriften erforderlich ist. Der für die Verarbeitung Verantwortliche ist auch dafür verantwortlich, die betroffenen Personen in einer Weise zu informieren, die mit den geltenden Datenschutzgesetzen und -vorschriften, einschließlich, aber nicht beschränkt auf die Artikel 12 bis 14 der DSGVO, übereinstimmt, wenn die personenbezogenen Daten und Gesundheitsdaten der Patient*innen in die Applikation und/oder die Dienste importiert werden.

Der für die Verarbeitung Verantwortliche ist allein für die Richtigkeit, Zuverlässigkeit und Relevanz der personenbezogenen Daten und Gesundheitsdaten verantwortlich. Insbesondere ist der/die Nutzer*in

verantwortlich für die Nutzung der App und/oder der Dienste und die Informationen, die er/sie in der App und/oder den Diensten hinterlegt, speichert, abfragt und entfernt. Der/die Nutzer*in erklärt sich damit einverstanden, Siilo, seine/ihre Vertreter*innen, Mitarbeiter*innen und Unterauftragnehmer von allen Ansprüchen, Haftungen, Schäden und Ausgaben (einschließlich Anwaltsgebühren und -kosten) freizustellen und schadlos zu halten, die Siilo, seinen/ihren Vertretern*innen, Mitarbeitern*innen und Unterauftragnehmern aufgrund der Verletzung dieser Verpflichtung gemäß den geltenden Datenschutzgesetzen und -vorschriften oder gemäß dieser Vereinbarung mit dem Auftragsverarbeiter entstehen.

Um Missverständnissen vorzubeugen: Personenbezogene Daten, die auf den Geräten des für die Verarbeitung Verantwortlichen oder eines Dritten gespeichert sind, stehen unter der Kontrolle des für die Verarbeitung Verantwortlichen oder des Dritten und sind nicht (oder gegebenenfalls nicht mehr) Teil der Verarbeitung durch den Auftragsverarbeiter, auch wenn diese personenbezogenen Daten über die App übertragen wurden oder in der App gespeichert sind.

Der für die Verarbeitung Verantwortliche verpflichtet sich:

- Die ärztliche Schweigepflicht zu respektieren und sicherzustellen;
- Sicherzustellen, dass personenbezogene Daten nur mit anderen Nutzer*innen der Apps und Dienste in Übereinstimmung mit den geltenden Datenschutzgesetzen und -vorschriften geteilt werden;
- Richtlinien zur Autorisierung, Verwaltung von Zugriffsrechten, Rollen und Privilegien zu implementieren, um die Vertraulichkeit von personenbezogenen Daten und Gesundheitsdaten in Übereinstimmung mit den geltenden Datenschutzgesetzen und -vorschriften sowie den geltenden Gesetzen und Vorschriften zum Gesundheitswesen zu gewährleisten;
- Schriftliche Dokumentation aller Anweisungen bezüglich der von Siilo durchgeführten Verarbeitung von personenbezogenen Daten und Gesundheitsdaten;
- Überwachung der von Siilo als Auftragsverarbeiter durchgeführten Verarbeitung;
- Benennung eines speziellen Ansprechpartners, der für die Vertretung des für die Verarbeitung Verantwortlichen zuständig ist;
- Benennung eines Datenschutzbeauftragten, wenn dies gemäß Artikel 37 DSGVO erforderlich ist, wenn der für die Verarbeitung Verantwortliche dies nicht bereits getan hat;
- Gewährleistung der Einhaltung der geltenden Datenschutzgesetze im Vorfeld und während der gesamten Dauer der Verarbeitung.

3.2. Verpflichtungen von Siilo

Siilo verpflichtet sich:

- Personenbezogene Daten und Gesundheitsdaten gemäß den in dieser Vereinbarung mit dem Auftragsverarbeiter festgelegten Zwecken und Rahmenbedingungen zu verarbeiten und die für personenbezogene Daten und Gesundheitsdaten geltenden technischen Standards und bewährten Verfahren einzuhalten;
- Nur nach vorheriger schriftlicher Anweisung des für die Verarbeitung Verantwortlichen und gemäß den in **Anhang 1** dieser Vereinbarung mit dem Auftragsverarbeiter beschriebenen Zwecken zu handeln, es sei denn, eine für den Auftragsverarbeiter geltende gesetzliche Verpflichtung verpflichtet den Auftragsverarbeiter zur Verarbeitung personenbezogener Daten. Im Falle der Unmöglichkeit oder Schwierigkeit, bestimmte Anweisungen auszuführen, informiert Siilo den für die Verarbeitung Verantwortlichen so schnell wie möglich, soweit dies nach den geltenden Gesetzen und Vorschriften zulässig ist. Siilo kann einen schriftlichen Antrag auf Abweichung von den Anweisungen formulieren. Siilo muss die vorherige und ausdrückliche schriftliche Genehmigung des für die Verarbeitung Verantwortlichen einholen, um diese Abweichung durchzuführen. Wenn eine Anweisung des für die Verarbeitung Verantwortlichen nach Ansicht des Auftragsverarbeiters gegen

geltende Datenschutzgesetze oder -vorschriften verstößt, wird der Auftragsverarbeiter den für die Verarbeitung Verantwortlichen unverzüglich darüber informieren;

- Der Auftragsverarbeiter unterstützt den für die Verarbeitung Verantwortlichen bei der Einhaltung der Verpflichtungen gemäß Artikel 35 DSGVO (Datenschutz-Folgenabschätzung) und Artikel 36 DSGVO (Vorherige Konsultation), wobei die Art der Verarbeitung und die dem Auftragsverarbeiter zur Verfügung stehenden Informationen berücksichtigt werden.
- Keine Kopien der personenbezogenen Daten und Gesundheitsdaten ohne die Genehmigung oder Anweisung des für die Verarbeitung Verantwortlichen anzufertigen, sie nicht an Dritte weiterzugeben und sie nicht für andere als die in der Vereinbarung über den Auftragsverarbeiter genannten Zwecke zu verwenden;
- Die ihm vom für die Verarbeitung Verantwortlichen anvertrauten personenbezogenen Daten und Gesundheitsdaten nicht für sich und/oder für Dritte zu verwerten oder zu verarbeiten, gleich zu welchem Zweck und auf welche Weise auch immer;
- Alle ihr zur Verfügung stehenden Mittel im Hinblick auf die vertraglichen Bestimmungen und die Regeln der Technik einzusetzen, um die Sicherheit und die Vertraulichkeit der ihr anvertrauten personenbezogenen Daten und Gesundheitsdaten zu gewährleisten und insbesondere zu verhindern, dass sie nicht verfälscht werden, beschädigt oder an unbefugte Dritte weitergegeben werden, und ganz allgemein die geeigneten technischen und organisatorischen Maßnahmen zu ergreifen, um die personenbezogenen Daten und Gesundheitsdaten vor versehentlicher oder unrechtmäßiger Zerstörung, versehentlichem Verlust, Veränderung, Verbreitung oder unberechtigtem Zugriff zu schützen, insbesondere wenn die Verarbeitung Datenübertragungen in einem Netzwerk beinhaltet, sowie vor jeder Form der unrechtmäßigen Verarbeitung;
- Den für die Verarbeitung Verantwortlichen so schnell wie möglich über jede Sicherheitsverletzung zu benachrichtigen, die sich direkt oder indirekt auf personenbezogene Daten, Gesundheitsdaten oder die Verarbeitung von personenbezogenen Daten auswirkt;
- Regelmäßige Backups der persönlichen Daten durchführen;
- Regelmäßig Penetrationstests (oder Pentest) durchzuführen;
- Die für das ordnungsgemäße Funktionieren der Dienste erforderliche Ausrüstung instand zu halten;
- Die Vertraulichkeit der verarbeiteten Persönlichen Daten und Gesundheitsdaten zu gewährleisten;
- Alle Aktualisierungen, Korrekturen, Löschungen oder sonstigen Änderungen zu berücksichtigen, die der für die Verarbeitung Verantwortliche in Bezug auf die personenbezogenen Daten und Gesundheitsdaten mitteilt;
- Die Aufbewahrungsfrist der personenbezogenen Daten und Gesundheitsdaten für die Zwecke, für die sie erhoben oder bereitgestellt wurden, einzuhalten und sie zu löschen/anonymisieren, sobald diese Zwecke nicht mehr bestehen, vorbehaltlich gesetzlicher Verpflichtungen.

4. Verletzung des Datenschutzes

4.1. Der Auftragsverarbeiter informiert den für die Verarbeitung Verantwortlichen unverzüglich über jede festgestellte Verletzung des Schutzes personenbezogener Daten durch eine elektronische Nachricht oder ein anderes ihm vom für die Verarbeitung Verantwortlichen zur Verfügung gestelltes Kommunikationsmittel.

4.2. Dieser Benachrichtigung sind auf Wunsch des für die Verarbeitung Verantwortlichen und soweit möglich Informationen über die Art der Verletzung des Schutzes personenbezogener Daten, die möglichen Folgen der Verletzung des Schutzes personenbezogener Daten und/oder die Maßnahmen beizufügen, die der für die Verarbeitung Verantwortliche ergriffen hat und/oder zu ergreifen

beabsichtigt, um die Verletzung des Schutzes personenbezogener Daten zu beheben.

4.3. Der Auftragsverarbeiter unterstützt den Verantwortlichen so weit wie möglich bei der Einhaltung der Verpflichtungen gemäß Artikel 33 DSGVO (Meldung einer Verletzung des Schutzes personenbezogener Daten an die Aufsichtsbehörde) und Artikel 34 DSGVO (Mitteilung einer Verletzung des Schutzes personenbezogener Daten an die betroffene Person), wobei er die Art der Verarbeitung und die dem Auftragsverarbeiter zur Verfügung stehenden Informationen berücksichtigt. Der für die Verarbeitung Verantwortliche entscheidet, ob eine Verletzung des Schutzes personenbezogener Daten der Aufsichtsbehörde gemeldet oder der betroffenen Person mitgeteilt werden soll.

5. Information und Rechte der betroffenen Personen

Es liegt in der Verantwortung des für die Verarbeitung Verantwortlichen, die betroffenen Personen (i) über die im Rahmen der Dienste durchgeführte Verarbeitung zu informieren und ihre Einwilligung(en) einzuholen, sofern dies nach geltendem Recht erforderlich ist; (ii) über die Rechtsgrundlage für die durchgeführte Verarbeitung, die Zwecke der Verarbeitung sowie über die Liste der Unterauftragnehmer, die ihre personenbezogenen Daten verarbeiten können, zu informieren.

6. Bearbeitung von Datenanfragen

Es liegt in der Verantwortung des für die Verarbeitung Verantwortlichen, den Anträgen der betroffenen Personen in Bezug auf die in den Artikeln 15 - 22 DSGVO verankerten Rechte bezüglich ihrer personenbezogenen Daten nachzukommen. Soweit dies möglich ist, kann Siilo in seiner Eigenschaft als Auftragsverarbeiter und auf Anfrage des für die Verarbeitung Verantwortlichen den für die Verarbeitung Verantwortlichen bei der Erfüllung seiner Verpflichtung zur Beantwortung solcher Anfragen der betroffenen Personen unterstützen.

7. Vertraulichkeit

7.1. Der Auftragsverarbeiter ist verpflichtet, alle personenbezogenen Daten, die ihm von der verantwortlichen Stelle zur Verfügung gestellt werden, vertraulich zu behandeln, es sei denn, es besteht eine für den Auftragsverarbeiter geltende gesetzliche Verpflichtung oder eine gegenteilige Anweisung der verantwortlichen Stelle.

7.2. Auf Anweisung autorisierter Verwaltungs- und Justizbehörden kann Siilo personenbezogene Daten, die es im Namen und im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet, weitergeben, um seinen rechtlichen Verpflichtungen nachzukommen. In diesem Fall und sofern gesetzlich nicht anders vorgesehen, verpflichtet sich Siilo, den für die Verarbeitung Verantwortlichen über diese Übermittlung zu informieren.

7.3. Der Auftragsverarbeiter stellt sicher, dass alle Personen, die personenbezogene Daten auf Anweisung des Auftragsverarbeiters verarbeiten, einschließlich, aber nicht beschränkt auf Mitarbeiter des Auftragsverarbeiters und Unterauftragnehmer des Auftragsverarbeiters, verpflichtet sind, die personenbezogenen Daten vorbehaltlich des Inhalts dieses Artikels vertraulich zu behandeln.

8. Sicherheit und Überwachung

8.1. Der Auftragsverarbeiter ergreift angemessene technische und organisatorische Maßnahmen gemäß Artikel 32 DSGVO (Sicherheit der Verarbeitung), die mindestens die in **Anhang 2** beschriebenen Maßnahmen umfassen.

8.2. Die oben genannten Verpflichtungen entbinden den für die Verarbeitung Verantwortlichen nicht davon, alle notwendigen technischen und organisatorischen Sicherheitsmaßnahmen für die Sicherheit und Vertraulichkeit aller Informationen, einschließlich personenbezogener Daten, in der App und/oder den Diensten zu treffen.

9. Unterauftragsverarbeiter

Der für die Verarbeitung Verantwortliche erteilt dem Auftragsverarbeiter eine allgemeine schriftliche Genehmigung zur Nutzung der in Anhang 3 aufgeführten Unterauftragsverarbeiter.

Im Rahmen dieser allgemeinen Ermächtigung verpflichtet sich der Auftragsverarbeiter, den für die Verarbeitung Verantwortlichen mit einer Frist von

fünfzehn (15) Tagen schriftlich über alle Änderungen hinsichtlich der Hinzufügung oder des Austauschs von Unterauftragnehmern zu informieren und dem für die Verarbeitung Verantwortlichen die Möglichkeit zu geben, etwaige Einwände gegen diese Änderungen zu erheben. Wenn der für die Verarbeitung Verantwortliche berechtigte und angemessene Gründe hat, gegen die Ernennung eines neuen Unterauftragnehmers Einspruch zu erheben, muss er dies dem Verarbeiter unverzüglich begründen, indem er innerhalb von fünfzehn (15) Werktagen eine schriftliche Mitteilung an den Verarbeiter unter privacy@siilo.com schickt; andernfalls wird davon ausgegangen, dass der für die Verarbeitung Verantwortliche diese Ernennung genehmigt und akzeptiert hat.

Nach Gesprächen und in Ermangelung einer Vereinbarung zwischen dem Auftragsverarbeiter und dem für die Verarbeitung Verantwortlichen kann der für die Verarbeitung Verantwortliche innerhalb von fünfzehn (15) Tagen nach der Benachrichtigung den von der fraglichen Aktualisierung betroffenen Teil des Vertrags kündigen.

In Bezug auf jeden Unterauftragnehmer ist der Auftragsverarbeiter verpflichtet, (i) bei der Bewertung, Beauftragung und Überwachung der Verarbeitungstätigkeiten der Unterauftragnehmer die wirtschaftlich angemessene Sorgfalt walten zu lassen; (ii) in den Vertrag zwischen dem Auftragsverarbeiter und jedem Unterauftragnehmer Klauseln aufzunehmen, die ein gleichwertiges Schutzniveau für die im Auftrag des Verantwortlichen verarbeiteten personenbezogenen Daten und Gesundheitsdaten gewährleisten, wie es in dieser Vereinbarung mit dem Auftragsverarbeiter vorgesehen ist.
Wenn ein Unterauftragnehmer seinen Verpflichtungen in Bezug auf den Schutz personenbezogener Daten nicht nachkommt, bleibt der Auftragsverarbeiter gegenüber dem für die Verarbeitung Verantwortlichen für die Erfüllung seiner Verpflichtungen aus der Vereinbarung mit dem Auftragsverarbeiter haftbar.

10. Audit

10.1. Um die Sicherheit der Dienste zu messen, kann der für die Verarbeitung Verantwortliche auf eigene Kosten und unter Einhaltung der in diesem Artikel festgelegten Bedingungen einen (1) Audit pro Jahr durchführen lassen, wobei die Dauer des Audits fünf (5) Arbeitstage nicht überschreiten darf. Der gesamte Zeitaufwand der Mitarbeiter*innen des Auftragsverarbeiters im Zusammenhang mit einem Audit wird dem Verantwortlichen in Rechnung gestellt.

10.2. Das Audit beschränkt sich auf die Überprüfung der Prozesse, der Organisation und der Tools, die direkt und ausschließlich mit der Umsetzung der Bestimmungen der DSGVO für die betreffenden Dienste zusammenhängen.

In keinem Fall darf das Audit darauf abzielen, (i) nicht-spezifische personenbezogene Daten oder Gesundheitsdaten, unabhängig davon, ob sie vertraulich sind oder nicht, oder Informationen, deren Offenlegung nach dem Ermessen des Auftragsverarbeiters die Sicherheit der Dienste oder anderer Nutzer*innen beeinträchtigen könnte, (ii) die Finanzdaten des Auftragsverarbeiters oder (iii) personenbezogene Daten von Mitarbeiter*innen des Auftragsverarbeiters oder seiner Unterauftragnehmer zu überwachen oder sich Zugang dazu zu verschaffen.

Es wird vereinbart, dass alle Aktivitäten, die im Rahmen eines Audits durchgeführt werden, nicht gleichzeitig oder anderweitig: (i) den Betrieb von Diensten, Systemen, Netzwerken, Software und/oder Hardware, die nicht für die ausschließliche Nutzung durch den für die Verarbeitung Verantwortlichen bestimmt sind, zu stören, zu verändern oder anderweitig zu beeinträchtigen; (ii) die Infrastruktur, in der die Dienste gehostet werden, zu beschädigen; (iii) Daten jeglicher Art zu beschädigen, zu löschen oder zu verändern; (iv) unbefugten Zugriff auf die vorgenannten Daten oder deren Wartung zu ermöglichen.

Penetrations- oder Intrusionstests der Plattform und/oder Applikation des Auftragsverarbeiters sind ohne vorherige schriftliche Zustimmung des Auftragsverarbeiters aus keinem Grund zulässig und von Audits ausgeschlossen.

Auf Verlangen des für die Verarbeitung Verantwortlichen übermittelt der Auftragsverarbeiter diesem die von der Zertifizierungsstelle ausgestellten Zertifizierungsauditberichte, die für eine solche Übermittlung bestimmt sind.

10.3. Der für die Verarbeitung Verantwortliche übermittelt dem Auftragsverarbeiter mindestens dreißig (30) Tage vor der Durchführung des Audits eine Vereinbarung, in der der genaue Umfang des Audits, die geplanten Daten und Zeiten sowie die damit verbundenen Bedingungen aufgeführt sind. Der/die Prüfer*in muss auch die für die Tests verwendeten Konten und Profile (Quell-IP-Adresse, Nutzer*in usw.), die angewandte Methodik sowie die zu prüfenden Beteiligten angeben.
Der Inhalt der Audit-Vereinbarung muss vom Auftragsverarbeiter im Voraus akzeptiert werden, bevor das Audit beginnt.

10.4. Die während der Prüfung erhaltenen Informationen sind vertrauliche Informationen und werden von dem für die Verarbeitung Verantwortlichen als solche behandelt. Diese Informationen dürfen nur an Personen weitergegeben werden, die strengen Vertraulichkeitsanforderungen unterliegen und ein direktes und erhebliches Interesse daran haben, sie zu kennen, und dürfen weder der Öffentlichkeit noch intern in irgendeiner Weise zugänglich gemacht werden.
Wenn der für die Verarbeitung Verantwortliche die Dienste eines/einer externen Prüfer*in in Anspruch nehmen möchte, muss er die vorherige schriftliche Zustimmung des für die Verarbeitung Verantwortlichen einholen, wobei der für die Verarbeitung Verantwortliche den/die Prüfer*in nur auf der Grundlage objektiver und fundierter Argumente ablehnen kann.

Der/die externe Prüfer*in darf unter keinen Umständen ein Mitbewerber des Auftragsverarbeiters sein und muss sich schriftlich verpflichten, die in diesem Artikel genannten Bedingungen einzuhalten.
Der für die Verarbeitung Verantwortliche verpflichtet sich, dem Auftragsverarbeiter den Auditbericht kostenlos zu übermitteln, und der Auftragsverarbeiter hat das Recht, seine Bemerkungen vorzubringen.
Der Auftragsverarbeiter verfügt über eine angemessene Frist nach Erhalt des Berichts, um festgestellte Mängel und/oder Nichtkonformitäten zu beheben.

11. Aufbewahrung und Vernichtung von persönlichen Daten

11.1. Zur Erinnerung: Der Siilo Messenger ist ein sicherer Kanal für den Austausch zwischen medizinischen Fachkräften. Er ist nicht dazu gedacht, Daten oder Dokumente im Zusammenhang mit der Überwachung von Patient*innen zu speichern. Die für die Überwachung Verantwortlichen sind dafür verantwortlich, die über Siilo Messenger ausgetauschten Daten und Dokumente regelmäßig zu sichern.

11.2. Der/die Verantwortliche hat die Möglichkeit, (i) alle nutzergenerierten Inhalte auf oder von seinen Geräten und seinem Konto zu löschen oder (ii) zu exportieren. Zur Klarstellung: Wenn der/die Nutzer*in sein/ihr Nutzerkonto oder die von ihm/ihr mit den Diensten geteilten nutzergenerierten Inhalte löscht, stehen die an andere Nutzer*innen der Apps gesendeten nutzergenerierten Inhalte unter der Kontrolle dieser Nutzer*innen und sind nicht Teil einer Löschung, wie oben beschrieben.

11.3. Bei der Nutzung von Siilo Messenger kann der/die Nutzer*in die nutzergenerierten Inhalte, die in seinem/ihrem Benutzerkonto verfügbar sind, abrufen, indem er/sie jede Unterhaltung manuell herunterlädt. Jede Konversation kann im PDF-Format heruntergeladen werden. Der/die Nutzer*in bestätigt, dass er/sie über alle erforderlichen Rechte und/oder Genehmigungen verfügt, um diese nutzergenerierten Inhalte abzurufen.

Der für die Verarbeitung Verantwortliche legt alle Aufbewahrungsfristen fest und stellt sicher, dass sie eingehalten werden, indem er die entsprechenden personenbezogenen Daten löscht.
Sofern der/die Nutzer*in nicht die Option „Konversation aufbewahren“ in den spezifischen Einstellungen jeder Konversation aktiviert hat, werden alle Nachrichten nach einer Frist von dreißig (30) Tagen gelöscht. Falls der/die Nutzer*in eine solche Option aktiviert hat, werden alle nutzergenerierten Inhalte, die sich auf die Konversation beziehen, für einen unbegrenzten Zeitraum aufbewahrt, d. h. bis der/die Nutzer*in sich entscheidet, sein/ihr Nutzerkonto zu löschen, oder bis diese Aufbewahrungsoption deaktiviert wird.

11.4. Bei Beendigung dieser Vereinbarung verpflichtet sich der Auftragsverarbeiter, nach Wahl des für die Verarbeitung Verantwortlichen

- die personenbezogenen Daten an den für die Verarbeitung Verantwortlichen zu übermitteln und anschließend die personenbezogenen Daten vorbehaltlich der gesetzlichen Aufbewahrungspflichten, denen der Auftragsverarbeiter unterliegt, innerhalb von fünfzehn (15) Tagen zu vernichten, ohne eine Kopie aufzubewahren; oder
- die personenbezogenen Daten vorbehaltlich der gesetzlichen Aufbewahrungspflichten, denen der Auftragsverarbeiter unterliegt, innerhalb von fünfzehn (15) Tagen zu vernichten, ohne eine Kopie aufzubewahren.

Der Auftragsverarbeiter stellt sicher, dass alle damit verbundenen, von seinen Unterauftragnehmern verarbeiteten personenbezogenen Daten vernichtet werden, es sei denn, eine weitere Speicherung der personenbezogenen Daten ist gesetzlich vorgeschrieben.

12. Übertragungen von personenbezogenen Daten

Personenbezogene Daten können an die Konzerngesellschaften des Auftragsverarbeiters, ihre Unterauftragnehmer oder Dienstleister in Ländern übermittelt werden, die ein angemessenes Schutzniveau oder angemessene Garantien für den Schutz der Privatsphäre und der Grundrechte und -freiheiten natürlicher Personen in Übereinstimmung mit den geltenden Rechtsvorschriften bieten.

Der Auftragsverarbeiter wird personenbezogene Daten nur dann an Unterauftragnehmer in Ländern außerhalb des Europäischen Wirtschaftsraums übermitteln, wenn eine solche Übermittlung für die Erbringung der bestellten Dienstleistungen erforderlich ist. Die Liste der Unterauftragnehmer ist in Anhang 3 verfügbar.

Wenn eine Übermittlung in ein Drittland außerhalb des Europäischen Wirtschaftsraums erfolgt, in dem die anwendbaren Datenschutzgesetze nicht als ein angemessenes Schutzniveau für personenbezogene Daten anerkannt wurden, stellt der Auftragsverarbeiter sicher, dass angemessene Maßnahmen in Übereinstimmung mit der DSGVO und den anwendbaren Datenschutzgesetzen und -vorschriften ergriffen werden, und insbesondere, falls erforderlich, dass Standardvertragsklauseln oder gleichwertige Ad-hoc-Klauseln in den zwischen dem Auftragsverarbeiter und dem Empfänger der personenbezogenen Daten geschlossenen Vertrag aufgenommen werden.

13. Sonstiges

13.1. Der Auftragsverarbeiter ist berechtigt, diese Vereinbarung zu ändern und zu ergänzen, um z. B. Entwicklungen in der Rechtsprechung, geänderten Vorschriften, von den Aufsichtsbehörden veröffentlichten Best Practices und dergleichen Rechnung zu tragen. Der Auftragsverarbeiter wird den Verantwortlichen über solche Änderungen und Ergänzungen informieren, bevor die neue Version in Kraft tritt. Sollte eine solche neue Version die Position des Auftraggebers wesentlich beeinträchtigen, ist der Auftraggeber berechtigt, die neue Version abzulehnen. In diesem Fall endet der Vertrag zwischen dem für die Verarbeitung Verantwortlichen und dem Auftragsverarbeiter.

13.2. Diese Vereinbarung mit dem Auftragsverarbeiter kann von keiner der Parteien ohne die schriftliche Zustimmung der anderen Partei übertragen werden. Im Falle einer Übertragung durch den Auftragsverarbeiter an eine Tochter- oder Muttergesellschaft des Auftragsverarbeiters ist jedoch keine Zustimmung erforderlich.

13.3. Diese Vereinbarung mit dem Auftragsverarbeiter unterliegt ausschließlich dem niederländischen Recht.

13.4. Die Parteien werden ihre Streitigkeiten im Zusammenhang mit dieser Vereinbarung ausschließlich vor dem zuständigen Gericht in Amsterdam austragen.

Anhang 1. Einzelheiten zur Verarbeitung personenbezogener Daten

Diese Vereinbarung gilt nicht für personenbezogene Daten von Nutzer*innen oder Kontaktpersonen von Nutzer*innen oder Kund*innen (z. B. Kontaktinformationen, E-Mail-Adressen, Telefonnummern, Bankkonten, Kreditinformationen usw.), die Siilo und seine Konzerngesellschaften als Verantwortliche gemäß DSGVO verarbeiten, wie in den online verfügbaren Datenschutzbestimmungen beschrieben.

Verantwortlicher: je nach Fall der Nutzer*in der App und der Dienste und/oder der Kunde, der sich bei Siilo Connect und/oder Prisma angemeldet hat.

Die Aktivitäten des für die Verarbeitung Verantwortlichen umfassen die Verarbeitung für die Aufgabe der Prävention, Diagnose und Pflege sowie die administrative Verwaltung seiner Gesundheitseinrichtung, seines Gesundheitszentrums oder seiner Privatpraxis.
Insbesondere umfasst die Verarbeitung zum Zwecke der Patientenbetreuung (i) Instant Messaging (Siilo Messenger und Siilo Webchat), (ii) ein privates Organisationsnetzwerk (Siilo Connect) und (iii) eine virtuelle kollaborative Beratung (Siilo Prisma).

Verarbeiter: Siilo

Im Folgenden werden die Aktivitäten beschrieben, die der Auftragsverarbeiter im Auftrag der für die Verarbeitung Verantwortlichen durchführt.

VERARBEITUNG Nr. 1: INSTANT MESSAGING (Siilo Messenger und Siilo Webchat)

VERARBEITUNGSVORGÄNGE:
Die Siilo-Dienste umfassen die Erhebung, die Aufzeichnung, die Organisation, die Speicherung, das Wiederauffinden, die Abfrage und die Nutzung, die Verwendung der Kommunikation, die Offenlegung durch Übermittlung, die Anonymisierung und die Löschung der unten aufgeführten personenbezogenen Daten.

ZWECKE DER VERARBEITUNG:
Der kostenlose Instant-Messaging-Dienst wurde entwickelt, um eine bessere Koordination der Pflege zu gewährleisten. Er ermöglicht Nutzer*innen die Kommunikation und den Versand von Textnachrichten, Videos, Fotos, Sprachnotizen und anderen Medien.
Siilo Messenger ermöglicht sowohl Einzel- als auch Gruppendiskussionen.

RECHTSGRUNDLAGE:
Es obliegt dem für die Verarbeitung Verantwortlichen, diese Rechtsgrundlage vor jeder Verarbeitung zu bestimmen.
Als Anhaltspunkt könnte ein berechtigtes Interesse die Rechtsgrundlage darstellen.
Es steht dem für die Verarbeitung Verantwortlichen frei, Siilo über eine andere Rechtsgrundlage zu informieren.
Für den Fall, dass der für die Verarbeitung Verantwortliche personenbezogene Daten oder Gesundheitsdaten von Patient*innen an medizinische Fachkräfte weitergibt, die nicht zum Behandlungsteam des/der betreffenden Patient*in gehören, muss er zunächst die Zustimmung des/der Betroffenen einholen.

BETROFFENE DATEN:
- Patient*innen
- Medizinische Fachkräfte oder Hilfskräfte mit einem Konto.

VERARBEITETE PERSONENBEZOGENE DATEN:
Grundsätzlich werden die folgenden Daten als relevant für die oben genannten Zwecke angesehen:
- Identifikationsdaten der medizinischen Fachkraft;
- Kontaktdaten der medizinischen Fachkraft;
- Krankengeschichte, Familiengeschichte und Allergien;
- Konsultationsdaten;
- Verschreibungsdaten;
- Biometrische und biologische Daten;
- Daten des Gesundheitsteams;
- Medizinische Bildgebung;
- Fotos, Videos;
- Sprachnotizen;
- Für Videos und Sprachanrufe: Video-/Sprachstream, der die Übertragung zwischen den medizinischen Fachkräften ermöglicht;
- Nutzungs- und Verbindungsprotokolle, die über die „geschäftlichen Aktionen“ der Nutzer*innen innerhalb der Siilo-Dienste berichten, sowie technische Protokolle, die

über die „Aktivität" der vom/von der Nutzer*in/Abonnent*in verwendeten Software- und Hardwarekomponenten berichten, sodass Siilo den Betrieb und den Zugang zu den angeforderten Funktionalitäten gewährleisten kann.

EMPFÄNGER:

- Medizinische Fachkräfte oder Betreuer*innen mit einem Nutzerkonto;

AUFBEWAHRUNG:
Sofern der/die Nutzer*in nicht in der spezifischen Einstellung jeder Konversation die Option „Aufrechterhaltung der Konversation" aktiviert hat, werden alle Nachrichten nach einer Frist von dreißig (30) Tagen gelöscht.

VERARBEITUNG Nr. 2: PRIVATES ORGANISATIONELLES NETZWERK (Siilo Connect)

VERARBEITUNGEN:

Die Siilo-Dienste umfassen die Erfassung, die Aufzeichnung, die Organisation, die Speicherung, das Wiederauffinden, die Abfrage und die Verwendung, die Nutzung der Kommunikation, die Offenlegung durch Übermittlung, die Anonymisierung und die Löschung der unten aufgeführten personenbezogenen Daten.

ZWECKE DER VERARBEITUNG:
Über Siilo Connect können die Mitarbeiter*innen/Mitglieder der Organisation einander leicht finden und kontaktieren und Informationen über den Bereich "News & Views" austauschen. Über das Siilo Connect Admin Tool können die Mitarbeiter*innen des Auftraggebers ihr Organisationsnetzwerk konfigurieren und personalisieren, Nachrichten versenden, Personen einladen, dem Netzwerk beizutreten und Konversationen für Nutzer*innen erstellen.

RECHTSGRUNDLAGE:
Es obliegt dem für die Verarbeitung Verantwortlichen, diese Rechtsgrundlage vor jeder Verarbeitung zu bestimmen.
Als Anhaltspunkt könnte ein berechtigtes Interesse die Rechtsgrundlage darstellen.
Es steht dem für die Verarbeitung Verantwortlichen frei, Siilo eine andere Rechtsgrundlage zu nennen.

BETROFFENE PERSONEN:

- Patient*innen
- Medizinische Fachkräfte oder Hilfskräfte mit einem Konto.

VERARBEITETE PERSONENBEZOGENE DATEN:
Grundsätzlich werden die folgenden Daten als relevant für die oben genannten Zwecke angesehen:

- Identifikationsdaten, berufliche Daten und Kontaktdaten der medizinischen Fachkräfte und Betreue*innen, die zur Organisation des für die Datenverarbeitung Verantwortlichen gehören;
- Identifikationsdaten der medizinischen Fachkräfte;
- Kontaktdaten der medizinischen Fachkräfte;
- Krankengeschichte, Familiengeschichte und Allergien;
- Konsultationsdaten;
- Verschreibungsdaten;
- Biometrische und biologische Daten;
- Daten des Gesundheitsteams;
- Medizinische Bildgebung;
- Foto;
- Nutzungs- und Verbindungsprotokolle, die über die „geschäftlichen Aktionen" der Nutzer*innen innerhalb der Siilo-Dienste berichten, sowie technische Protokolle, die über die „Aktivität" der vom/von der Nutzer*in/Abonnent*in verwendeten Software- und Hardwarekomponenten berichten, sodass Siilo den Betrieb und den Zugriff auf die angeforderten Funktionalitäten gewährleisten kann.

EMPFÄNGER:

- Medizinische Fachkräfte oder Betreuer*innen mit einem Nutzerkonto;

AUFBEWAHRUNG:
Sofern der für die Verarbeitung Verantwortliche nicht ausdrücklich eine andere Anweisung erteilt, wendet Siilo die von den zuständigen Aufsichtsbehörden oder der geltenden Gesetzgebung empfohlenen Aufbewahrungsfristen an.

VERARBEITUNG Nr. 3: VIRTUELLE KOLLABORATIVE BERATUNG (Siilo Prisma)

VERARBEITUNGSVORGÄNGE:
Die Siilo-Dienste umfassen die Erhebung, die Aufzeichnung, die Organisation, die Speicherung, das Wiederauffinden, die Abfrage und die Nutzung, die Kommunikationsnutzung, die Offenlegung durch Übermittlung, die Anonymisierung und die Löschung der unten aufgeführten personenbezogenen Daten.

ZWECKE DER VERARBEITUNG:
Über Siilo Prisma können Allgemeinmediziner*innen schnell, zugänglich und anonym eine virtuelle kollaborative Konsultation an ein multidisziplinäres Netzwerk von Spezialist*innen übermitteln, die solche Konsultationen überprüfen und beantworten; und sie haben Zugang zu einer durchsuchbaren Wissensdatenbank von zuvor beantworteten kollaborativen Konsultationen

RECHTSGRUNDLAGE:
Es obliegt dem für die Verarbeitung Verantwortlichen, diese Rechtsgrundlage vor jeder Verarbeitung zu bestimmen.
Als Anhaltspunkt könnte ein berechtigtes Interesse die Rechtsgrundlage darstellen.
Es steht dem für die Verarbeitung Verantwortlichen frei, Siilo eine andere Rechtsgrundlage zu nennen.

BETROFFENE DATEN:
- Patient*innen
- Medizinische Fachkräfte oder Hilfskräfte mit einem Konto.

VERARBEITETE PERSONENBEZOGENE DATEN:
Grundsätzlich werden die folgenden Daten als relevant für die oben genannten Zwecke angesehen:
- Identifikationsdaten der medizinischen Fachkraft;
- Kontaktdaten der medizinischen Fachkraft;
- Krankengeschichte, Familiengeschichte und Allergien;
- Konsultationsdaten;
- Verschreibungsdaten;
- Biometrische und biologische Daten;
- Daten des Gesundheitsteams;
- Medizinische Bildgebung;
- Foto;
- Nutzungs- und Verbindungsprotokolle, die über die „geschäftlichen Aktionen" der Nutzer*innen innerhalb der Siilo-Dienste berichten, sowie technische Protokolle, die über die „Aktivität" der vom/von der Nutzer*in/Abonnent*in verwendeten Software- und Hardwarekomponenten berichten, sodass Siilo den Betrieb und den Zugang zu den angeforderten Funktionalitäten gewährleisten kann.

EMPFÄNGER:
- Medizinische Fachkräfte oder Betreuer*innen mit einem Nutzerkonto;

AUFBEWAHRUNG:
Sofern der für die Verarbeitung Verantwortliche keine besonderen Anweisungen erteilt, wendet Siilo die von den zuständigen Aufsichtsbehörden oder den geltenden Rechtsvorschriften empfohlenen Aufbewahrungsfristen an.

Anhang 2. Organisatorische und sicherheitstechnische Maßnahmen

Organisatorische und administrative Bestimmungen und Kontrollen

Siilo hat ein Informationssicherheitsmanagementsystem (ISMS) eingeführt und ist nach ISO27001 und NEN7510 (niederländischer Standard für das Management der Informationssicherheit im Gesundheitswesen) zertifiziert.

Im Rahmen des ISMS hat Siilo verschiedene organisatorische und administrative Richtlinien und Kontrollen eingeführt, wie z. B. regelmäßige und standardmäßige Risikobewertungen, interne Audits, Richtlinien zur Informationssicherheit, eine Least-Privilege-Richtlinie, Mitarbeiterschulungen, ein Verfahren zum Management von (Sicherheits-)Vorfällen und ein Verfahren zur Meldung von Datenschutzverletzungen. Das Ziel des ISMS von Siilo ist es, die Organisation, die Mitarbeiter*innen und die Produkte weiter zu verbessern.
Jede Lösung, die Siilo implementiert, durchläuft eine Risikobewertung und eine Datenschutzfolgenabschätzung. Sie folgt einem strengen Prozess, der durch unsere ISMS-Bestimmungen abgesichert ist, die durch unsere Zertifikate ISO-27001 und NEN7510 nachgewiesen werden.

Siilo hat eine*n unabhängigen Sicherheitsbeauftragte*n und Datenschutzbeauftragte*n ernannt, die*der bei der niederländischen Datenschutzbehörde registriert ist.

Entwicklungsprozess

Im Entwicklungsprozess von Siilo kommen mehrere Strategien zum Einsatz, um sowohl die Qualität als auch die Sicherheit der Daten zu gewährleisten:
(1) Unit-Tests: Für jede Funktion entwickeln wir eine Reihe grundlegender Tests, die diese Funktion isoliert testen;
(2) Peer Code Review: Änderungen an der App werden von mindestens zwei Entwickler*innen überprüft, bevor sie in eine Beta-Version aufgenommen werden. Bei Funktionen, die sicherheits- oder datenschutzrelevante Aufgaben betreffen, werden diese neuen Codezeilen von einem/einer leitenden Entwickler*in außerhalb des Teams überprüft, und der/die leitende Entwickler*in setzt sich mit dem Sicherheitsbeauftragten und dem Datenschutzbeauftragten zusammen, bevor er/sie die neue(n) Funktion(en) für den Messenger freigibt.
(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-Tester*innen".

Dieser Ansatz wird verwendet, um gerätespezifische Funktionen sowie Funktionen zu testen, die sich erst herauskristallisieren, nachdem sie einer Vielzahl von Arbeitsabläufen ausgesetzt wurden.

Geringste Privilegien

Privilegien werden den Siilo-Mitarbeiter*innen auf einer strikten Need-to-have-Basis gewährt. Dies wird jährlich von einem/einer Sicherheitsbeauftragten überwacht und überprüft. Alle Siilo-Mitarbeiter*innen, die Zugriff auf Informationen außerhalb ihrer zugewiesenen Rolle benötigen, müssen die Anfrage zunächst mit unserer Standardvorlage protokollieren. Diese Anfragen werden protokolliert und vom Datenschutzbeauftragten autorisiert, wenn eine Anfrage vor ihrer Erfüllung als konform mit der Allgemeinen Datenschutzverordnung angesehen wird. Diese Anfragen werden außerdem einmal pro Quartal vom Siilo ISO-27001-Ausschuss überprüft, der sich aus dem Datenschutzbeauftragten und dem Chief Executive Officer und/oder dem Chief Financial Officer von Siilo zusammensetzt.

Technische Bestimmungen und Kontrollen

Nachrichtendaten – Daten im Transit

Um die Lösungen zur Minderung der Risiken für Daten im Transit zu verstehen, lesen Sie bitte unser Sicherheits-Whitepaper (https://www.siilo.com/resources/security-white-paper), in dem unser Security-by-Design-Ansatz, das Bedrohungsmodell und die kryptografischen Protokolle ausführlich beschrieben werden.
Zusammenfassend lässt sich sagen, dass Siilo eine Ende-zu-Ende-Verschlüsselung verwendet, die mit LibSodium, einer Abspaltung der Krypto-Bibliothek NaCl https://nacl.cr.yp.to/, implementiert wurde.

Das bedeutet, dass jede Nachricht zwischen Sender*in und Empfänger*in über ein öffentliches/privates Schlüsselpaar geschützt ist. Nur Sender*in und Empfänger*in sind in der Lage, die zwischen ihnen ausgetauschten Nachrichten zu entschlüsseln und zu lesen, und die Authentizität jeder Nachricht kann empirisch überprüft werden. Dritte, einschließlich des Unternehmens Siilo und seiner Mitarbeiter*innen, können sie niemals lesen.

Siilo verwendet Zertifikats-Pinning, um so genannte „Man-in-the-Middle"-Angriffe zu verhindern, bei denen Angreifer auf den Datenverkehr zwischen den Telefonen zugreifen und versuchen, die Kommunikationsleitungen 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 Sicherheitslücken, die sich aus den Problemen bei der Schlüsselverteilung im Zusammenhang mit der Infrastruktur der Zertifizierungsstellen im Internet ergeben.

Nachrichtendaten – Ruhende Daten auf dem Nutzer*in-Gerät

Für Daten, die sich auf dem Gerät (iPhone, iPad, Android) befinden, gelten die folgenden Sicherheitsvorkehrungen:

- Das gesamte „Schlüsselmaterial", auch bekannt als die vom Kryptographen verwendeten Codes, wird in der iOS KeyChain bzw. dem Android KeyStore gespeichert;
- Das gesamte „Schlüsselmaterial" wird mit einem „Hauptschlüssel" verschlüsselt, der von dem vom/von der Nutzer*in gewählten Pin-Code abgeleitet wird;
- Die gesamte Datenbank wird mit SQLiteCipher verschlüsselt. Alle Nachrichten, Nachrichten-Metadaten und Kontaktinformationen werden auf diese Weise gespeichert;
- Alle empfangenen Medien werden mit einem symmetrischen Einwegschlüssel verschlüsselt gespeichert. Der Zugriff auf diesen Schlüssel erfolgt über die oben erwähnte Datenbank;
- Ein Pincode-Mechanismus auf Applikationsebene verhindert den Zugriff durch Menschen, die physischen Zugang zum Gerät haben. Dies verhindert die meisten Formen von Social Engineering, wie z. B. die Bitte, sich das Telefon für einen kurzen Anruf auszuleihen, usw.
- Alle in der Siilo-App ausgetauschten Informationen werden nach 30 Tagen automatisch gelöscht. Nutzer*innen 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 vorgesehen, da wir glauben, dass dadurch ein Gefühl der Dringlichkeit erstellt wird, das beim/bei der Empfänger*in zu Screenshots und anderem unerwünschten Verhalten führt;
- Wenn ein/e Nutzer*in weiß, dass sein/ihr Gerät verloren gegangen ist, gestohlen wurde oder anderweitig gefährdet ist, kann er/sie sein/ihr Unternehmen benachrichtigen (dies ist eine Siilo Connect-Funktion) und ein Siilo Connect-Administrator kann die Siilo-Daten aus der Ferne von dem Gerät löschen. Nachrichtendaten – ruhende Daten auf Siilo-Servern Für ruhende Daten auf Siilo-Servern gelten die folgenden Sicherheitsvorkehrungen:
- Alle Siilo-Server befinden sich innerhalb der Europäischen Union und erfüllen die höchsten Sicherheits- und Compliance-Normen;
- Firewall-Regeln verhindern den Netzwerkzugriff auf die Datenbanken (MySQL und ElasticSearch) und beschränken sich auf ein Subnetz, das die Siilo-Server und ein VPN enthält, auf das eine begrenzte Anzahl von Siilo-Mitarbeiter*innen zugreifen kann;
- Die MySQL-Datenbank ist passwortgeschützt und nach dem Industriestandard AES-256 verschlüsselt und speichert Messaging-Daten, Messaging-Metadaten, Siilo Connect-Konfigurationsdaten und Nutzer*innen-Profil-Daten;
- 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 Applikation versendet werden und daher als sensibel gelten) werden gespeichert und mit dem symmetrischen Einwegschlüssel verschlüsselt. Dieser Schlüssel wird auf keinem Siilo-Server gespeichert, außer als Teil der verschlüsselten Nachrichtendaten, die in MySQL gespeichert sind. Die Schlüssel zur Entschlüsselung dieser Daten sind nur auf den Geräten des/der Absender*in und des/der Empfänger*in verfügbar. Speicherung personenbezogener Daten auf Siilo-Servern Die Nachrichtendaten werden auf Servern in Frankfurt (Deutschland) gespeichert. Zu Sicherungszwecken werden täglich automatische „Snapshots" erstellt, die nicht länger als 7 Tage gespeichert werden. Diese Snapshots werden im Ruhezustand verschlüsselt. Die Server-Infrastruktur von Siilo wird von Amazon, Inc. gehostet. Siilo hat sich bewusst für Amazon Web Services (AWS) entschieden, da dort die höchsten Sicherheits- und Verschlüsselungsstandards gelten und die Einhaltung der DSGVO durch die Zertifizierungen SOC Level I-II-III, ISO9001, ISO27001, ISO27017 und ISO27018 gewährleistet ist.

Nutzer*innen-Daten Nutzer*innen-Daten werden auf Servern in Dublin (Irland) gespeichert. Sie werden täglich gesichert und nicht länger als 30 Tage in einem vorkonfigurierten Bucket gespeichert, der im Ruhezustand verschlüsselt ist.

Telefonnummernabgleich auf Siilo

Siilo ermöglicht es dem/der Nutzer*in optional, andere Siilo-Kontakte durch einen Abgleich mit dem Adressbuch des Telefons zu finden. Wenn sich der/die Nutzer*in dafür entscheidet, werden die folgenden Informationen über eine verschlüsselte TLS-Verbindung auf den Server hochgeladen:
(1) Die ersten 64 Bits des SHA1-Hashes der E.164-normierten Form jeder Telefonnummer aus dem Adressbuch des Telefons
(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 im Adressbuch des Telefons gespeichert sind. Der Siilo-Server vergleicht dann die Liste der Hashes des/der Nutzer*in mit den bekannten Telefon-Hashes der aktuellen Siilo-Nutzer*innen. Der Server gleicht nur mit aktuellen Siilo-Nutzer*innen ab. Nach der Rückgabe der Übereinstimmungen an den mobilen Client verwirft der Server die übermittelten Hashes sofort.

Die Sicherheitsmaßnahmen werden im Siilo Security Whitepaper beschrieben, das hier verfügbar ist.

Anhang 3: Liste der Unterauftragnehmer

Um seine Dienstleistungen zu erbringen, setzt Siilo Dienstleister ein. Diese Dienstleister dürfen nur im Rahmen und zu den Zwecken der unten genannten Vorgänge Zugang zu den von Siilo erhobenen personenbezogenen Daten haben.
Siilo stellt sicher, dass jeder dieser Dienstleister angemessene technische und organisatorische Maßnahmen ergreift, um die Sicherheit und Vertraulichkeit der verarbeiteten Daten zu gewährleisten.

In Übereinstimmung mit der Allgemeinen Datenschutzverordnung und im Interesse der Transparenz teilt Siilo im Folgenden die Liste seiner Unterauftragnehmer mit.

Unternehmen	**Amazon Web Services**
Funktion	Unterauftragsverarbeiter
Allgemein	Die Server-Infrastruktur von Siilo wird von Amazon gespeichert.
Wo werden die Daten gespeichert?	Alle Aktivitäten im Zusammenhang mit Messaging finden in den Frankfurter Rechenzentren von Amazon statt. Für Dienste wie die E-Mail-Verifizierung (Amazon Simple Email Service) und die Protokollierung der Richtlinien für die Sicherheit von Website-Inhalten (Amazon Lambda) werden diese Dienste nur im irischen Rechenzentrum angeboten. Amazon Web Services verwendet Standardvertragsklauseln als Mechanismus für die Übermittlung von Daten außerhalb der Europäischen Union. Siilo nutzt auch die Dienste von Cloudfront, um die Sicherheit seiner Plattform zu gewährleisten und sich vor Angriffen wie CDS und DDos zu schützen. Die Server befinden sich weltweit, je nach Standort des/der Nutzer*in. Für weitere Informationen besuchen Sie bitte diese Webseite.
Welche Daten werden verarbeitet?	Verarbeitet von Amazon AWS: ● E-Mail-Adressen und E-Mail-Inhalte; ● Profildaten der Nutzer*innen; ● Verschlüsselte Nachrichtendaten; ● Metadaten der Nachricht (pseudonymisiert); ● Anfrage-Metadaten. Für Cloudfront-Dienste: ● IP-Adresse ● Technische Metadaten (Gerätetyp usw.).
Weitere Informationen	https://aws.amazon.com/compliance/gdpr-center/ https://aws.amazon.com/privacy/

Unternehmen	**Twilio**
Funktion	Unterauftragsverarbeiter
Allgemein	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-Funktionen bereitzustellen. Die Inhalte Ihrer Anrufe werden Ende-zu-Ende verschlüsselt (DTLS/SRTP). Wenn dies aufgrund von Firewalls erforderlich ist, ermittelt Twilio zunächst, welcher seiner Server am besten zwischen dem/der Anrufer*in und dem/der Empfänger*in positioniert ist.
Wo werden die Daten gespeichert?	https://www.twilio.com/docs/video/ip-address-whitelisting
Welche Daten werden verarbeitet?	● Telefonnummer ● SMS-Inhalte ● In-App-Metadaten für Sprach-/Videoanrufe
Weitere Informationen	https://www.twilio.com/legal/privacy

Unternehmen	**CM.com**
Funktion	Unterauftragsverarbeiter
Allgemein	Im Rahmen der Siilo-Registrierung werden Nutzer*innen gebeten, ihre Telefonnummer anzugeben. Diese Telefonnummer ist ein wesentlicher Bestandteil der Kontaktfindung für neue Nutzer*innen. Im Rahmen der Richtlinien von Siilo zur Überprüfung von Informationen verwenden wir CM als SMS-Anbieter, um dem/der Nutzer*in eine SMS mit einem Code zu senden, den er/sie eingibt, um zu bestätigen, dass er/sie tatsächlich Zugriff auf das mit dieser Nummer verbundene Gerät hat.
Wo werden die Daten gespeichert?	Das Rechenzentrum befindet sich in den Niederlanden.
Welche Daten werden verarbeitet?	● Telefonnummer ● SMS-Inhalte
Weitere Informationen	https://www.cm.com/about-cm/security-compliance/ https://legal.cmtelecom.com/en/cm-online-bv/privacy-policy

Unternehmen	**Firebase**

Funktion	Unterauftragsverarbeiter
Allgemein	Firebase wird von Siilo für Analytics und Crash Reporting in den mobilen iOS- und Android-Applikationen verwendet, um Push-Benachrichtigungen für die Android-Applikation zu versenden und um dynamische Links für Nicht-Nutzer*innen zu erstellen. Die Daten der Nutzer*innen werden anonymisiert gesendet. Nutzer*innen können sich bei der Registrierung der App gegen den Analysedienst entscheiden.
Wo werden die Daten gespeichert?	Google Rechenzentren: https://www.google.com/about/datacenters/locations/index.html Firebase verwendet Standardvertragsklauseln als Mechanismus für die Übermittlung von Daten außerhalb der Europäischen Union.
Welche Daten werden verarbeitet?	Keine persönlich identifizierbaren Daten Firebase Crash Reporting: ● Instanz-IDs ● Absturzspuren Crashlytics: ○ Installations-UUID ○ IP-Adressen Firebase Cloud Messaging ● Instanz-IDs Firebase Dynamische Links: ○ Gerätespezifikationen (iOS)
Weitere Informationen	https://firebase.google.com/support/privacy

Unternehmen	**ZenDesk**
Funktion	Unterauftragsverarbeiter
Allgemein	Nutzer*innen von Siilo haben mehrere Möglichkeiten, uns Feedback zu geben, z. B. über die Siilo Messenger-App, aber natürlich auch über das Siilo-Kontaktformular auf www.siilo.com oder über die folgende E-Mail-Adresse: info@siilo.com. Aufgrund des hohen Volumens dieser Interaktionen verfügt Siilo über ein Ticketingsystem, das eine Software namens ZenDesk verwendet, um die Kommunikation zwischen Mitarbeiter*innen und Nutzer*innen zu verfolgen.
Wo werden die Daten gespeichert?	Zendesk hat Rechenzentren in drei Hauptregionen - den Vereinigten Staaten, dem asiatisch-pazifischen Raum und der Europäischen Union. Service-Daten können in jeder Region gespeichert werden. ZenDesk verwendet Standardvertragsklauseln als Mechanismus für die Übermittlung von Daten außerhalb der Europäischen Union.
Welche Daten werden verarbeitet?	● Namen ● E-Mail-Adressen

	● Telefonnummer
Weitere Informationen	https://www.zendesk.nl/company/customers-partners/privacy-policy/ https://www.zendesk.com/blog/update-privacy-shield-invalidation-european-cour t-justice/

Unternehmen	**Salesforce**
Funktion	Unterauftragsverarbeiter
Allgemein	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 gespeichert?	Frankfurt, DE / Paris, FRA
Welche Daten werden verarbeitet?	● Namen ● E-Mail-Adressen ● Name des Unternehmens ● Eigenschaften und Bedürfnisse.
Weitere Informationen	https://www.salesforce.com/company/privacy/

Unternehmen	**Zapier**
Funktion	Unterauftragsverarbeiter
Allgemein	Informationen, die in das Kontaktformular auf der Website eingegeben werden, werden von Zapier verarbeitet und an verschiedene Endpunkte weitergeleitet.
Wo werden die Daten gespeichert?	Die Rechenzentren von Zapier befinden sich in den Vereinigten Staaten. Zapier verwendet Standardvertragsklauseln als Mechanismus für die Übertragung von Daten außerhalb der Europäischen Union.
Welche Daten werden verarbeitet?	● Namen ● E-Mail-Adressen ● Name des Unternehmens ● Eigenschaften und Bedürfnisse.
Weitere Informationen	https://zapier.com/privacy https://zapier.com/tos

Unternehmen	**Verifai**
Funktion	Unterauftragsverarbeiter
Allgemein	Siilo verwendet Verifai, um die Identität der Nutzer*innen von Siilo zu überprüfen und Ausweisdokumente zu authentifizieren. In der Siilo-App ermöglichen wir es Nutzer*innen, ihren Reisepass, Führerschein oder andere Identitätsnachweise zu fotografieren, um ihre Identität zu bestätigen.
Wo werden die Daten gespeichert?	Verifai hat seinen Sitz in den Niederlanden
Welche Daten werden verarbeitet?	Verifai speichert niemals persönliche Daten auf den Geräten seiner Kund*innen und sendet keine persönlichen Daten 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.
Weitere Informationen	https://www.verifai.com/en/privacy/ https://www.verifai.com/en/terms-use/

Unternehmen	**Looker**
Funktion	Unterauftragsverarbeiter
Allgemein	Siilo verwendet Looker als Plattform für Dashboarding und BI, die sich mit unserem Amazon Redshift Data Warehouse verbinden würde. Es werden zwar keine Daten dauerhaft bei Looker gespeichert, aber sie verarbeiten und visualisieren unsere Daten und benötigen dazu eine laufende Verbindung und einen temporären Cache aus unserem Redshift-Warehouse. Alle Daten sind pseudomisiert (nach Nutzer*innen-Id) und enthalten keine P(H)I (Name, E-Mail, IP-Adresse, aktuelle Nachrichten usw.).
Wo werden die Daten gespeichert?	Looker hat seinen Sitz in den Vereinigten Staaten, aber es werden keine persönlichen Daten in der Datenbank von Looker gespeichert.
Welche Daten werden verarbeitet?	Eindeutige (Geräte-)Kennungen, Geräteinformationen, Nutzungsdaten, Analysedaten, Lizenznachweise.
Weitere Informationen	https://looker.com/product/security https://looker.com/trust-center/privacy/policy

Unternehmen	**Mailchimp**
Funktion	Unterauftragsverarbeiter
Allgemein	Siilo verwendet Mailchimp, um E-Mail-Kampagnen an Nutzer*innen von Siilo zu senden, um sie über Produktaktualisierungen zu informieren, und an potenzielle Nutzer*innen von Siilo, wenn deren Organisation ihre E-Mail-Adresse zur Verfügung gestellt hat, um sie einzuladen.
Wo werden die Daten gespeichert?	Vereinigte Staaten von Amerika
Welche Daten werden verarbeitet?	Name, E-Mail, Standort
Weitere Informationen	https://mailchimp.com/en-au/legal/data-processing-addendum/ https://mailchimp.com/en-au/help/mailchimp-european-data-transfers/

Unternehmen	**Mailjet**
Funktion	Unterauftragsverarbeiter
Allgemein	Siilo verwendet Mailjet, um Transaktions-E-Mails an Nutzer*innen von Siilo, an potenzielle Nutzer*innen von Siilo, wenn Organisationen ihre E-Mail-Adresse angegeben haben, um sie einzuladen, und an Personen, die ihre Daten in das Prisma-Abonnementformular auf der Website eingeben, zu senden.
Wo werden die Daten gespeichert?	Deutschland und Belgien
Welche Daten werden verarbeitet?	Name, E-Mail, Land, Standort
Weitere Informationen	https://www.mailjet.com/legal/dpa/