Verwerkersovereenkomst

Deze Verwerkersovereenkomst is een overeenkomst tussen de Gebruiker/Klant van de Apps en/of Diensten (hierna: '**Verwerkingsverantwoordelijke**') en Siilo Holding B.V., een bedrijf naar Nederlands Recht, gevestigd aan de Keizersgracht 585, 1072 DR Amsterdam, Nederland (hierna: '**Verwerker**').

OVERWEGINGEN:

In het kader van hun contractuele relaties verbinden Verwerker en Verwerkingsverantwoordelijke (hierna samen: '**Partijen**') zich ertoe om te voldoen aan de toepasselijke wet- en regelgeving inzake gegevensbescherming, met inbegrip van, maar niet beperkt tot, de bepalingen van Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 die van toepassing is vanaf 25 mei 2018 (hierna de "AVG").

Het doel van deze Verwerkersovereenkomst is het definiëren van de voorwaarden waaronder de Verwerker zich ertoe verbindt de Persoonsgegevens te verwerken welke door de Verwerkingsverantwoordelijke zijn verstrekt om de Diensten uit te voeren.

OVEREENKOMST:

1. Definities

De definities die bij deze Verwerkersovereenkomst horen, zijn hier beschikbaar.

2. Inwerkingtreding en geldigheidsduur

Deze Overeenkomst is van kracht bij de uitvoering van het Contract waaraan het is gekoppeld en blijft van kracht voor de duur van de contractuele relatie tussen Verwerker en Verwerkingsverantwoordelijke.

3. Status van de Partijen

Verwerker is door Verwerkingsverantwoordelijke gemachtigd om namens Verwerkingsverantwoordelijke de Persoonsgegevens, waaronder Gezondheidsgegevens, die nodig zijn voor het leveren van de Diensten, te verwerken in strikte overeenstemming met de voorwaarden in deze Verwerkersovereenkomst.

Wanneer de Verwerkingsverantwoordelijke Persoonsgegevens of Gezondheidsgegevens van derden invoert in de App en/of Diensten of wanneer deze gebruik maakt van de Diensten en werkt met gegevens van collega 's of Patiënten, moet hij/zij voldoen aan de vereisten van toepasselijke wet- en regelgeving inzake gegevensbescherming.

3.1. Verplichtingen van de Verwerkingsverantwoordelijke

De Verwerkingsverantwoordelijke is als enige verantwoordelijk voor het bijhouden van een register van verwerkingsactiviteiten zoals vereist in artikel 30 paragraaf 1 (AVG) en, indien van toepassing, voor het vervullen van formaliteiten, inclusief, maar niet beperkt tot, kennisgevingen, registraties of voorafgaande kennisgevingen, voorafgaand aan de implementatie van de verwerking van Persoonsgegevens en Gezondheidsgegevens bij de bevoegde toezichthoudende autoriteit voor zover vereist door toepasselijke wet- en regelgeving inzake gegevensbescherming. Het is ook de verantwoordelijkheid van de Verwerkingsverantwoordelijke om de betrokkenen te informeren op een manier die in overeenstemming is met de toepasselijke wet- en regelgeving inzake gegevensbescherming, met inbegrip van, maar niet beperkt tot, de artikelen 12 – 14 van de AVG, indien Persoonsgegevens en Gezondheidsgegevens van Patiënten worden geïmporteerd in de App en/of Diensten.

De Verwerkingsverantwoordelijke is als enige verantwoordelijk voor de juistheid, betrouwbaarheid en relevantie van de Persoonsgegevens en Gezondheidsgegevens. In het bijzonder is de Gebruiker verantwoordelijk voor het gebruik van de App en/of Diensten en de informatie die hij/zij deponeert, opslaat, raadpleegt en verwijdert uit de App en/of Diensten. De Gebruiker stemt ermee in om Siilo, zijn vertegenwoordigers, werknemers en onderaannemers te vrijwaren en schadeloos te stellen voor alle claims, aansprakelijkheden, schade en uitgaven (inclusief juridische kosten en uitgaven) die worden opgelegd aan of worden opgelopen door Siilo, zijn agenten, werknemers en onderaannemers als gevolg van de schending van deze verplichting onder toepasselijke wet- en regelgeving inzake gegevensbescherming of onder deze Verwerkersovereenkomst.

Om misverstanden te voorkomen, Persoonsgegevens die zijn opgeslagen op de apparaten van Verwerkingsverantwoordelijke of een derde partij staan onder controle van Verwerkingsverantwoordelijke of een dergelijke derde partij en maken geen deel uit (of maken in voorkomend geval geen deel meer uit) van de Verwerking door Verwerker, zelfs niet in het geval dat dergelijke Persoonsgegevens zijn overgedragen via de App of zijn opgeslagen in de App.

De Verwerkingsverantwoordelijke verbindt zich ertoe:

- Het medisch geheim te respecteren en er voor te zorgen dat dit wordt gerespecteerd;

- Ervoor te zorgen dat Persoonsgegevens alleen worden gedeeld met andere gebruikers van de Apps en Diensten in overeenstemming met de toepasselijke wet- en regelgeving inzake gegevensbescherming;

- Een beleid van autorisatie, beheer van toegangsrechten en rollen en privileges te implementeren, om de vertrouwelijkheid van Persoonsgegevens en Gezondheidsgegevens te waarborgen in overeenstemming met de toepasselijke wet- en regelgeving inzake gegevensbescherming, evenals toepasselijke wet- en regelgeving met betrekking tot gezondheidszorg;

- Schriftelijk elke instructie met betrekking tot de Verwerking van Persoonsgegevens en Gezondheidsgegevens uitgevoerd door Siilo te documenteren;

- Toezicht te houden op de Verwerkingen die Siilo als Verwerker uitvoert;

- Een bevoorrechte gesprekspartner aan te wijzen die belast is met het vertegenwoordigen van de Verwerkingsverantwoordelijke;

- Een functionaris voor gegevensbescherming aan te wijzen indien vereist door artikel 37 (AVG), als de Verwerkingsverantwoordelijke dit nog niet heeft gedaan;

- Ervoor te zorgen dat vooraf en gedurende de hele verwerking, de toepasselijke wetgeving inzake gegevensbescherming wordt nageleefd.

3.2. Verplichtingen van Siilo

Siilo verbindt zich ertoe:

- Persoonsgegevens en Gezondheidsgegevens te verwerken volgens de doelen en kaders zoals gedefinieerd in deze Verwerkersovereenkomst, en te voldoen aan de technische standaarden en good practices die van toepassing zijn op Persoonsgegevens en Gezondheidsgegevens;

- Alleen te handelen op voorafgaande schriftelijke instructies van Verwerkingsverantwoordelijke en conform de doeleinden van de verwerking zoals beschreven in **Bijlage 1** bij deze Verwerkersovereenkomst, tenzij een op Verwerker toepasselijke wettelijke verplichting vereist dat Verwerker Persoonsgegevens verwerkt. In geval van onmogelijkheid of moeilijkheid om bepaalde instructies uit te voeren, zal Siilo Verwerkingsverantwoordelijke hiervan zo spoedig mogelijk op de hoogte stellen, voor zover toegestaan door toepasselijke wet- en regelgeving. Siilo kan een schriftelijk verzoek formuleren om af te wijken van de instructies. Siilo moet de voorafgaande en specifieke schriftelijke toestemming van de Verwerkingsverantwoordelijke verkrijgen alvorens tot deze afwijking wordt

overgegaan. Als een instructie van de Verwerkingsverantwoordelijke naar het oordeel van Verwerker inbreuk maakt op toepasselijke wet- of regelgeving inzake gegevensbescherming, zal Verwerker de Verwerkingsverantwoordelijke hiervan onmiddellijk op de hoogte stellen;

- Verwerker zal Verwerkingsverantwoordelijke helpen bij het waarborgen van de naleving door Verwerkingsverantwoordelijke van de verplichtingen uit hoofde van artikel 35 van de AVG (Gegevensbeschermings-effectbeoordeling) en artikel 36 van de AVG (Voorafgaande raadpleging), rekening houdend met de aard van de Verwerking en de informatie waarover Verwerker beschikt;

- Geen kopie te maken van de Persoonsgegevens en Gezondheidsgegevens zonder toestemming of instructie van Verwerkingsverantwoordelijke, deze niet aan derden mee te delen en niet te gebruiken voor andere doeleinden dan vermeld in de Verwerkersovereenkomst;

- Niet de Persoonsgegevens en Gezondheidsgegevens die haar door de Verwerkingsverantwoordelijke zijn toevertrouwd te exploiteren of te verwerken voor eigen rekening en/of voor rekening van derden, voor welk doel dan ook en op welke manier dan ook;

- Alle middelen in haar bezit te stellen met betrekking tot de contractuele bepalingen en de stand der techniek om de veiligheid en de vertrouwelijkheid van de Persoonsgegevens en Gezondheidsgegevens die haar zijn toevertrouwd te waarborgen en in het bijzonder te voorkomen dat ze worden vervormd, beschadigd of meegedeeld aan onbevoegde derden en meer in het algemeen om de juiste technische en organisatorische maatregelen te nemen om de Persoonsgegevens en Gezondheidsgegevens te beschermen tegen onopzettelijke of ongeoorloofde vernietiging, onopzettelijk verlies, wijziging, verspreiding of ongeoorloofde toegang, in het bijzonder wanneer de Verwerking doorgifte van gegevens in een netwerk inhoudt, evenals tegen elke vorm van ongeoorloofde verwerking;

- De Verwerkingsverantwoordelijke zo snel mogelijk op de hoogte te stellen van elke inbreuk op de beveiliging die direct of indirect van invloed is op Persoonsgegevens, Gezondheidsgegevens of Verwerkingen die hem/haar betreffen;

- Regelmatig backups van Persoonsgegevens te maken;

- Regelmatig penetratietests (of Pentests) uit te voeren;

- De apparatuur te onderhouden welke nodig is voor de goede werking van de Diensten;

- Te zorgen voor de vertrouwelijkheid van de verwerkte Persoonsgegevens en Gezondheidsgegevens;

- Rekening te houden met elke update, correctie, verwijdering of andere wijziging die door de Verwerkingsverantwoordelijke is meegedeeld met betrekking tot de Persoonsgegevens en Gezondheidsgegevens;

- Om de bewaartermijn van de Persoonsgegevens en Gezondheidsgegevens te respecteren welke van toepassing zijn op de doeleinden waarvoor ze zijn verzameld of verstrekt en deze te verwijderen/anonimiseren zodra deze doeleinden niet langer bestaan, behoudens wettelijke verplichtingen.

4. Inbreuk in verband met Persoonsgegevens

4.1. Verwerker zal Verwerkingsverantwoordelijke onverwijld informeren over elke vastgestelde Inbreuk in verband met Persoonsgegevens door middel van een elektronisch bericht of enig ander communicatiemiddel dat hem door Verwerkingsverantwoordelijke ter beschikking wordt gesteld.

4.2. Deze melding gaat op verzoek van Verwerkingsverantwoordelijke, voor zover mogelijk, vergezeld van alle informatie over de aard van de Inbreuk in verband met Persoonsgegevens, de mogelijke gevolgen van de Inbreuk in verband met Persoonsgegevens en/of de maatregelen die Verwerker heeft genomen en/of voornemens is te implementeren om de Inbreuk in verband met Persoonsgegevens aan te pakken.

4.3. Verwerker zal, voor zover mogelijk, Verwerkingsverantwoordelijke helpen bij het waarborgen van de naleving door Verwerkingsverantwoordelijke van de verplichtingen uit hoofde van artikel 33 van de AVG (Melding van een inbreuk in verband met persoonsgegevens aan de toezichthoudende autoriteit) en artikel 34 van de AVG (Mededeling van een inbreuk in verband met persoonsgegevens aan de betrokkene), rekening houdend met de aard van de Verwerking en de informatie waarover Verwerker beschikt. Het is aan de Verwerkingsverantwoordelijke om te bepalen of een Inbreuk in verband met Persoonsgegevens aan de toezichthoudende autoriteit moet worden gemeld of door de verwerkingsverantwoordelijke aan de Betrokkene(n) moet worden meegedeeld.

5. Informatie en rechten van Betrokkenen

Het is de verantwoordelijkheid van de Verwerkingsverantwoordelijke om de Betrokkenen te informeren (i) over de Verwerking die wordt uitgevoerd in het kader van de Diensten en om hun toestemming(en) te verkrijgen wanneer dit volgens de toepasselijke wetgeving noodzakelijk is; (ii) over de rechtsgrondslag voor de uitgevoerde Verwerking, de doeleinden van de Verwerking alsmede de lijst van onderaannemers die hun Persoonsgegevens waarschijnlijk zullen verwerken.

6. Beheer van gegevensverzoeken

Het is de verantwoordelijkheid van de Verwerkingsverantwoordelijke om gevolg te geven aan de verzoeken van de Betrokkenen inzake de rechten met betrekking tot hun Persoonsgegevens die zijn vastgelegd in de artikelen 15 – 22 (AVG). Voor zover mogelijk kan Siilo, in haar hoedanigheid van Verwerker en op verzoek van de Verwerkingsverantwoordelijke, de Verwerkingsverantwoordelijke helpen bij het nakomen van zijn/haar verplichting om aan dergelijke verzoeken van Betrokkenen te voldoen.

7. Vertrouwelijkheid

7.1. Verwerker is verplicht alle Persoonsgegevens die door Verwerkingsverantwoordelijke aan haar worden verstrekt vertrouwelijk te houden, behoudens in geval van een wettelijke verplichting die op Verwerker van toepassing is of een andersluidende instructie van Verwerkingsverantwoordelijke.

7.2. Op aanwijzing van bevoegde administratieve en gerechtelijke autoriteiten kan Siilo Persoonsgegevens, die zij verwerkt in naam en voor rekening van de Verwerkingsverantwoordelijke, meedelen om te voldoen aan haar wettelijke verplichtingen. In dat geval, tenzij de wet anders bepaalt, verplicht Siilo zich om de Verwerkingsverantwoordelijke op de hoogte te stellen van deze communicatie.

7.3. Verwerker draagt er zorg voor dat alle personen die in opdracht van Verwerker Persoonsgegevens verwerken, waaronder, maar niet beperkt tot, medewerkers van Verwerker en Onderaannemers van Verwerker, verplicht zijn de Persoonsgegevens vertrouwelijk te houden, onder voorbehoud van de inhoud van dit artikel.

8. Beveiliging en controle

8.1. Verwerker treft op grond van artikel 32 van de AVG (Beveiliging van de verwerking) passende technische en organisatorische maatregelen, welke in ieder geval die maatregelen omvatten die zijn beschreven in **Bijlage 2**.

8.2. De bovenstaande verplichtingen ontslaan de Verwerkingsverantwoordelijke niet van het implementeren van alle noodzakelijke technische en organisatorische beveiligingsmaatregelen voor de beveiliging en vertrouwelijkheid van alle informatie, inclusief Persoonsgegevens, aanwezig op de App en/of Diensten.

9. Subverwerkers

Verwerkingsverantwoordelijke verleent Verwerker een algemene schriftelijke machtiging tot het gebruik van de in Bijlage 3 genoemde Subverwerkers.

Op grond van deze algemene machtiging stemt Verwerker ermee in Verantwoordelijke vijftien (15) dagen van tevoren schriftelijk op de hoogte te stellen van eventuele wijzigingen met betrekking tot de toevoeging of vervanging van Onderaannemers, waardoor Verantwoordelijke de mogelijkheid krijgt om bezwaar te maken tegen dergelijke wijzigingen. Indien de Verwerkingsverantwoordelijke legitieme en redelijke gronden heeft om bezwaar te maken tegen de benoeming van een nieuwe Onderaannemer, moet hij dit onmiddellijk motiveren door een schriftelijke kennisgeving te sturen naar Verwerker op privacy@siilo.com, binnen vijftien (15) werkdagen, bij gebreke waarvan Verwerkingsverantwoordelijke geacht wordt deze benoeming te hebben goedgekeurd en aanvaard.

Na overleg en bij gebreke van overeenstemming tussen Verwerker en Verwerkingsverantwoordelijke kan Verwerkingsverantwoordelijke binnen vijftien (15) dagen na kennisgeving het gedeelte van de Overeenkomst waarop de betreffende update betrekking heeft, beëindigen.

Met betrekking tot elke Onderaannemer zal Verwerker (i) commercieel redelijke zorgvuldigheid betrachten bij de uitvoering van zijn evaluatie, benoeming en monitoring van de Verwerkingsactiviteiten van de Onderaannemers; (ii) in het contract tussen Verwerker en elke Onderaannemer clausules opnemen die een gelijkwaardig niveau van bescherming bieden voor de Persoonsgegevens en Gezondheidsgegevens die namens Verwerkingsverantwoordelijke worden verwerkt, zoals bepaald in deze Verwerkersovereenkomst.

Indien een Onderaannemer zijn verplichtingen met betrekking tot de bescherming van Persoonsgegevens niet nakomt, blijft Verwerker jegens Verwerkingsverantwoordelijke aansprakelijk voor de nakoming door Onderaannemers van zijn verplichtingen uit hoofde van de Verwerkersovereenkomst.

10. Audit

10.1. Om de veiligheid van de Diensten te meten, kan de Verwerkingsverantwoordelijke op eigen kosten beveiligingsaudits laten uitvoeren, met inachtneming van de in dit artikel uiteengezette voorwaarden en binnen de limiet van één (1) audit per jaar, waarvan de duur het maximum van vijf (5) werkdagen niet zal overschrijden. Alle tijd die medewerkers van Verwerker besteden aan een audit wordt gefactureerd aan Verwerkingsverantwoordelijke.

10.2. De controle is beperkt tot de verificatie van de processen, organisatie en hulpmiddelen die rechtstreeks en uitsluitend verband houden met de uitvoering van de bepalingen van de AVG voor de betrokken Diensten.

In geen geval zal de audit bedoeld zijn om toezicht te houden op of toegang te verkrijgen tot (i) niet-specifieke Persoonsgegevens of Gezondheidsgegevens, al dan niet vertrouwelijk, of informatie waarvan de openbaarmaking, naar goeddunken van Verwerker, de veiligheid van de Diensten of een van haar Gebruikers nadelig zou kunnen beïnvloeden; (ii) Financiële gegevens van Verwerker; of (iii) Persoonsgegevens met betrekking tot werknemers van Verwerker of haar Onderaannemers.

Er wordt overeengekomen dat alle activiteiten die in de loop van een audit worden ondernomen, niet, gelijktijdig of anderszins: (i) de werking van Diensten, systemen, netwerken, software en/of hardware verstoren, wijzigen of anderszins beïnvloeden, anders dan die welke zijn toegewezen voor exclusief gebruik door de Controller; (ii) de infrastructuur die de Services host beschadigen; (iii) wat voor type gegevens dan ook beschadigen, verwijderen of wijzigen; (iv) ongeoorloofde toegang tot of onderhoud van een van de voorgaande gegevens toestaan.

Penetratie- of inbraaktesten van het platform en/of de applicatie van de Verwerker zijn niet toegestaan, om welke reden dan ook, en dergelijke testen zijn uitgesloten van audits zonder voorafgaande schriftelijke toestemming van de Verwerker.

Op verzoek van Verwerkingsverantwoordelijke zal Verwerker met deze laatste de door de certificeringsinstantie afgegeven certificerings-auditrapporten, bestemd voor dergelijke communicatie, delen.

10.3. Verwerkingsverantwoordelijke zal Verwerker ten minste dertig (30) dagen voordat de audit wordt uitgevoerd een auditovereenkomst sturen waarin de exacte reikwijdte, de geplande data en tijden en de bijbehorende voorwaarden worden vermeld. De auditor moet ook alle accounts en profielen specificeren die voor de tests worden gebruikt (bron-IP-adres, user agent, enz.), alsmede de gebruikte methodologie en de te auditen actoren.

De inhoud van de auditovereenkomst moet vooraf door Verwerker worden geaccepteerd, voordat de audit begint.

10.4. De informatie die tijdens de audit wordt verkregen, is Vertrouwelijke Informatie en moet als zodanig door de verwerkingsverantwoordelijke worden behandeld. Deze informatie mag alleen worden meegedeeld aan personen die onderworpen zijn aan strikte geheimhoudingsvereisten en die een rechtstreeks en zwaarwegend belang hebben bij het hiervan op de hoogte zijn; het mag op geen enkele manier publiekelijk of intern worden vrijgegeven.

Indien Verwerkingsverantwoordelijke een beroep wenst te doen op de diensten van een externe auditor, moet Verwerkingsverantwoordelijke voorafgaande schriftelijke toestemming van Verwerker verkrijgen, met dien verstande dat Verwerker de auditor alleen mag weigeren op basis van objectieve en onderbouwde argumenten.

De externe auditor mag in geen geval een concurrent van Verwerker zijn en moet zich er schriftelijk toe verbinden de in dit artikel uiteengezette voorwaarden na te leven.

Verwerkingsverantwoordelijke verbindt zich ertoe het auditrapport kosteloos met Verwerker te delen, en Verwerker is gerechtigd haar opmerkingen kenbaar te maken.

De verwerker zal een redelijke termijn hebben vanaf de datum van ontvangst van het rapport om eventuele gevonden tekortkomingen en/of afwijkingen te corrigeren.

11. Bewaring en vernietiging van Persoonsgegevens

11.1. Ter herinnering, Siilo Messenger is een veilig uitwisselingskanaal tussen Zorgverleners en is niet bedoeld als een plek om gegevens of documenten met betrekking tot de monitoring van patiënten op te slaan. Verwerkingsverantwoordelijken zijn verantwoordelijk voor het regelmatig maken van backups van gegevens en documenten die worden uitgewisseld via Siilo Messenger.

11.2. Verwerkingsverantwoordelijke heeft de mogelijkheid om alle door de Gebruiker Gegenereerde Content van zijn apparaten en account (i) te verwijderen of (ii) te exporteren.

Voor alle duidelijkheid, als de Gebruiker zijn/haar Gebruikersaccount verwijdert of door de Gebruiker Gegenereerde Content, die wordt gedeeld bij gebruik van de Diensten, valt de door de Gebruiker Gegenereerde Content die naar andere Gebruikers van de apps wordt verzonden onder de controle van die Gebruikers en maakt geen deel uit van een dergelijke verwijdering zoals hierboven beschreven.

11.3. Met betrekking tot het gebruik van Siilo Messenger kan de Gebruiker de door de Gebruiker Gegenereerde Content die beschikbaar is op zijn/haar Gebruikersaccount ophalen door elk gesprek handmatig te downloaden. Elk gesprek kan worden gedownload in PDF-formaat. De Gebruiker erkent dat hij/zij alle benodigde rechten en/of machtigingen heeft om dergelijke door de Gebruiker Gegenereerde Content op te halen.

Verwerkingsverantwoordelijke stelt alle bewaartermijnen vast en zorgt ervoor dat deze in acht worden genomen door de respectieve Persoonsgegevens te verwijderen.

Tenzij de Gebruiker de optie heeft geactiveerd om "het gesprek te bewaren" in de specifieke instelling van elk gesprek, worden alle berichten na een periode van dertig (30) dagen verwijderd. In het geval dat een dergelijke optie door de gebruiker is geactiveerd, wordt alle door de Gebruiker Gegenereerde Content met betrekking tot het gesprek voor onbepaalde tijd bewaard, d.w.z. totdat de gebruiker besluit zijn/haar gebruikersaccount te verwijderen of totdat een dergelijke bewaaroptie is gedeactiveerd.

11.4. Aan het einde van deze Verwerkersovereenkomst verplicht Verwerker zich om, naar keuze van Verwerkingsverantwoordelijke,

- de Persoonsgegevens aan Verwerkingsverantwoordelijke te verstrekken en vervolgens de Persoonsgegevens te vernietigen zonder enige kopie te bewaren, behoudens

wettelijke bewaarverplichtingen waaraan Verwerker kan worden onderworpen, binnen vijftien (15) dagen of

- om de Persoonsgegevens binnen vijftien (15) dagen te vernietigen zonder enige kopie te bewaren, behoudens wettelijke bewaarverplichtingen waaraan Verwerker kan worden onderworpen.

De Verwerker zal ervoor zorgen dat alle bijbehorende Persoonsgegevens die door zijn Onderaannemers worden verwerkt, worden vernietigd, behalve als verdere opslag van Persoonsgegevens wettelijk vereist is.

12. Doorgifte van persoonsgegevens

Persoonsgegevens kunnen worden doorgegeven aan groepsmaatschappijen van Verwerker, hun onderaannemers of dienstverleners die gevestigd zijn in landen die een passend beschermingsniveau genieten of die passende waarborgen bieden met betrekking tot de bescherming van privacy en de fundamentele rechten en vrijheden van individuen, in overeenstemming met de toepasselijke wetgeving.

Verwerker zal alleen Persoonsgegevens doorgeven aan onderaannemers in landen buiten de Europese Economische Ruimte wanneer een dergelijke doorgifte vereist is voor de uitvoering van de bestelde Diensten. De lijst van Onderaannemers is beschikbaar in Bijlage 3.

Als een doorgifte plaatsvindt naar een derde land buiten de Europese Economische Ruimte waar de toepasselijke wetgeving inzake gegevensbescherming niet is erkend als een adequaat niveau van bescherming van Persoonsgegevens, zorgt Verwerker ervoor dat passende maatregelen worden getroffen in overeenstemming met de AVG en de toepasselijke wet- en regelgeving inzake gegevensbescherming, en in het bijzonder, waar nodig, dat standaard contractbepalingen of gelijkwaardige ad hoc-clausules worden opgenomen in het contract dat wordt gesloten tussen Verwerker en de ontvanger van de Persoonsgegevens.

13. Overig

13.1. Verwerker is gerechtigd deze Verwerkersovereenkomst te wijzigen en aan te passen om bijvoorbeeld ontwikkelingen in jurisprudentie, gewijzigde regelgeving, door de Toezichthouders gepubliceerde best practices en dergelijke weer te geven. Verwerker zal Verwerkingsverantwoordelijke op de hoogte stellen van dergelijke wijzigingen en aanpassingen voordat een dergelijke nieuwe versie van kracht wordt. In het geval dat een dergelijke nieuwe versie de positie van Verwerkingsverantwoordelijke wezenlijk negatief beïnvloedt, is

Verwerkingsverantwoordelijke gerechtigd de nieuwe versie te weigeren. In dat geval eindigt de Overeenkomst tussen Verwerkingsverantwoordelijke en Verwerker.

13.2. Deze Verwerkersovereenkomst is door geen van beide Partijen overdraagbaar zonder schriftelijke toestemming van de andere Partij. Bij overdracht door Verwerker aan een dochteronderneming of moedermaatschappij van Verwerker is echter geen toestemming vereist.

13.3. Op deze overeenkomst is uitsluitend Nederlands Recht van toepassing.

13.4. Partijen zullen hun geschillen in verband met deze Verwerkersovereenkomst uitsluitend voorleggen aan de bevoegde rechtbank te Amsterdam.

Bijlage 1. Details over de Verwerking van Persoonsgegevens

Deze Verwerkersovereenkomst is niet van toepassing op Persoonsgegevens van Gebruiker/Klant of contactpersonen van Gebruiker/Klant (bijv. contactgegevens, e-mailadressen, telefoonnummers, bankrekeningen, kredietinformatie enz.) die Siilo en haar groepsmaatschappijen verwerken als verwerkingsverantwoordelijke onder de AVG zoals beschreven in het Privacybeleid dat online beschikbaar is.

Verwerkingsverantwoordelijke: wat van toepassing is, de Gebruiker van de App en de Diensten, en/of de Klant die zich heeft geabonneerd op Siilo Connect en/of Prisma.

De activiteiten van de Verwerkingsverantwoordelijke omvatten Verwerking voor de uitoefening van preventie-, diagnose- en zorgactiviteiten, evenals het administratief beheer van zijn gezondheidsinstelling, gezondheidscentrum of privépraktijk.

Voor patiëntenzorg omvat de Verwerking met name (i) instant messaging (Siilo Messenger en Siilo Webchat), (ii) een privaat organisatienetwerk (Siilo Connect) en (iii) virtueel samenwerkingsconsult (Siilo Prisma).

Verwerker: Siilo

De werkzaamheden die Verwerker in opdracht van Verwerkingsverantwoordelijken uitvoert, worden hieronder beschreven.

VERWERKING N°1: INSTANT MESSAGING (Siilo Messenger en Siilo Webchat)

VERWERKINGSACTIVITEITEN

Siilo Diensten omvat het verzamelen, vastleggen, organiseren, opslaan, opvragen, raadplegen en gebruiken, communicatiegebruik, openbaarmaking door verzending, anonimisering en verwijdering van de hieronder vermelde Persoonsgegevens.

DOELEINDEN VAN DE VERWERKING

De gratis instant messaging-dienst is ontworpen om een betere zorgcoördinatie te garanderen, waardoor Gebruikers kunnen communiceren en tekstberichten, video's, foto's, gesproken notities en andere media kunnen verzenden.

Siilo Messenger maakt één-op-één discussies mogelijk, evenals groepsdiscussies.

RECHTSGROND

Het is aan de Verwerkingsverantwoordelijke om deze rechtsgrond te bepalen voordat een Verwerking plaatsvindt.

Ter indicatie, gerechtvaardigd belang zou de rechtsgrond kunnen vormen.

Het staat de Verwerkingsverantwoordelijke vrij om Siilo op de hoogte te stellen van elke andere rechtsgrond.

In het geval dat de Verwerkingsverantwoordelijke Persoons- of Gezondheidsgegevens van de patiënt meedeelt aan een Zorgverlener die geen deel uitmaakt van het zorgteam van de betreffende patiënt, moet hij eerst de toestemming van deze patiënt vragen.

BETROKKENEN

- Patiënten
- Zorgverleners of assistenten met een Account.

VERWERKTE PERSOONSGEGEVENS:

In principe worden de volgende gegevens relevant geacht voor de hierboven genoemde doeleinden:

- Identificatiegegevens Zorgverlener;
- Contactgegevens Zorgverlener;
- Medische voorgeschiedenis, familiegeschiedenis en allergieën;
- Consultgegevens;
- Receptgegevens;
- Biometrische en biologische gegevens;
- Gegevens van het Zorgteam;
- Beeldvormend medisch onderzoek;

- Foto, video's;
- Spraaknotities;
- Voor video- en spraakoproepen: video/spraak-stream om de overdracht tussen de Zorgverleners mogelijk te maken;
- Gebruiks- en verbindingslogboeken die rapporteren over de "zakelijke acties" van Gebruikers binnen de Siilo Diensten, evenals technische logboeken die rapporteren over de "activiteit" van de software- en hardwarecomponenten die door de Gebruiker/Abonnee worden gebruikt, zodat Siilo de werking en toegang tot de gevraagde functionaliteiten kan garanderen.

ONTVANGERS

- Zorgverleners of assistenten met een Gebruikersaccount;

BEWARING

Tenzij de Gebruiker de optie heeft geactiveerd om "het gesprek te bewaren" in de specifieke instelling van elk gesprek, worden alle berichten na een periode van dertig (30) dagen verwijderd.

VERWERKING N°2: PRIVAAT ORGANISATIENETWERK (Siilo Connect)

VERWERKINGSACTIVITEITEN

Siilo Diensten omvat het verzamelen, vastleggen, organiseren, opslaan, opvragen, raadplegen en het gebruiken, communicatiegebruik, openbaarmaking door verzending, anonimisering en verwijdering van de hieronder vermelde Persoonsgegevens.

DOELEINDEN VAN DE VERWERKING

Via Siilo Connect kunnen medewerkers/leden van de organisatie elkaar eenvoudig vinden en contacteren en informatie delen via de ruimte “News & Views”. Via de admin tool van Siilo Connect kan het personeel van de Klant zijn organisatienetwerk configureren en personaliseren, berichten uitzenden, mensen uitnodigen om lid te worden van het netwerk en vooraf gesprekken maken voor Gebruikers.

RECHTSGROND

Het is aan de Verwerkingsverantwoordelijke om deze rechtsgrond te bepalen voordat een Verwerking plaatsvindt.

Ter indicatie, gerechtvaardigd belang zou de rechtsgrond kunnen vormen.

Het staat de Verwerkingsverantwoordelijke vrij om Siilo op de hoogte te stellen van elke andere rechtsgrond.

BETROKKENEN

- Patiënten
- Zorgverleners of assistenten met een Account.

VERWERKTE PERSOONSGEGEVENS

In principe worden de volgende gegevens relevant geacht voor de hierboven genoemde doeleinden:

- Identificatiegegevens, professionele gegevens en contactgegevens van de Zorgverleners en assistenten die deel uitmaken van de organisatie van de Verwerkingsverantwoordelijke;
- Identificatiegegevens Zorgverlener;
- Contactgegevens Zorgverlener;
- Medische voorgeschiedenis, familiegeschiedenis en allergieën;
- Consultgegevens;
- Receptgegevens;
- Biometrische en biologische gegevens;
- Gegevens van het Zorgteam;
- Beeldvormend medisch onderzoek;
- Foto;

- Gebruiks- en verbindingslogboeken die rapporteren over de "zakelijke acties" van Gebruikers binnen de Siilo Diensten, evenals technische logboeken die rapporteren over de "activiteit" van de software- en hardwarecomponenten die door de Gebruiker/Abonnee worden gebruikt, zodat Siilo de werking en toegang tot de gevraagde functionaliteiten kan garanderen.

ONTVANGERS

- Zorgverleners of assistenten met een Gebruikersaccount;

BEWARING

Tenzij de Verwerkingsverantwoordelijke uitdrukkelijk anders heeft bepaald, past Siilo de bewaartermijnen toe zoals aanbevolen door de bevoegde toezichthoudende autoriteiten of de toepasselijke wetgeving.

VERWERKING NR. 3: VIRTUEEL SAMENWERKINGSCONSULT (Siilo Prisma)

VERWERKINGSACTIVITEITEN

Siilo Diensten omvat het verzamelen, vastleggen, organiseren, opslaan, opvragen, raadplegen en het gebruiken, communicatiegebruik, openbaarmaking door verzending, anonimisering en verwijdering van de hieronder vermelde Persoonsgegevens.

DOELEINDEN VAN DE VERWERKING

Huisartsen kunnen via Siilo Prisma snel, laagdrempelig en anoniem een virtueel samenwerkingsconsult indienen bij een multidisciplinair netwerk van specialisten, die dit overleg beoordelen en erop reageren; en ze hebben toegang tot een doorzoekbare kennisbank van eerder beantwoorde samenwerkingsconsulten.

RECHTSGROND

Het is aan de Verwerkingsverantwoordelijke om deze rechtsgrond te bepalen voordat een Verwerking plaatsvindt.

Ter indicatie, gerechtvaardigd belang zou de rechtsgrond kunnen vormen.

Het staat de Verwerkingsverantwoordelijke vrij om Siilo op de hoogte te stellen van elke andere rechtsgrond.

BETROKKENEN

- Patiënten
- Zorgverleners of assistenten met een Account.

VERWERKTE PERSOONSGEGEVENS

In principe worden de volgende gegevens relevant geacht voor de hierboven genoemde doeleinden:

- Identificatiegegevens Zorgverlener;
- Contactgegevens Zorgverlener;
- Medische voorgeschiedenis, familiegeschiedenis en allergieën;
- Consultgegevens;
- Receptgegevens;
- Biometrische en biologische gegevens;
- Gegevens van het Zorgteam;
- Beeldvormend medisch onderzoek;
- Foto;
- Gebruiks- en verbindingslogboeken die rapporteren over de "zakelijke acties" van Gebruikers binnen de Siilo Diensten, evenals technische logboeken die rapporteren over de "activiteit" van de software- en hardwarecomponenten die door de Gebruiker/Abonnee worden gebruikt, zodat Siilo de werking en toegang tot de gevraagde functionaliteiten kan garanderen.

ONTVANGERS

- Zorgverleners of assistenten met een Gebruikersaccount;

BEWARING

Tenzij de Verwerkingsverantwoordelijke uitdrukkelijk anders heeft bepaald, past Siilo de bewaartermijnen toe zoals aanbevolen door de bevoegde toezichthoudende autoriteiten of de toepasselijke wetgeving.

Bijlage 2. Organisatorische- en beveiligingsmaatregelen

Organisatorische en administratieve beleidsregels en controles

Siilo heeft een beheerssysteem voor informatiebeveiliging (ISMS) geïmplementeerd en Siilo is gecertificeerd volgens ISO27001 en NEN7510 (Nederlandse norm voor het beheer van informatiebeveiliging in de gezondheidszorg).

Als onderdeel van het ISMS heeft Siilo verschillende organisatorische en administratieve beleidsmaatregelen en controles geïmplementeerd, zoals periodieke en standaard risicobeoordelingen, interne audits, een informatiebeveiligingsbeleid, een "least privilege policy", training van personeel, een (beveiligings-) incidentmanagementprocedure en een meldprocedure voor gegevensinbreuken. Het doel van Siilo 's ISMS is om verdere verbetering van de organisatie, het personeel en de producten mogelijk te maken.

Elke oplossing die Siilo implementeert, doorloopt een risicobeoordeling en een assessment van de gevolgen voor de gegevensbescherming. Het volgt een strikt proces dat wordt gewaarborgd door ons ISMS-beleid, aangetoond door onze ISO-27001- en NEN7510-certificaten.

Siilo heeft een onafhankelijke Functionaris Beveiliging en Functionaris Gegevensbescherming aangesteld die zijn aangemeld bij de Autoriteit Persoonsgegevens in Nederland.

Ontwikkelingsproces

Siilo's ontwikkelingsproces maakt gebruik van verschillende strategieën om zowel de kwaliteit als de veiligheid van gegevens te waarborgen:

(1) Unittests: voor elk functie ontwikkelen we een reeks basistests die die functie losstaand uitvoeren;

(2) Peer code review: wijzigingen in de app worden beoordeeld door ten minste twee ontwikkelaars voordat ze worden geaccepteerd in een betaversie. Voor functies die van invloed zijn op beveiligings- of privacy gerelateerde taken, worden nieuwe regels softwarecode beoordeeld door een senior ontwikkelaar van buiten het team en de senior ontwikkelaar communiceert met de Functionaris Beveiliging en Functionaris Privacy voor het vrijgeven van de nieuwe functie(s) aan de messenger.

(3) Handmatig testen en beperkte openbare beta: voorafgaand aan de release worden functies intern vrijgegeven voor handmatig testen en worden ze vaak ook vrijgegeven aan een selecte pool van 'vriendelijke betatesters'.

Deze aanpak wordt gebruikt om apparaat specifieke functies te screenen, evenals alle functies die mogelijk pas optreden nadat ze zijn blootgesteld aan een diverse reeks workflows.

Least privilege

Privileges worden verstrekt aan personeel van Siilo op een strikte need-to-have basis. Dit wordt jaarlijks gemonitord en gecontroleerd door een Functionaris Beveiliging. Elke Siilo-medewerker die toegang nodig heeft tot informatie buiten zijn toegewezen rol, moet de aanvraag eerst registreren met ons standaardsjabloon. Deze aanvragen worden, alvorens te worden uitgevoerd, geregistreerd en geautoriseerd door de Functionaris Gegevensbescherming indien een aanvraag wordt geacht in overeenstemming te zijn met de Algemene Verordening Gegevensbescherming. Deze aanvragen worden ook eenmaal per kwartaal beoordeeld door het Siilo ISO-27001-comité, bestaande uit de Functionaris Gegevensbescherming en Siilo's Chief Executive Officer en/of de Chief Financial Officer.

Technische beleidsregels en controles

Berichtgegevens – gegevens in transit

Om inzicht te krijgen in de oplossingen om de risico's voor gegevens tijdens het transport te beperken, kunt u onze whitepaper lezen over beveiliging (https://www.siilo.com/resources/security-white-paper) waarin onze security-by-design-aanpak, het bedreigingsmodel en cryptografische protocollen in detail worden beschreven.

In het kort betekent dit, dat Siilo gebruik maakt van end-to-end encryptie geïmplementeerd met LibSodium, een afsplitsing van de NaCl cryptobibliotheek https://nacl.cr.yp.to/.

Dit betekent dat elk bericht tussen verzender en ontvanger wordt beveiligd via een openbaar/privé sleutelpaar. Alleen afzender en ontvanger kunnen de berichten die ze uitwisselen decoderen en lezen, en de authenticiteit van elk bericht kan empirisch worden geverifieerd. Derden, waaronder het bedrijf Siilo en haar werknemers zijn nooit in staat om ze te lezen.

Siilo gebruikt "certificate pinning" om zogenaamde "man-in-the-middle" -aanvallen te voorkomen, een proces waarbij aanvallers toegang krijgen tot het verkeer tussen de telefoons en proberen in te breken en de communicatielijnen "af te luisteren" om de berichten te lezen. Voor standaard TLS v1.2-communicatie is een geldig SSL-certificaat vereist dat is uitgegeven door een vertrouwde certificeringsinstantie die door het apparaat wordt herkend. Certificate pinning gaat verder en schrijft voor dat deze certificaten alleen mogen worden uitgegeven vanuit een vertrouwensketen die zin "roots" heeft bij een gespecificeerde uitgever. Hiermee wordt een lange reeks van kwetsbaarheden die het gevolg zijn van problemen met de distributie van de sleutels in verband met de infrastructuur van de certificeringsinstantie van het internet aangepakt.

Berichtgegevens – gegevens in rust op het apparaat van de gebruiker

Voor gegevens in rust op het apparaat (iPhone, iPad, Android) zijn de volgende voorzorgsmaatregelen getroffen:

- Al het "sleutel-materiaal", ook bekend als de codes die door de cryptografie worden gebruikt, worden opgeslagen in de iOS-sleutelhanger of de Android KeyStore, naargelang het geval;
- Al het "sleutel-materiaal" wordt versleuteld met een "hoofdsleutel" die is afgeleid van de door de gebruiker gekozen pincode;
- De gehele database is versleuteld met SQLiteCipher. Alle berichten, metagegevens van berichten en contactgegevens worden op deze manier opgeslagen;
- Alle ontvangen media worden versleuteld opgeslagen door de symmetrische coderingssleutel voor eenmalig gebruik. Deze sleutel is toegankelijk via de hierboven genoemde database;
- Een pincodemechanisme op toepassingsniveau voorkomt toegang door mensen die fysieke toegang hebben tot het apparaat. Dit behandelt de meeste vormen van persoonlijke social engineering, zoals het vragen om de telefoon te lenen voor een snel gesprek, enz.

- Alle uitgewisselde informatie in de Siilo-app wordt na 30 dagen automatisch verwijderd. Gebruikers kunnen zelf beslissen om individuele berichten op ad-hoc basis te verwijderen als ze 30 dagen te lang vinden. We hebben bewust geen afteltimers en berichtenlevensduur van seconden/uren opgenomen, omdat we geloven dat dit een gevoel van urgentie zal creëren, wat resulteert in screenshots en ander ongewenst gedrag aan de ontvangende kant;

- Wanneer een gebruiker weet dat zijn/haar apparaat verloren, gestolen of anderszins gecompromitteerd is, kan hij/zij zijn organisatie waarschuwen (dit is een Siilo Connect-functie) en een Siilo Connect-beheerder kan de Siilo-gegevens op afstand van het apparaat wissen.

- Berichtgegevens – gegevens in rust op Siilo-servers; voor gegevens in rust op Siilo-servers zijn de volgende beveiligingsmaatregelen getroffen:

- Alle Siilo servers bevinden zich binnen de Europese Unie met de hoogste beveiligings- en compliance normen;

- Firewallregels verhinderen netwerktoegang tot de databases (MySQL en ElasticSearch) en is beperkt tot een subnet met Siilo's servers en een VPN, waartoe een beperkte subset van Siilo-medewerkers toegang heeft;

- De MySQL-database is met een wachtwoord beveiligd en gecodeerd volgens industriestandaard AES-256 en slaat berichtgegevens, bericht-metagegevens, Siilo Connect-configuratiegegevens en gebruikersprofielgegevens op;

- ElasticSearch versleutelt specifieke velden zoals e-mail en telefoonnummers om matching mogelijk te maken. Andere profielvelden die in de app als "openbaar" worden weergegeven aan Siilo-leden, worden opgeslagen in platte tekst;

- Alle media (verzonden via de applicatie en dus als gevoelig beschouwd) worden opgeslagen en versleuteld door de symmetrische encryptiesleutel voor eenmalig gebruik. Die sleutel wordt niet opgeslagen op enige Siilo-server, behalve als onderdeel van de gecodeerde berichtgegevens die zijn opgeslagen in MySQL. De sleutels om die gegevens te decoderen zijn alleen beschikbaar op de apparaten van de afzender en ontvanger.

Opslag van persoonsgegevens op Siilo servers. Berichtgegevens worden opgeslagen op servers in Frankfurt (Duitsland) en voor backup-doeleinden worden dagelijks geautomatiseerde 'snapshots' gemaakt die niet langer dan 7 dagen worden bewaard.

Deze snapshots worden in rust versleuteld. Siilo's serverinfrastructuur wordt gehost door Amazon, Inc. Siilo heeft doelbewust gekozen voor Amazon Web Services (AWS) omdat ze de hoogste beveiligings- en encryptienormen hanteren en ervoor zorgen hun SOC-

niveau I-II-III, ISO9001, ISO27001, ISO27017 en ISO27018-certificeringen voldoen aan de AVG.

Gebruikersgegevens worden opgeslagen op servers in Dublin (Ierland) en worden dagelijks gebackupt en niet langer dan 30 dagen opgeslagen in een vooraf geconfigureerde "bucket" die in rust wordt gecodeerd.

Telefoonnummer-matching op Siilo

Siilo laat de gebruiker optioneel andere Siilo-contacten ontdekken door te vergelijken met het adresboek van de telefoon. Als de gebruiker ervoor kiest om dit te doen, wordt de volgende informatie geüpload via een versleutelde TLS-verbinding met de server:

(1) Eerste 64 bits van de SHA1-hash van de E.164 genormaliseerde vorm van elk telefoonnummer in het adresboek van de telefoon

(2) Sleutel: EEDAAC207FC6BA08727C

(3) Alleen de telefoonnummers worden gehasht en vergeleken. Siilo leest geen geassocieerde namen, e-mailadressen en andere informatie die in het adresboek van de telefoon staan. De Siilo-server vergelijkt vervolgens de lijst met hashes van de gebruiker met de bekende telefoonhashes van huidige Siilo-gebruikers. De server zal alleen matchen met huidige Siilo-gebruikers, en na het doorgeven van de matches aan de mobiele client, gooit de server onmiddellijk de ingediende hashes weg.

Beveiligingsmaatregelen worden beschreven in de hier beschikbare Siilo Security Whitepaper.

Bijlage 3: Lijst van Onderaannemers

Voor het leveren van haar diensten maakt Siilo gebruik van dienstverleners. Deze dienstverleners hebben alleen toegang tot persoonsgegevens die door Siilo zijn verzameld in het kader van en voor de doeleinden van de hieronder vermelde activiteiten.

Siilo zorgt ervoor dat elk van deze dienstverleners passende technische en organisatorische maatregelen treft om de veiligheid en vertrouwelijkheid van de verwerkte gegevens te waarborgen.

In overeenstemming met de Algemene Verordening Gegevensbescherming en in het belang van transparantie communiceert Siilo hieronder de lijst van haar onderaannemers.

Bedrijf	**Amazon Web Services**
Rol	Subverwerker
Algemeen	Siilo's serverinfrastructuur wordt gehost door Amazon.
Waar worden de gegevens gehost?	Alle berichten gerelateerde activiteiten bevinden zich in de datacenters van Amazon in Frankfurt. Voor services zoals de e-mailverificatie (Amazon Simple Email Service) en het registreren van het beveiligingsbeleid voor website-content (Amazon Lambda), worden deze services alleen aangeboden in het datacenter in Ierland. Amazon Web Services gebruikt Standaardcontractbepalingen als een mechanisme voor het doorgeven van gegevens buiten de Europese Unie. Siilo gebruikt ook Cloudfront-services om de veiligheid van zijn platform te garanderen en zichzelf te beschermen tegen aanvallen zoals CDS EN DDoS. Servers bevinden zich wereldwijd, afhankelijk van de locatie van de eindgebruiker. Voor meer informatie kunt u deze pagina raadplegen.

Welke gegevens worden verwerkt?	Verwerkt door Amazon AWS: ● E-mailadressen en e-mailinhoud; ● Gebruikersprofielgegevens; ● Gecodeerde berichtgegevens; ● Berichtmetagegevens (gepseudonimiseerd); ● Verzoek metagegevens. Voor Cloudfront-services: ● IP-adres ● Technische metagegevens (apparaattype enz.).
Meer informatie	https://aws.amazon.com/compliance/gdpr-center/ https://aws.amazon.com/privacy/

Bedrijf	**Twilio**
Rol	Subverwerker

Algemeen	Twilio wordt in sommige gevallen gebruikt om sms-berichten te verzenden. Ook wordt Twilio gebruikt om Siilo 's in-app VOIP (bellen via internet) en video-oproepfunctionaliteit te bieden. De inhoud van uw oproepen is end-to-end versleuteld (DTLS/SRTP). Indien nodig vanwege firewalls, werkt Twilio door eerst te bepalen welke van hun servers het beste is gepositioneerd tussen de beller en de ontvanger.
Waar worden de gegevens gehost?	https://www.twilio.com/docs/video/ip-address-whitelisting
Welke gegevens worden verwerkt?	● Telefoonnummers ● SMS content ● Metagegevens voor spraak-/videogesprekken in de app
Meer informatie	https://www.twilio.com/legal/privacy

Bedrijf	**CM.com**
Rol	Subverwerker

Algemeen	Als onderdeel van de registratiestroom van Siilo worden gebruikers gevraagd hun telefoonnummer op te geven. Dit telefoonnummer is een integraal onderdeel van het ontdekken van contacten voor nieuwe gebruikers. Als onderdeel van het beleid van Siilo voor het verifiëren van informatie, gebruiken we CM als sms-provider om een sms naar de gebruiker te sturen met een code welke ze invoeren om te bevestigen dat ze inderdaad toegang hebben tot het apparaat dat op dat nummer is aangesloten.
Waar worden de gegevens gehost?	Het datacenter bevindt zich in Nederland.
Welke gegevens worden verwerkt?	• Telefoonnummers • SMS content
Meer informatie	https://www.cm.com/about-cm/security-compliance/ https://legal.cmtelecom.com/nl/cm-online-bv/privacy-policy

Bedrijf	**Firebase**
Rol	Subverwerker

Algemeen	Firebase wordt door Siilo gebruikt voor Analytics en Crash rapportage in de iOS en Android Mobiele applicaties, om push notificaties te versturen voor de Android applicatie en om Dynamische links te creëren voor niet-gebruikers. Gebruikersgegevens worden geanonimiseerd verzonden. Gebruikers kunnen zich afmelden voor de analyseservice tijdens de registratie van de app.
Waar worden de gegevens gehost?	Google-datacenters: https://www.google.com/about/datacenters/locations/index.html Firebase gebruikt Standaardcontractbepalingen als mechanisme voor de doorgifte van gegevens buiten de Europese Unie, aangezien het Hof van Justitie van de Europese Unie dit heeft gevalideerd.
Welke gegevens worden verwerkt?	Geen persoonlijk identificeerbare gegevens Firebase Crash Reporting: ● Instance IDs ● Crashsporen Crashlytics: ○ Installatie UUID ○ IP-adressen Firebase Cloud Messaging ● Instance IDs Firebase Dynamische Links: ○ Apparaatspecificaties (iOS)

Meer informatie	https://firebase.google.com/support/privacy

Bedrijf	**ZenDesk**
Rol	Subverwerker
Algemeen	Siilo-gebruikers hebben verschillende manieren om gebruikersfeedback te geven, zoals via de Siilo messenger-app, maar natuurlijk ook via het contactformulier van Siilo op www.siilo.com of via het volgende e-mailadres: info@siilo.com. Vanwege het hoge volume van deze interacties heeft Siilo een ticketsysteem, gebruikmakend van een softwarepakket genaamd ZenDesk, om de communicatie tussen werknemers en gebruikers bij te houden.
Waar worden de gegevens gehost?	Zendesk heeft datacenters in drie belangrijke regio 's: de Verenigde Staten, Azië-Pacific en de Europese Unie. Servicegegevens kunnen in elke regio worden opgeslagen. ZenDesk gebruikt Standaardcontractbepalingen als mechanisme voor de doorgifte van gegevens buiten de Europese Unie.

Welke gegevens worden verwerkt?	• Namen • E-mailadressen • Telefoonnummers
nformatie	https://www.zendesk.nl/company/customers-partners/privacy-policy/ https://www.zendesk.com/blog/update-privacy-shield-invalidation-european-cour t-justice/

Bedrijf	**Salesforce**
Rol	Subverwerker
Algemeen	Informatie die wordt ingevoerd in het contactformulier op de website wordt verwerkt in Salesforce. We gebruiken Salesforce om correct en efficiënt te reageren op verzoeken van (potentiële) klanten.
Waar worden de gegevens gehost?	Frankfurt (Duitsland) / Parijs (Frankrijk)
Welke gegevens worden verwerkt?	• Namen • E-mailadressen • Naam organisatie

	• Kenmerken en behoeften.
Meer informatie	https://www.salesforce.com/company/privacy/

Bedrijf	**Zapier**
Rol	Subverwerker
Algemeen	Informatie die in het contactformulier op de website wordt ingevoerd, wordt door Zapier verwerkt en doorgestuurd naar verschillende eindpunten.
Waar worden de gegevens gehost?	De datacenters van Zapier bevinden zich in de Verenigde Staten. Zapier gebruikt Standaardcontractbepalingen als mechanisme voor de doorgifte van gegevens buiten de Europese Unie.

Welke gegevens worden verwerkt?	• Namen • E-mailadressen • Naam organisatie • Kenmerken en behoeften.
Meer informatie	https://zapier.com/privacy https://zapier.com/tos

Bedrijf	**Verifai**
Rol	Subverwerker
Algemeen	Siilo gebruikt Verifai om de identiteit van Siilo-gebruikers te verifiëren en identiteitsdocumenten te authenticeren. In de Siilo-app stellen we de gebruiker in staat om zijn paspoort, rijbewijs of ander identiteitsbewijs te fotograferen om zijn/haar identiteit te valideren.
Waar worden de gegevens gehost?	Verifai is gevestigd in Nederland

Welke gegevens worden verwerkt?	Verifai slaat nooit persoonlijke informatie op de apparaten van hun clienten op en Verifai verzendt nooit persoonlijke informatie naar hun eigen servers. Verifai verwerkt alleen statistische gegevens, waaronder het aantal scans, datum en tijd, documenttypen, het land van afgifte van de gescande documenten en het aantal successen en mislukkingen. Voor log- en monitoringdoeleinden worden basisgegevens over uw apparaat verzameld, zoals het besturingssysteem (OS), de OS-versie en het type apparaat.
Meer informatie	https://www.verifai.com/nl/privacy/ https://www.verifai.com/nl/terms-use/

Bedrijf	**Looker**
Rol	Subverwerker
Algemeen	Siilo gebruikt Looker als een platform voor dashboarding en BI dat verbinding zou maken met ons Amazon Redshift-datawarehouse. Hoewel er geen gegevens permanent zouden worden opgeslagen bij Looker, zouden ze onze gegevens verwerken en visualiseren en een voortdurende verbinding en tijdelijke cache van ons Redshift-magazijn vereisen om dat te kunnen doen. Alle gegevens zijn gepseudomiseerd (door userId) en bevatten

	geen P(H)I (naam, e-mailadres, IP-adres, werkelijke berichten, enz.).
Waar worden de gegevens gehost?	Looker is gevestigd in de Verenigde Staten, maar er worden geen Persoonsgegevens opgeslagen in de database van Looker.
Welke gegevens worden verwerkt?	Unieke (apparaat) identificatiegegevens, apparaatinformatie, gebruiksgegevens, analysegegevens, licentiegegevens,
Meer informatie	https://looker.com/product/security https://looker.com/trust-center/privacy/policy

Bedrijf	**MailChimp**
Rol	Subverwerker

Algemeen	Siilo gebruikt Mailchimp om e-mailcampagnes te verzenden naar Siilo-gebruikers om hen te informeren over productupdates alsmede naar potentiële Siilo-gebruikers wanneer hun organisatie hun e-mailadres heeft verstrekt om hen uit te nodigen.
Waar worden de gegevens gehost?	Verenigde Staten
Welke gegevens worden verwerkt?	Namen, e-mail, locatie
Meer informatie	https://mailchimp.com/nl-nl/legal/data-processing-addendum/ https://mailchimp.com/nl-nl/help/mailchimp-european-data-transfers/

Bedrijf	**Mailjet**
Rol	Subverwerker
Algemeen	Siilo gebruikt Mailjet om transactionele e-mails te verzenden naar Siilo-gebruikers, naar potentiële Siilo-gebruikers wanneer organisaties hun e-mailadres hebben opgegeven om hen uit te nodigen en naar mensen die hun informatie invoeren in het

	formulier voor het Prisma-abonnement op de website.
Waar worden de gegevens gehost?	Duitsland & België
Welke gegevens worden verwerkt?	Namen, e-mail, land, locatie
Meer informatie	https://www.mailjet.com/legal/dpa/