PROCESSOR AGREEMENT

This Processor Agreement is an agreement between the User/Client of the Apps and/or Services (hereafter: '**Controller**') and Siilo Holding B.V., a company incorporated under the laws of the Netherlands, having its office at Keizersgracht 585, 1072 DR Amsterdam, The Netherlands (hereafter: '**Processor**').

CONSIDERATIONS:

Within the framework of their contractual relations, Processor and Controller (hereafter together: '**Parties**') undertake to comply with applicable data protection laws and regulations, including, but not limited to, the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 applicable as of 25 May 2018 (hereinafter the " GDPR").

The purpose of this Processor Agreement is to define the conditions under which the Processor undertakes to carry out the Processing of Personal Data provided by the Controller to perform the Services.

AGREEMENT:

1. Definitions

The definitions attached to this Processor Agreement are available here.

2. Entry into force and duration

This Agreement shall be effective upon execution of the Contract to which it is attached and shall remain in effect for the duration of the contractual relationship between Processor and Controller.

3. Status of Parties

Processor is authorized by the Controller to process, on behalf of the Controller, the Personal Data, including Health Data, necessary for the provision of the Services and in strict compliance with the conditions provided in this Processing Agreement.

When the Controller enters Personal Data or Health Data of third parties in the App and/or Services or when using the Services, such as data from colleagues or Patients, he/she must comply with the requirements of applicable data protection laws and regulations.

3.1. Controller obligations

The Controller is solely responsible for keeping a record of processing activities as required by article 30 paragraph 1 GDPR and, where applicable, for completing any formalities, including, but not limited to, notifications, registrations, or prior notifications, prior to the implementation of the processing of Personal Data and Health Data with the competent supervisory authority in so far as required by applicable data protection laws and regulations. It is also the responsibility of the Controller to inform the data subjects in a manner which is compliant with applicable data protection laws and regulations, including, but not limited to, articles 12 – 14 of the GDPR, if Patients' Personal Data and Health Data are imported into the App and/or Services.

The Controller is solely responsible for the accuracy, reliability and relevance of the Personal Data and Health Data. In particular, the User is responsible for the use of the App and/or Services and the information that he/she deposits, stores, consults and removes from the App and/or

Services. The User agrees to indemnify and hold harmless Siilo, its representatives, employees and subcontractors from and against all claims, liabilities, damages and expenses (including legal fees and expenses) imposed on or incurred by Siilo to or suffered by Siilo, its agents, employees, and subcontractors resulting from the breach of this obligation under applicable data protection laws and regulations or under this Processor Agreement.

To avoid misunderstanding, Personal Data stored on the devices of Controller or a third party is under the control of Controller or such third party and is not part (or, as the case may be, is not part anymore) of the Processing by Processor even in the event such Personal Data have been transferred through the App or is stored in the App.

The Controller agrees to:

- Respect and ensure the respect of medical secrecy;
- Ensure that Personal Data is only shared with other users of the Apps and Services in accordance with applicable data protection laws and regulations;
- Implement a policy of authorization, management of access rights and roles and privileges, to ensure the confidentiality of Personal Data and Health Data in accordance with applicable data protection laws and regulations, as well as applicable laws and regulations concerning healthcare;
- Document in writing any instruction concerning the Processing of Personal Data and Health Data carried out by Siilo;
- Supervise the Processing carried out by Siilo as a Processor;
- Designate a privileged interlocutor in charge of representing the Controller;
- Designate a data protection officer if required by article 37 GDPR, if Controller has not already done so;
- Ensure, beforehand and throughout the duration of the processing, compliance with applicable data protection laws.

3.2. Siilo obligations

Siilo agrees to:

- Process Personal Data and Health Data according to the purposes and framework defined in this Processor Agreement, and comply with the technical standards and good practices applicable to Personal Data and Health Data;
- Act only upon the prior written instruction of the Controller and pursuant to the purposes of the processing as described in **Annex 1** to this Processor Agreement, unless a legal obligation applicable to the Processor requires the Processor to process Personal Data. In case of impossibility or difficulty in carrying out certain instructions, Siilo shall inform the Controller as soon as possible, in so far as allowed by applicable laws and regulations. Siilo may formulate a written request to deviate from the instructions. Siilo shall obtain the prior and specific written authorization of the Controller to proceed with this deviation. If any instruction of the Controller infringes upon applicable data protection laws or regulations in the opinion of Processor, Processor shall immediately inform the Controller thereof;
- Processor shall assist Controller in ensuring Controller's compliance with the obligations pursuant to article 35 GDPR (Data protection impact assessment) and article 36 GDPR (Prior consultation), taking into account the nature of Processing and the information available to the Processor.
- Not to make any copy of the Personal Data and Health Data without the authorization or instruction of the Controller, not to

communicate them to third parties and not to use them for purposes other than those specified in the Processor Agreement;
- Not to exploit or process for its own account and/or for the account of third parties, for any purpose whatsoever and in any manner whatsoever, the Personal Data and Health Data entrusted to it by the Controller;
- Put all the means in its possession with regard to the contractual stipulations and the rules of the art to ensure the safety and the confidentiality of the Personal Data and Health Data which are entrusted to it and in particular to prevent that they are not deformed, damaged or communicated to unauthorized third parties and more generally to implement the appropriate technical and organizational measures to protect the Personal Data and Health Data against accidental or illicit destruction, accidental loss, alteration, dissemination or unauthorized access, in particular when the Processing involves data transmissions in a network, as well as against any form of illicit processing;
- Notify the Controller as soon as possible of any security breach that directly or indirectly affects Personal Data, Health Data or Processing concerning him/her;
- Carry out regular backups of Personal Data;
- Carry out regular penetration tests (or Pentest);
- Maintain the equipment necessary for the proper functioning of the Services;
- Ensure the confidentiality of the Personal Data and Health Data processed;
- Take into account any update, correction, deletion or other modifications communicated by the Controller concerning the Personal Data and Health Data;
- Respect the retention period of the Personal Data and Health Data applicable to the purposes for which they were collected or provided and delete/anonymize them as soon as these purposes no longer exist, subject to legal obligations.

4. Personal Data Breach

4.1. Processor shall without undue delay inform Controller of any established Personal Data Breach by electronic message or any other means of communication made available to him by the Controller.

4.2. This notification shall be accompanied, at the request of the Controller and in so far as possible, by any information concerning the nature of the Personal Data Breach, the potential consequences of the Personal Data Breach and/or the measures that Processor has implemented and/or intends to implement to address the Personal Data Breach.

4.3. Processor shall, in so far as possible, assist Controller in ensuring Controller's compliance with the obligations pursuant to article 33 GDPR (Notification of a personal data breach to the supervisory authority) and article 34 GDPR (Communication of a personal data breach to the data subject), taking into account the nature of Processing and the information available to the Processor. It is up to Controller to determine whether a Personal Data breach shall be notified to the supervisory authority or communicated to the Data Subject(s) by Controller.

5. Information and rights of Data Subjects

It is the responsibility of the Controller to inform the Data Subjects (i) of the Processing carried out in the context of the Services and to obtain their consent(s) where this is necessary under the applicable law; (ii) of the legal basis for the

Processing carried out, the purposes of the Processing as well as the list of subcontractors likely to process their Personal Data.

6. Management of data requests

It is the responsibility of the Controller to follow up on the Data Subjects' requests relating to those rights concerning their Personal Data enshrined in articles 15 – 22 GDPR. To the extent possible, Siilo, in its capacity as a Processor and at the request of the Controller, may assist the Controller in fulfilling his/her obligation to comply with such requests of Data Subjects.

7. Confidentiality

7.1. Processor is obligated to keep all Personal Data which is provided to her by Controller confidential, except in case of a legal obligation which is applicable to Processor or an instruction of Controller to the contrary.

7.2. At the instruction of authorized administrative and judicial authorities, Siilo may communicate Personal Data that it processes in the name and on behalf of the Controller in order to comply with its legal obligations. In this case, and unless otherwise provided by law, Siilo undertakes to notify the Controller of this communication.

7.3. Processor shall ensure that all persons that process Personal Data on the instruction of Processor, including, but not limited to, employees of Processor and Subcontractors of Processor, are obligated to keep confidential the Personal Data, subject to the contents of this article.

8. Security and control

8.1. Processor shall implement appropriate technical and organizational measures pursuant to article 32 GDPR (Security of processing), which measures shall include at least those measures that are described in **Annex 2**.

8.2. The above obligations do not relieve the Controller from implementing all necessary technical and organizational security measures for the security and confidentiality of all information, including Personal Data, present on the App and or Services.

9. Subprocessors

Controller grants the Processor a general written authorization to use the Subprocessors listed in Annex 3.

Pursuant to this general authorization, Processor agrees to notify Controller, by way of fifteen (15) days prior written notice, of any changes regarding the addition or replacement of Subcontractors, thereby affording Controller the opportunity to raise any objections they may have to such changes. If the Controller has legitimate and reasonable grounds for objecting to the appointment of a new Subcontractor, they must immediately give reasons to Processor by sending written notice to Processor at privacy@siilo.com, within fifteen (15) business days, failing which Controller shall be deemed to have approved and accepted such appointment.

After discussions and in the absence of agreement between Processor and Controller, Controller may, within fifteen (15) days of notification, terminate the portion of the Contract affected by the update in question.

With respect to each Subcontractor, Processor shall (i) exercise commercially reasonable care in the performance of its evaluation, appointment and monitoring of the Processing activities of the Subcontractors; (ii) include in the contract between Processor and each Subcontractor clauses providing an equivalent level of protection for the Personal Data and Health Data processed on behalf of Controller, as provided for in this Processor Agreement.

If a Subcontractor does not fulfill its obligations with respect to the protection of Personal Data, Processor shall remain liable to the Controller for the performance by the Subcontractors of its obligations under the Processor Agreement.

10. Audit

10.1. In order to measure the security of the Services, the Controller may have security audits carried out at its own expense, in compliance with the conditions set out in this article and within the limit of one (1) audit per year, the duration of which audit will not exceed the maximum of five (5) working days. All time spent by staff of Processor in relation to an audit will be invoiced to the Controller.

10.2. The audit shall be limited to the verification of the processes, organization and tools directly and exclusively related to the implementation of the provisions of the GDPR for the Services concerned.

In no event shall the audit be intended to monitor or acquire access to (i) any non-specific Personal Data or Health Data, whether or not confidential, or any information the disclosure of which could, in Processor's discretion, adversely affect the security of the Services or any other of its Users; (ii) Processor's financial data; or (iii) Personal Data relating to Processor's employees or its Subcontractors.

It is agreed that all activities undertaken in the course of an audit shall not, concurrently or otherwise: (i) interfere with, modify or otherwise affect the operation of any Services, systems, networks, software and/or hardware other than those allocated for the exclusive use of the Controller; (ii) damage the infrastructure hosting the Services; (iii) damage, delete, modify any type of data; (iv) allow unauthorized access to or maintenance of any of the foregoing data.

No penetration or intrusion testing of the Processor's platform and/or application is permitted for any reason and such testing is excluded from audits without Processor's prior written consent.

At the request of the Controller, Processor shall communicate to the latter the certification audit reports issued by the certification body intended for such communication.

10.3. The Controller shall send Processor at least thirty (30) days before the audit is carried out an audit agreement detailing its exact scope, the planned dates and times, and the conditions relating thereto. The auditor must also specify any accounts and profiles used for the tests (source IP address, user agent, etc.), the methodology used, as well as the actors to be audited.
The content of the audit agreement must be accepted in advance by Processor before the audit begins.

10.4. The information obtained during the audit is Confidential Information and shall be treated as such by the Controller. This information may only be communicated to persons who are subject to strict confidentiality requirements and who have a direct and major interest in knowing it and must not be disclosed to the public or internally in any way.
If the Controller wishes to call upon the services of an external auditor, the Controller shall obtain Processor's prior written consent, it being understood that Processor may only refuse the auditor on the basis of objective and substantiated arguments.

The external auditor may under no circumstances be a competitor of Processor and must undertake in writing to respect the conditions set out in this article.
The Controller undertakes to communicate the audit report to Processor free of charge, and Processor shall be entitled to present its observations.

Processor shall have a reasonable period of time from the date of receipt of the report to correct any shortcomings and/or non-conformities found.

11. Retention and destruction of personal data

11.1. As a reminder, Siilo Messenger is a secure exchange channel between Health Actors and it is not intended to serve as a place to store data or documents relating to the monitoring of Patients. Controllers are responsible to regularly back up data and documents exchanged through Siilo Messenger.

11.2. Controller has the option to (i) delete, or (ii) export all User Generated Content on or from its devices and Account.
For the sake of clarity, if the User deletes his/her User Account or any User generated Content shared using the Services, User Generated Content sent to other Users of the apps are under the control of those Users and are not part of any deletion such as described above.

11.3. Regarding the use of Siilo Messenger, the User will be able to retrieve the User Generated Content available on his/her User Account by downloading manually each conversation. Each conversation is downloadable under the PDF format. The User acknowledges that he/she has all necessary rights and/or permissions to retrieve such User Generated Content.

Controller shall determine all retention periods and ensure that they are observed by deleting the respective Personal Data.
Unless the User has activated the option to "Retain the conversation" in the specific setting of each conversation, all messages will be deleted after a thirty (30) days period. In case such an option has been activated by the User, all User Generated Content relating to the conversation will be retained for an unlimited period, meaning until the User decides to delete his/her User Account, or until such retention option is deactivated.

11.4. At the end of this Processor Agreement, Processor undertakes to, at the choice of the Controller,

- provide the Personal Data to Controller and subsequently destroy the Personal Data without keeping any copy, subject to legal retention obligations to which Processor may be subject, within fifteen (15) days.; or
- to destroy the Personal Data without keeping any copy, subject to legal retention obligations to which Processor may be subject, within fifteen (15) days.

The Processor will ensure that all the associated Personal Data processed by its Subcontractors shall be destroyed except if further storage of Personal Data is required by law.

12. Transfers of Personal data

Personal Data may be transferred to Processor's group companies, their subcontractors or service providers established in countries benefiting from an adequate level of protection or offering adequate safeguards regarding the protection of privacy and fundamental rights and freedoms of individuals, in accordance with applicable legislation.

Processor will only transfer Personal Data to Subcontractors in countries outside of the European Economic Area when such transfer is required for the performance of the ordered Services. The list of Subcontractors is available in Annex 3.

If a transfer takes place to a third country outside of the European Economic Area where applicable data protection legislation has not been recognized as providing an adequate level of protection of Personal Data, Processor shall ensure that adequate measures are put in place in

accordance with the GDPR and applicable data protection laws and regulations, and in particular, where necessary, that Standard Contractual Clauses or equivalent ad hoc clauses are included in the contract concluded between Processor and the recipient of the Personal Data.

13. Other

13.1. Processor is entitled to change and amend this Processor Agreement to reflect e.g. developments in jurisprudence, changed regulations, best practices published by the Supervisory Authorities and the like. Processor shall inform Controller of such changes and amendments before such new version becomes effective. In the event such new version shall materially negatively affect Controller's position, Controller shall be entitled to refuse the new version. In that event the Contract between Controller and Processor shall end.

13.2. This Processor Agreement is not transferable by either Party without the written consent of the other Party. However, no consent is required in case of transfer by Processor to a subsidiary or parent company of Processor.

13.3. This Processor Agreement is governed exclusively by Dutch law.

13.4. Parties will exclusively submit their disputes related to this Processor Agreement to the relevant court in Amsterdam.

Annex 1. Details on Personal Data Processing activities

This Processing Agreement does not apply to Personal Data of User/Client or contact persons of User/Client (e.g. contact information, e-mail address, phone numbers, bank accounts, credit information etc.) that Siilo and its group companies process as controller under GDPR as described in the Privacy Policy available online.

Controller : as the case may be, the User of the App and the Services, and/or the Client who subscribed to Siilo Connect and/or Prisma.

The activities of the Controller include Processing for the exercise of prevention, diagnosis and care activities as well as the administrative management of his health establishment, health center or private practice.
In particular, for the purposes of patient care, the Processing covers (i) instant messaging (Siilo Messenger and Siilo Webchat), (ii) a private organizational network (Siilo Connect) and (iii) virtual collaborative consultation (Siilo Prisma).

Processor : Siilo

The activities carried out by the Processor on behalf of the Controllers are described below.

PROCESSING N°1 : INSTANT MESSAGING (Siilo Messenger and Siilo Webchat)

PROCESSING OPERATIONS:
Siilo Services involve the collection, recording, organization, storage, retrieval, consultation and use, communication use, disclosure by transmission, anonymization and deletion of the Personal Data listed below.

PURPOSES OF THE PROCESSING:
The free instant messaging service is designed to ensure better care coordination, enabling Users to communicate and send text messages, video, photos, voice notes and other media.
Siilo Messenger enables one to one discussions, as well as group discussions.

LEGAL BASIS:
It is up to the Controller to determine this legal basis before any Processing operation.

As an indication, legitimate interest could constitute the legal basis.
The Controller is free to inform Siilo of any other legal basis.
In the event that the Controller communicates patient Personal or Health Data to a Health Actors who are not part of the given patient's care team, he must first request the consent of this patient.

DATA SUBJECTS:
- Patients
- Health Actors or assistants with an Account.

PERSONAL DATA PROCESSED:
In principle, the following data are considered relevant for the purposes mentioned above:
- Health Actor identification data;
- Health Actor contact data;
- Medical history, family history and allergies;
- Consultation data;
- Prescription data;
- Biometrics and biology data;
- Health care team data;
- Medical imaging;
- Photo, videos;
- Voice notes;
- For videos and voice calls: video/voice stream allowing the transmission between the Health Actors;
- Usage and connection logs that report on the "business actions" of Users within the

Siilo Services as well as technical logs that report on the "activity" of the software and hardware components used by the User/Subscriber so that Siilo can ensure the operation and access to the requested functionalities.

RECIPIENTS :

- Health Actors or assistants with a User Account;

RETENTION:

Unless the User has activated the option to “Retain the conversation” in the specific setting of each conversation, all messages will be deleted after a thirty (30) days period.

PROCESSING N°2 : PRIVATE ORGANIZATIONAL NETWORK (Siilo Connect)

PROCESSING OPERATIONS:

Siilo Services involve the collection, recording, organization, storage, retrieval, consultation and use, communication use, disclosure by transmission, anonymization and deletion of the deletion of the Personal Data listed below.

PURPOSES OF THE PROCESSING:

Via Siilo Connect, employees / members of the organization can easily find and contact each other and share information via the “News & Views” space. Through the Siilo Connect admin tool, the Client’s personnel can configure and personalize their organization network, broadcast messages, invite people to join the network, pre-create conversation for Users.

LEGAL BASIS:

It is up to the Controller to determine this legal basis before any Processing operation.

As an indication, legitimate interest could constitute the legal basis.

The Controller is free to inform Siilo of any other legal basis.

DATA SUBJECTS :

- Patients
- Health Actors or assistants with an Account.

PERSONAL DATA PROCESSED :

In principle, the following data are considered relevant for the purposes mentioned above:

- Identification data, professional data and contact details of the Health Actors and assistants part of the Data Controller’s organization;
- Health Actor identification data;
- Health Actor contact data ;
- Medical history, family history and allergies ;
- Consultation data ;
- Prescription data;
- Biometrics and biology data;
- Health care team data;
- Medical imaging;
- Photo;
- Usage and connection logs that report on the "business actions" of Users within the Siilo Services as well as technical logs that report on the "activity" of the software and hardware components used by the User/Subscriber so that Siilo can ensure the operation and access to the requested functionalities.

RECIPIENTS:

- Health Actors or assistants with a User Account;

RETENTION:

Unless specifically instructed otherwise by the Controller, Siilo shall apply the retention periods as recommended by the competent supervisory authorities or applicable legislation.

PROCESSING N° 3 : VIRTUAL COLLABORATIVE CONSULTATION (Siilo Prisma)

PROCESSING OPERATIONS :
Siilo Services involve the collection, recording, organization, storage, retrieval, consultation and use, communication use, disclosure by transmission, anonymization and deletion of the deletion of the Personal Data listed below.

PURPOSES OF THE PROCESSING :
Via Siilo Prisma general practitioners can quickly, accessibly and anonymously submit a virtual collaborative consultation to a multidisciplinary network of specialists, who review and respond to such consultations; and have access to a searchable knowledge base of previously answered collaborative consultations

LEGAL BASIS :
It is up to the Controller to determine this legal basis before any Processing operation.

As an indication, legitimate interest could constitute the legal basis.
The Controller is free to inform Siilo of any other legal basis.

DATA SUBJECTS:
- Patients
- Health Actors or assistants with an Account.

PERSONAL DATA PROCESSED:
In principle, the following data are considered relevant for the purposes mentioned above :
- Health Actor identification data;
- Health Actor contact data;
- Medical history, family history and allergies;
- Consultation data;
- Prescription data;
- Biometrics and biology data;
- Health care team data;
- Medical imaging;
- Photo;
- Usage and connection logs that report on the "business actions" of Users within the Siilo Services as well as technical logs that report on the "activity" of the software and hardware components used by the User/Subscriber so that Siilo can ensure the operation and access to the requested functionalities.

RECIPIENTS :
- Health Actors or assistants with a User Account;

RETENTION:
Unless specifically instructed by the Controller, Siilo shall apply the retention periods as recommended by the competent supervisory authorities or applicable legislation.

Annex 2. Organizational and security measures

Organizational and administrative policies and controls

Siilo has implemented an information security management system (ISMS) and Siilo is certified against ISO27001 and NEN7510 (Dutch standard for managing information security in healthcare).

As part of the ISMS, Siilo has implemented several organizational and administrative policies and controls such as periodic and standard risk assessments, internal audits, an information security policy, a least privilege policy, training of staff, a (security) incident management procedure and a data breach notification procedure. The objective of Siilo's ISMS is to enable further improvement of the organization, staff and its products.
Every solution that Siilo implements goes through a risk assessment and data protection impact assessment. It follows a strict process safeguarded by our ISMS policies demonstrated by our ISO-27001 and NEN7510 certificates.

Siilo has appointed an independent Security Officer and Data Protection Officer who is registered with the Dutch Data Protection Authority.

Development process

Siilo's development process employs several strategies to ensure both the quality as well as the security of data:
(1) Unit tests: for every feature we develop a set of basic tests which exercise that feature in isolation;
(2) Peer code review: changes to the app are reviewed by at least two developers before acceptance into a beta release. For features which impact security or privacy-related tasks, those new lines of software code are reviewed by a senior developer from outside of the team and the senior developer interacts with the security officer and privacy officer before releasing the new feature(s) to the messenger.
(3) Manual testing and limited public beta: prior to release, features are released internally for manual testing and are often also released to a select pool of "friendly beta testers."

This approach is used to screen device-specific features, as well as any features which may only emerge after being exposed to a diverse set of work flows.

Least privilege

Privileges are provided to Siilo staff on a strict need-to-have basis. This is monitored and checked annually by a security officer. Any Siilo employee who needs access to information outside of their allocated role, must first log the request with our standard template. These requests are logged and authorized by the Data Protection Officer if a request is deemed compliant with the General Data Protection Regulation prior to its fulfilment. These requests are also reviewed once per quarter by the Siilo ISO-27001 committee comprised of the Data Protection Officer, and Siilo's Chief Executive Officer and/or the Chief Financial Officer.

Technical policies and controls

Message data – data in transit

To understand the solutions to mitigate the risks for data in transit, please read our security white paper (https://www.siilo.com/resources/security-white-paper) as it describes in detail our security-by-design approach, the threat model and cryptographic protocols.

In short, Siilo uses end-to-end encryption implemented with LibSodium, a fork of the NaCl crypto library https://nacl.cr.yp.to/.
This means that each message between sender and receiver is protected via a public/private keypair. Only sender and recipient are able to decrypt and read the messages they exchange, and the authenticity of any message can be empirically verified. Third parties, including Siilo company and its employees are never able to read them.

Siilo uses certificate pinning to prevent so-called “man-in-the-middle” attacks, a process whereby attackers access the traffic between the phones and try to break in and tap the communication lines to read the messages. Standard TLS v1.2 communications require a valid SSL certificate that was issued from a trusted certificate authority, recognized by the device. Certificate pinning goes further and mandates that those certificates must be only issued from a chain of trust rooted to a specified issuer. This closes a litany of vulnerabilities arising from the key distribution problems associated with the internet's certificate authority infrastructure.

Message data – data at rest on user device

For data at rest on the device (iPhone, iPad, Android) the following safeguards are in place :

- All "key material" also known as the codes used by the cryptograph are stored in the iOS KeyChain or the Android KeyStore as appropriate;
- All "key material" is encrypted by a "master key" that is derived from the pin code chosen by the user;
- The entire database is encrypted using SQLiteCipher. All messages, message metadata, and contact information are stored in this manner;
- All received media is stored encrypted by the single use, symmetric encryption key. This key is accessed via the database mentioned above;
- An application level pin code mechanism prevents access by humans that have physical access to the device. This addresses most forms of in-person social engineering such as asking to borrow the phone for a quick call, etc.
- All exchanged information in the Siilo app is automatically deleted after 30 days. Users can decide for themselves to delete individual messages on an ad hoc basis if they deem 30 days too long. We have consciously not included count-down timers and message lifespans such as seconds/ hours as we believe it will create a sense of urgency resulting in screenshots and other unwanted behavior at the receiving end;
- When a user knows his/her device is lost, stolen or otherwise compromised, he/she can alert its organization (this is a Siilo Connect feature) and a Siilo Connect Admin can remotely wipe the Siilo data off the device. Message data – data at rest on Siilo servers For data at rest on Siilo servers the following safeguards are in place:
- All Siilo servers are located within the European Union with the highest security- and compliance norms;
- Firewall rules prevent network access to the databases (MySQL and ElasticSearch) and is restricted to a subnet containing Siilo's servers and a VPN, which a limited subset of Siilo employees are able to access;
- The MySQL database is password protected and encrypted industry standard AES-256 and stores messaging data, messaging metadata, Siilo Connect configuration data, and user profile data;
- ElasticSearch encrypts specific fields such as email and phone numbers to enable matching. Other profile fields which are

shown in the app as "public" to Siilo members are stored in plain text;
- All media (sent via the application and thus considered sensitive) is stored and encrypted by the single use, symmetric encryption key. That key is not stored on any Siilo server except as part of the encrypted message data stored in MySQL. The keys to decrypt that data are only available on the devices of the sender and recipient. Storage of personal data on Siilo servers Message data is stored at servers in Frankfurt (Germany) and for backup purposes, daily automated 'snapshots' are taken that are stored for no more than 7 days. These snapshots are encrypted at rest. Siilo's server infrastructure is hosted by Amazon, Inc. Siilo has purposefully chosen Amazon Web Services (AWS) as they employ the highest security and encryption standards and ensure (GDPR) compliance with their SOC level I-II-III, ISO9001, ISO27001, ISO27017, and ISO27018 certifications.

User data User data is stored at servers in Dublin (Ireland) and is backed up daily and stored for no longer than 30 days in a preconfigured bucket that is encrypted at rest.

Phone number matching on Siilo

Siilo optionally lets the user discover other Siilo contacts by cross-referencing with the phone's address book. If the user chooses to do so, the following information is uploaded through an encrypted TLS connection to the server:
(1) First 64bits of the SHA1 hash of the E.164 normalized form of each phone number found in the phone's address book
(2) Key: EEDAAC207FC6BA08727C
(3) Only the phone numbers are hashed and cross-referenced. Siilo does not touch associated names, email address(es) and other information the phone's address book holds. The Siilo server then compares the list of hashes from the user with the known phone hashes of current Siilo users. The server will only match against current Siilo users, and after returning the matches to the mobile client, the server immediately discards the submitted hashes.

Security measures are described in Siilo Security Whitepaper available here.

Annex 3 : List of Subcontractors

In order to provide its services, Siilo uses service providers. These service providers may have access to personal data collected by Siilo only in the context of and for the purposes of the operations mentioned below.
Siilo ensures that each of these service providers implements appropriate technical and organizational measures to guarantee the security and confidentiality of the data processed.

In accordance with the General Data Protection Regulation and in the interest of transparency, Siilo communicates below the list of its subcontractors.

Company	**Amazon Web Services**
Role	Sub Processor
General	Siilo's server infrastructure is hosted by Amazon.
Where is the data hosted?	All messaging related activities are in Amazon's Frankfurt data centers. For services such as the email verification (Amazon Simple Email Service), and website content security policy logging (Amazon Lambda), those services are only offered in the Ireland datacenter. Amazon Web Services uses Standard Contractual Clauses as a mechanism for transferring data outside the European Union. Siilo also uses Cloudfront services to guarantee the security of its platform and to protect itself against attacks such as CDS and DDos. Servers are located globally depending on the location of the end user. For more information, you can consult this page.
Which data is processed?	Processed by Amazon AWS : ● Email addresses and email content; ● User profile data; ● Encrypted message data; ● Message meta data (pseudonymised); ● Request meta data. For Cloudfront services : ● IP address ● Technical meta data (device type etc).

More info	https://aws.amazon.com/compliance/gdpr-center/ https://aws.amazon.com/privacy/

Company	**Twilio**
Role	Sub Processor
General	Twilio is used in some cases to send SMS messages. Also, Twilio is used to provide Siilo's in-app VOIP (calling via internet) and video call functionality. The contents of your calls are end-to-end encrypted (DTLS/SRTP). If necessary due to firewalls, Twilio works by first determining which of their servers is best positioned between the caller and recipient.
Where is the data hosted?	https://www.twilio.com/docs/video/ip-address-whitelisting
Which data is processed?	● Phone numbers ● Sms content ● In-app voice/video call meta data
More info	https://www.twilio.com/legal/privacy

Company	**CM.com**
Role	Sub Processor
General	As part of the Siilo registration flow, users are asked to provide their phone number. This phone number is integral to contact discovery for new users. As part of Siilo's policy on verifying information, we use CM as an SMS provider to send an SMS to the user with a code which they input to confirm that they indeed have access to the device connected to that number.
Where is the data hosted?	The datacenter is located in the Netherlands.
Which data is processed?	● Phone numbers ● Sms content
More info	https://www.cm.com/about-cm/security-compliance/

	https://legal.cmtelecom.com/en/cm-online-bv/privacy-policy

Company	**Firebase**
Role	Sub Processor
General	Firebase is used by Siilo for Analytics and Crash reporting in the iOS and Android Mobile applications, to send push notifications for the Android application and to create Dynamic links for non-users. User data is sent anonymized. Users can opt out of the analytics service during the registration of the app.
Where is the data hosted?	Google datacenters: https://www.google.com/about/datacenters/locations/index.html Firebase uses Standard Contractual Clauses as a mechanism for transferring data outside the European Union, since the Court of Justice of the European Union has validated this.
Which data is processed?	No personal identifiable data Firebase Crash Reporting: ● Instance IDs ● Crash traces Crashlytics: ○ Installation UUID ○ IP Addresses Firebase Cloud Messaging ● Instance IDs Firebase Dynamic Links: ○ Device specs (iOS)
More info	https://firebase.google.com/support/privacy

Company	**ZenDesk**
Role	Sub Processor
General	Siilo users have several ways to provide user feedback, such as via the Siilo messenger app, but also of course through either Siilo's contact form on www.siilo.com or the following email address: info@siilo.com. Due to the high volume of these interactions, Siilo has a ticketing system, using a software called ZenDesk, to keep track of

	employee-user communication exchanges.
Where is the data hosted?	Zendesk has data centers in three main regions — the United States, Asia Pacific, and the European Union. Service Data may be stored in any region. ZenDesk uses Standard Contractual Clauses as a mechanism for transferring data outside the European Union.
Which data is processed?	● Names ● Email addresses, ● Phone numbers
More info	https://www.zendesk.nl/company/customers-partners/privacy-policy/ https://www.zendesk.com/blog/update-privacy-shield-invalidation-european-cour t-justice/

Company	**Salesforce**
Role	Sub Processor
General	Information that is entered in the contact form on the website is processed in Salesforce. We use Salesforce to correctly and efficiently respond to requests from (potential) customers.
Where is the data hosted?	Frankfurt, GER / Paris, FRA
Which data is processed?	● Names ● Email addresses ● Organization name ● Characteristics and needs.
More info	https://www.salesforce.com/company/privacy/

Company	**Zapier**
Role	Sub Processor
General	Information that is entered in the contact form on the website is processed and routed by Zapier to different end-points.
Where is the data hosted?	Zapier's datacenters are located in the United States. Zapier uses Standard Contractual Clauses as a

	mechanism for transferring data outside the European Union.
Which data is processed?	• Names, • Email addresses, • Organization name, • Characteristics and needs.
More info	https://zapier.com/privacy https://zapier.com/tos

Company	**Verifai**
Role	Sub Processor
General	Siilo uses Verifai to verify the identity of Siilo users and authenticate ID documents. In the Siilo-app we enable the user to photograph their passport, driver's license or other proof of identity to validate their identity.
Where is the data hosted?	Verifai is located in the Netherlands
Which data is processed?	Verifai never stores any personal information on their clients devices and Verifai does never send any personal information to their own servers. Verifai only processes statistical data, which includes the number of scans, date and time, document types, the issuing country of the scanned documents, and number of successes and fails. For logging and monitoring purposes, basic details about your device such as operating system (OS), OS version and the type of device are collected.
More info	https://www.verifai.com/en/privacy/ https://www.verifai.com/en/terms-use/

Company	**Looker**
Role	Sub Processor
General	Siilo uses Looker as a platform for dashboarding and BI that would connect to our Amazon Redshift data warehouse. While no data would permanently be stored with Looker, they would process and visualize our data and require an ongoing connection

	and temporary cache from our Redshift warehouse to be able to do that. All data is pseudomized (by userId) and does not contain P(H)I (name, email, ip address, actual messages, etc).
Where is the data hosted?	Looker is located in the United States, but no Personal Data is stored within Looker's database.
Which data is processed?	Unique (device) identifiers, device information, usage data, analytics data, license credentials,
More info	https://looker.com/product/security https://looker.com/trust-center/privacy/policy

Company	**Mailchimp**
Role	Sub Processor
General	Siilo uses Mailchimp to send email campaigns to Siilo users informing them about product updates and to potential Siilo users when their organization has provided their email address to invite them.
Where is the data hosted?	United States
Which data is processed?	Names, email, locale
More info	https://mailchimp.com/en-au/legal/data-processing-addendum/ https://mailchimp.com/en-au/help/mailchimp-european-data-transfers/

Company	**Mailjet**
Role	Sub Processor
General	Siilo uses Mailjet to send transactional emails to Siilo users, potential Siilo users when organisations have provided their email address to invite them and to people entering their information in the Prisma subscription form on the website.
Where is the data hosted?	Germany & Belgium
Which data is processed?	Names, email, country, locale
More info	https://www.mailjet.com/legal/dpa/