Siilo Privacy Policy

This privacy policy (the "Policy") applies to the processing of your Personal Data as a user of the Siilo App and as a visitor to the website www.siilo.com (the "Site").

This policy does not govern data that Users send through the App or Services to other Users (e.g. through Siilo Messenger, Siilo Webchat). Users can find more information on how Personal and Health Data is shared through Siilo Services in the Processor Agreement attached to the Terms of Use."

Definition

Capitalized terms used in the Policy have been defined in the "Definitions" document available here.

In the event of a conflict between the terms defined in the Policy and the terms in the "Definitions" document, the terms in the Policy shall prevail.

Who controls the processing of your Personal Data?

In accordance with the General Regulation on the Protection of Personal Data (hereinafter referred to as GDPR), the Controller is the person who determines the means and purposes of a processing activity. The Processor is a person processing Personal Data on behalf of the Controller. He acts under the authority of the controller and authority of the data controller and on the latter's instructions.

Siilo Holding B.V., located at Keizersgracht 585, 1017 DR Amsterdam, the Netherlands, or a designated group company is the Controller for the Personal Data collected in particular in the context of (i) the administration and management of User Accounts, (ii) browsing on the Site or the App, (iii) the creation of statistics relating to the use of the App and Services, their computation and anonymization (iv) sending of marketing campaigns to Siilo's Users and prospects.

As a Data Controller, Siilo takes the appropriate measures to ensure the protection and confidentiality of the Personal Data it holds or processes in compliance with the provisions of the GDPR.

For more information on Personal and Health data processed by Siilo acting as a Data Processor on the behalf of Siilo's Users acting as Data Controllers, refer to the Processor Agreement attached to the ToU.

Providing your Personal Data is not compulsory

Providing Personal Data is never compulsory. Users can always decide whether or not to provide Personal Data. However, in order to be able to make use of a number of Services the provision of Personal Data is necessary. Siilo will indicate which data are necessary to make use of the Service and therefore must be provided, and which Personal Data can be provided optionally.

Source of Personal Data

The Personal Data processed by Siilo are collected through different channels.

- **Personal Data provided by the Users**

Siilo may process Personal Data provided directly by the User or Client (i) when creating a User Account or using the Services, (ii) via contact forms or any other document available online on the Sites and or provided during external events such as trade shows, (iii) during telephone exchanges with Siilo.

When a Client subscribes to Siilo Connect or Prisma, the Personal Data about the personnel of the Client organization may be communicated to Siilo, in order for Siilo to create the Client network and to invite such personnel to become Users of the App and Services, and to join the network.

- **Personal Data that Siilo automatically collects when using the Services**

As described below, Siilo may automatically collect Personal Data when using the Services and browsing the Siilo App and Services. This automatic collection may take place through the use of cookies and other trackers.

For more information on Siilo use of cookies and trackers, you can consult our Cookies Policy.

Which Personal Data do we process ?

When we provide our Services, we may process Personal Data.

This could include the following:

1. **Users data necessary to provide the Services**

Data processed	Purpose for processing	Legal basis	Retention
Names (first, last)	Relevant for verification, establish peer trust	Necessary for the performance of a contract to which the data subject is is a party to or for the the performance of pre-contractual measures taken at the request of request of the data subject	Deletion after end of the contractual relationship
Phone number	Relevant to establish connections on the Siilo Messenger	Necessary for the performance of a contract to which the data subject is is a party to or for the the performance of pre-contractual measures taken at the request of request of the data subject	
Email address(es)	Relevant for part of the verification process, to identify users as part of a customer's organization	Necessary for the performance of a contract to which the data subject is is a party to or for the the performance of pre-contractual measures taken at the request of request of the data subject	
Medical registration number (optional)	Relevant for verification, establish peer trust	Necessary for the performance of a contract to which the data subject is is a party to or for the the performance of pre-contractual measures taken at the request of request of the data subject	

Avatar picture, Title(s), Specialization(s), Interest(s), Organisation/ association	Relevant for peer to peer trust *(optional)*	Necessary for the performance of a contract to which the data subject is is a party to or for the the performance of pre-contractual measures taken at the request of request of the data subject	
Phone contacts telephone numbers	Relevant to immediately establish connections on Siilo Messenger *(Optional: only for users who activated the feature).*	Consent	
Findable group name, group description	Relevant to establish connections on Siilo Messenger*(optional)*	Necessary for the performance of a contract to which the data subject is is a party to or for the the performance of pre-contractual measures taken at the request of request of the data subject	
Copy of official identification document (e.g. medical ID/registration number, driver's license, ID card or passport)	Relevant for verification, establish peer trust *(optional)*	Necessary for the performance of a contract to which the data subject is is a party to or for the the performance of pre-contractual measures taken at the request of request of the data subject	Deletion after verification.
Organization specific profile fields	Relevant to the members of a specific organization on Siilo to custom their profile field	Necessary for the performance of a contract to which the data subject is is a party to or for the the performance of pre-contractual measures taken at the request of request of the data subject	Deletion after end of the contractual relationship
Number of connections on the App	Relevant to receive information on how to get started with Siilo	Legitimate interest of Siilo	

Device information: user IP address, mobile device type, operating system version of the app, language of the device, push destination, Touch-ID enabled, Face-ID enabled.	Relevant for development process, and understand bugs in the software and how to fix them	Legitimate interest Users can opt out of the analytics service during the registration of the app (by switching the “Anonymous report” toggle).	
Number of groups	Relevant to understand level of engagement on Siilo Messenger for Siilo customers	Legitimate interest of Siilo	
Organizational role	Relevant for privileges in the Siilo Connect environment	Necessary for the performance of a contract to which the data subject is is a party to or for the the performance of pre-contractual measures taken at the request of request of the data subject	
How many messages sent/ received, How many and which days online, Web app activation and current sessions	Relevant to understand level of engagement on Siilo for Siilo customers	Legitimate interest of Siilo	
Message events: Type of message (chat message, voice call, video call), Timestamp, User / Installation ID sender, Type of session (webchat or not), Client type, Siilo version, Location on the basis of IP address.	We gather this information to trace the performance of our application divided over different versions and countries.	Legitimate interest of Siilo	
Message events:	We gather this information to	Legitimate interest of Siilo	

Group ID destination (only applicable during a group message), Destination of message (user or group), User ID destination (only applicable during a user message).	be able to generate statistics like unique active groups and unique recipients.		No retention period is applied to the meta-data. All Personal Data will be deleted after ending the contractual relationship. This means that the meta-data can no longer be traced back to the user.
Message events: Message ID	This information gives us the ability to count unique messages.	Legitimate interest of Siilo	
Message events: Topic ID (only applicable if a case is made within a conversation)	This information is used to trace the performance of our chat cases feature	Legitimate interest of Siilo	
Message events: Envelop type (normal message or new case), Quote (has a quote been used yes or no?).	This information is used to trace the performance of certain features in our applications.	Legitimate interest of Siilo	
Message events: Length of (video or voice) call	This information is created on any asynchronous messenger platform	Legitimate interest of Siilo	
Activity events: Type of activity, User ID, Installation ID, Web session ID, Client type, Siilo version, Location on the basis of IP address, Used language, User agent	This information is used to generate analytics on the performance of our applications split over versions, countries and languages, etc.	Legitimate interest of Siilo	
Registration progress	We track registration progress	Legitimate interest of Siilo	

events: Step within registration process, Status of entered data, Client type, Siilo version, Device model, Location on the basis of IP address, User ID (if registration is completed).	events to trace the performance of our registration flow and to identify issues in our registration flow by looking at drop-off points.		
Generic analytic events: User ID, Client type, Siilo version, Type of action.	We track generic analytic events to trace the performance of several of the features in our applications in different versions and over unique users.	Legitimate interest of Siilo	
Accounts events	Account events allow us to track the total amount of accounts in our system over time, divided by platform and language.	Legitimate interest of Siilo	
Name, Phone number, Email address,	Relevant to contact users for further product improvement	Legitimate interest of Siilo	Deletion after end of the contractual relationship
Siilo webchat Names (first, last) Any information shared by the User	Management of support requests sent by Users to Siilo team via the chat	Necessary for the performance of a contract to which the data subject is is a party to or for the the performance of pre-contractual measures taken at the request of request of the data subject	Deletion after the end of the contractual relationship

For security reasons, in particular to ensure the continuity of its Services, certain Personal Data may be stored by Siilo in protected backup files for seven (7) additional days. Indeed, for backup purposes, daily automated 'snapshots' are taken that are stored for no more than seven (7) days. These snapshots are encrypted at rest.

In case of restoration of these backup files, the retention periods indicated above will be automatically taken into account.

2. **Address book data**

When creating a Siilo Account, Users are offered to connect their mobile phone contact lists and/or address book to (i) indicate to them connections already using Siilo Services (ii) alert Users' connections of their arrival on Siilo Services.
By activating this feature, Users can connect and communicate with other Siilo Users and allow other Siilo Users to communicate with them.

When allowing the match, Users authorize Siilo to collect the phone numbers of User's contact lists and/or address book ("Address Book Data"). No other contact information than the phone number, such as the names that correspond with the phone numbers or email addresses, will be collected or used.

In order to do this, and to make sure Siilo gives users the most up-to-date information, Siilo will periodically check for updates to User contact lists and/or Address Book Data.

Address Book Data (if the user has given permission) is only transmitted to the server in hashed form and additionally protected using industry standard transport layer security. Only Address Book Data that has been matched will be stored (in hashed form). Address Book Data of non-users will not be stored. No Address Book Data will be given to third parties or used for advertising purposes.

Subprocessors and recipients of Personal Data

Personal Data may be transferred, for the purposes listed in this Policy, to Siilo'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.

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.
For example: when a Siilo User signs up for the App, a SMS is sent to the phone number of that User to verify that phone number. Siilo has not developed its own SMS verification service but uses software from another provider to do this. Thus, that provider processes a Siilo User's phone number on behalf of Siilo.

Siilo has contractual Data Protection Agreements with all sub-processors. Monitoring of the security and the performance of sub-processors is part of the information security management system (ISMS) policies of our ISO-27001 certification.

Cross-border transfer:

Siilo may use service providers located outside the European Union. If the transfer takes place toward a third country in which the legislation has not been recognized as providing an adequate level of protection of Personal Data, Siilo shall ensure that adequate measures are put in place in accordance with Articles 46, paragraphs 2 and 3 as well as Article 49 paragraph 1 of the GDPR, and in particular, where necessary to ensure that European Union standard contractual clauses or equivalent ad hoc clauses are incorporated into the contract between Siilo and the subsequent subcontractor.

List of Subcontractors is available in the Processor Agreement.

Cookies and Trackers

Please refer to our Cookie Information Policy.

Social networks

Link to social networks

Each User has the possibility to click on the icons dedicated to the social networks Twitter, Facebook, Linkedin, appearing on the Site or on the App. By clicking on these icons the User is redirected to external websites.

The social networks make the Site or the App more user-friendly and help promote them through sharing. Video sharing services enable the Site or the App to be enriched with video content and increase their visibility.

When the User clicks on these icons, Siilo does not collect and process any data concerning the User or the shares made by the User via Twitter, Facebook, Linkedin. These are only links referring the User to these social networks when clicking on the icons. When the User is directed to the social networks, the User's interactions and information collected by the social networks are subject to the privacy settings set by the User with each social network: Twitter - USA / Facebook - USA / Linkedin - USA.

Exercise of rights

In accordance with the GDPR, the Users have the following rights relating to their Personal Data:

- **Right of access** (Article 15 GDPR): the User may at any time access the personal information concerning him/her and held by Siilo.
- **Right of rectification** (Article 16 GDPR), and right of deletion (Article 17 GDPR): the User may request the modification or deletion of his/her Personal Data.
- **Right to object** (Article 21 GDPR): the User may object to the processing of his/her Personal Data for direct marketing purposes and/or may object to processing carried out on the basis of Siilo's legitimate interest.
- **Right to limitation of processing** (Article 18 GDPR): any User has the right ask for the limitation of the processing carried out in relation to his/her Personal Data, only when one of the following situations arises: (i) when the User disputes the accuracy of his/her data, (ii) when the User believes that the processing of his/her Personal Data is unlawful, or (iii) when the User needs such limitation for the establishment, exercise or defense of his/her legal rights.
- **Right to data portability** (Article 20 GDPR): any User has the possibility to request to retrieve the Personal Data he/she has provided to Siilo, for personal use or to transmit them to a third party of his/her choice, only when these Personal Data are subject to automated processing based on the User's consent or on a contract.
- **Right to define the fate of Users' Personal Data after their death** and to choose to whom Siilo shall communicate (or not) their Personal Data to a third party that they have previously designated.

For more information or to exercise their rights, the Users may contact Siilo in writing at the following address Siilo Holding B.V., Privacy Department, Keizersgracht 585, 1017 DR Amsterdam, The Netherlands or by email at privacy@siilo.com. In general, Siilo will respond within one (1) month to a request.

In this case, the User shall specify as much as possible which Personal Data he refers to. For deletion, access and portability requests, the User might be requested to provide a copy of an identity document (identity card or passport) or any other element allowing to justify his identity.

Users always have the right to lodge a complaint with the supervisory privacy authority in their country of residence or in the Netherlands.

Security and retention

We have taken appropriate technical and organizational measures to protect your Personal Data against loss or any form of unlawful processing. We will not retain or keep your data longer than allowed by law, required by law and/or necessary for the purposes for which the data are processed. The retention period therefore depends on the nature of the data and the purposes for which the data is processed. Retention periods may vary accordingly.

Conditions of application of the Policy

Siilo may modify, supplement or update this Policy in order to take into account any legal, regulatory, jurisprudential and/or technical developments.
In the event of significant changes (relating to the purposes of processing, the Personal Data collected, the exercise of rights, the transfer of the Professionals' Personal Data) to the terms of this Policy, Siilo undertakes to inform the Professionals at least fifteen (15) days before the effective date.
Any access to and use of the Services after this period shall be subject to the terms of the new Policy.

This Privacy Policy was last amended on February 2023.

Need to contact us?

You can contact Siilo Holding B.V.:

- with the contact form on www.siilo.com
- by e-mail to info@siilo.com or for any questions regarding the processing of your Persona Data to privacy@siilo.com.
- by mail to Siilo Holding B.V., Privacy Department, Keizersgracht 585, 1017 DR Amsterdam, The Netherlands.