Privacy Statement MattiMilo

Provided by Matti Caretech BV
Version 1.0 – September 2026

Your care. Your safety. Your data.

At MattiMilo, we believe that everyone is entitled to safe care, both for themselves and for the people they care about. MattiMilo helps clients gain greater insight into who will be providing their care, whether the care organisation has carried out the relevant checks on that care professional, how trusted persons may be involved, and how assistance may be requested more easily where something appears to be wrong or where the client feels unsafe.

Responsibility for checking a care professional does not lie with the client.

Care organisations have statutory responsibilities relating to the quality and safety of care, including, where the statutory duty to verify suitability applies, the obligation to establish before deployment that a care professional is suitable. MattiMilo does not assume that responsibility: we do not independently check or screen care professionals, nor do we request copies of diplomas, certificates, Certificates of Conduct (VOGs), identity documents or passports. MattiMilo facilitates, on behalf of the client, a request to the care organisation and makes the status of that request visible.

In order to provide these functions, MattiMilo processes personal data. In this Privacy Statement, we explain in clear language which personal data we process, why we use them, who may access them, how we protect them, and what rights you have.

Privacy at a glance

- **MattiMilo is not a medical record**. The app is not intended for entering diagnoses, medical conditions, medication, treatment plans or other medical information.
- **MattiMilo does not itself screen care professionals**. The employer and/or care organisation carries out the screening and checks and assesses whether the care professional is appropriately qualified and competent.
- **MattiMilo seeks clarification on behalf of the client** by means of an automated request to the care organisation.
- **We do not request or retain supporting documents** relating to care professionals. We record only the confirmation provided and, where relevant, an effective or expiry date.
- **Client feedback consists, as far as possible, of closed-response options**. There is no general free-text field.
- **Not everyone can see everything**. Access depends on role and permissions.
- **A signal is not a judgement**. MattiMilo does not itself determine that someone has acted improperly or that fraud has occurred.
- **We do not sell personal data** and do not use them for commercial advertising.
- **MattiMilo does not process biometric data**. Where a user makes use of biometric unlocking, those biometric data remain on the relevant iPhone or Android device and are not stored by MattiMilo.

1. When does this Privacy Statement apply?

This Privacy Statement applies to the processing of personal data through the MattiMilo app, the MattiMilo care portal, the restricted environment for care purchasers, the MattiMilo website insofar as personal data are processed there, and other digital MattiMilo services that refer to this Statement. This Statement is intended for everyone whose personal data are processed by MattiMilo.

2. Who is the data controller?

MattiMilo is provided by:

Matti Caretech BV
Chamber of Commerce number: **42117759**
Correspondence address: **Burgemeester Drijbersingel 51, 8021 JB Zwolle, the Netherlands**
General e-mail address: **contact@mattimilo.nl**
Privacy e-mail address: **privacy@mattimilo.nl**
Website: **www.mattimilo.nl**

Where MattiMilo itself determines why and how personal data are processed, Matti Caretech BV acts as the data controller within the meaning of the General Data Protection Regulation (GDPR).
For certain processing activities, a care organisation, care purchaser or other organisation involved may itself act as controller, or a different allocation of roles may apply. The precise allocation of responsibilities is determined for each processing activity and, where necessary, recorded contractually.

Data Protection Officer (DPO). MattiMilo assesses whether the appointment of a Data Protection Officer is legally required or otherwise desirable under Article 37 GDPR, taking into account the nature of the processing activities and the vulnerable target group concerned.

3. Whose personal data do we process?

Depending on the functions used, MattiMilo may process personal data relating to:

- clients;
- legal representatives;
- authorised representatives;
- contact persons and other trusted persons selected by the client;
- care professionals;
- employees of care organisations, including personnel administration and Human Resources staff;
- authorised officials who issue statements on behalf of care organisations; and
- authorised employees of care purchasers.

Not everyone has access to the same personal data.

4. How do we obtain personal data?

Personal data may be provided directly by:

- the client;
- an authorised representative;
- an appointed representative;
- a contact person;
- a care organisation; or
- another authorised user.

For example, a client may create an account, add a care appointment, invite a contact person, or answer questions after an appointment. A care organisation may provide information and statements through the care portal. During use of MattiMilo, technical data may also be generated where necessary for purposes such as authentication, security, notifications and logging.

Data received from someone other than the data subject. Some personal data are not obtained directly from the individual concerned, but for example from a care organisation, such as data relating to a care professional. In such cases, we inform the data subject about the processing and the source of the data in accordance with Article 14 GDPR, unless a statutory exemption applies.

5. Which personal data do we process?

Depending on the functions used, MattiMilo may process, among other things:

- name, contact and account details, including e-mail address, first name, birth surname, current surname where applicable, date of birth, postcode and house number;
- MattiMilo does not request the client's Dutch Citizen Service Number (BSN) for this identification purpose;
- information relating to care appointments, including the date, agreed time, relevant care organisation, relevant care purchaser and announced care professional;
- Contact Person Data, including name, e-mail address, telephone number, relationship to the Client, invitation status, and the permissions granted by Client;
- information concerning the course of and experience following a care appointment, using structured closed-response options;
- information relating to verification requests and their status;
- SOS notifications and their follow-up;
- technical security data and log data.

6. Medical data and special-category personal data

MattiMilo is not intended for collecting or recording medical or health data and is not an electronic client or patient record. We do not request diagnoses, medical conditions, medication, treatment plans, test results, or a medical description of the care provided. The input fields are designed in such a way that such information is not required. The guiding principle is that MattiMilo seeks to establish whether a care appointment took place safely and in accordance with what was agreed, rather than to record the medical substance of the care.

At the same time, we recognise that the mere fact that a person receives care may reveal information about that person's health or vulnerability. Where a processing activity involves data that may qualify as special-category personal data under Article 9 GDPR, we process such data only where a valid exception applies, generally explicit consent under Article 9(2)(a) GDPR or processing in a care context under Article 9(2)(h) GDPR, in addition to an appropriate lawful basis under Article 6 GDPR.

7. For what purposes, and on what lawful basis, do we process data?

MattiMilo processes personal data only for specified and legitimate purposes and always on the basis of a valid lawful basis under the GDPR. Not every processing activity relies on the same lawful basis, and the use of a particular function does not automatically mean that consent is the relevant legal basis.
For each processing activity, we determine: the purpose, the lawful basis, who may have access and the applicable retention period.

The overview below is indicative and will be definitively recorded in the record of processing activities.

Purpose / processing activity	Indicative GDPR lawful basis	Retention period last login
Creating, managing and authenticating an account and providing secure access	Performance of a contract (art. 6.1.b)	24 months
Recording care appointments	Performance of a contract/legitimate interests (art. 6.1.b/f)	24 months
Sending a verification request to the care organisation on behalf of the client	Consent and/or performance of a contract (art. 6.1.a/b)	24 months
Recording statements and statuses provided by care organisations	Legitimate interests / performance of a contract (art. 6.1.f/b)	24 months
Structured client feedback following a care appointment	Consent and/or legitimate interests, (art. 6.1.a/f)	24 months
Involving an authorised care purchaser in follow-up	Client consent + legitimate interests/in some cases statutory task of the care purchaser (art.6.1.a/f/c/e)	24 months
Operating the SOS and assistance function	Consent and, where applicable, vital interests (art. 6.1.a/d)	24 months
Security, prevention of misuse, logging and fraud investigation	Legitimate interests / legal obligation (art. 6.1.f/c)	24 months
Compliance with legal obligations	Legal obligation (art. 6.1.c)	Statutory period
Processing that may concern health or vulnerability	Explicit consent (art. 9.2.a), or care context (art. 9.2.h), in addition to an art. 6 lawful basis	Not applicable

Please note:

Data will be retained for a maximum of **24 months following the last login**, after which they will be deleted.

Where an active request for deletion is made, the relevant data will be retained for a maximum of **30 days** and will then be deleted, unless certain data must be retained for longer in order to comply with a legal obligation or on the basis of another valid lawful basis.

The legal bases set out above constitute a starting point and must be confirmed for each processing activity. Where we rely on **legitimate interests**, the relevant interest and the associated balancing assessment will be documented.

8. How MattiMilo works and which data are involved

Identification of the client

Where a request or notification is sent from MattiMilo on your behalf to a care organisation or care purchaser, your e-mail address, first name, birth surname, current surname where applicable, date of birth, postcode and house number may be provided to the relevant organisation. These data are used so that the organisation can check within its own records whether you are known to it as a client receiving care or as a person for whom care is being purchased or funded.

You should therefore enter your own personal details and use your name as it appears on your passport or identity card. **MattiMilo does not request your BSN for this identification purpose.**

Verification by the care organisation

If a care professional is expected to visit you, MattiMilo may send an automated verification request to the relevant care organisation on your behalf, for example to personnel administration, Human Resources, or another authorised officer. We ask the care organisation to confirm that the client and the care professional are known to the organisation, the necessary screening has been carried out, the required documents have been checked and, where applicable, remain valid and the organisation considers the care professional appropriately qualified and competent for the relevant assignment. MattiMilo records what the care organisation states, but does not independently check, verify or assess the underlying documents and does not retain copies of supporting documentation. Where relevant, an effective or expiry date may also be provided.

If the care organisation does not respond, or does not respond clearly

The absence of a response does not automatically mean that the care professional has not been screened, is unqualified, or is not competent. MattiMilo may, however, make visible that the requested confirmation has not yet been received. Where a valid legal basis and authority exist and the relevant functionality has been implemented within MattiMilo, the client may involve an authorised care purchaser in the follow-up.

The role of the care purchaser

A care purchaser may impose requirements relating to quality, screening, qualifications and competence of deployed care professionals through tendering, purchasing and contractual arrangements.
Within its own responsibilities and contractual position, the care purchaser may request information or accountability from the care organisation. A question raised by a client may give rise to such further enquiries. MattiMilo does not impose sanctions and does not itself determine that an organisation has failed to comply with its obligations. MattiMilo assists in directing the relevant question to the party that may be in a position to take further action.

Feedback after the care appointment

Following an appointment, MattiMilo may ask how the care proceeded, for example whether it was good, satisfactory or poor. Depending on the response, several follow-up questions may be asked, for example whether the care was provided respectfully and carefully, whether sufficient time was taken, and whether

the care was delivered as agreed. The client may also be asked whether the announced care professional actually attended and approximately when the appointment took place and how long it lasted.
The questions are deliberately structured. There is no general free-text field for a medical or detailed narrative report.

If someone else attended or an unexpected person is at the door

If a different care professional attends from the one announced, the client may enter the name of the person whom they believe actually provided the care. This is one of the limited situations in which free text may be entered. The field is intended exclusively for the person's name:
"Enter only the name of the care professional here." It is not intended for comments or medical information. If an unexpected person is at the door, MattiMilo may, on behalf of the client, ask the named care organisation whether that individual is associated with the relevant appointment. MattiMilo does not independently verify the person's identity, documents or qualifications and does not decide whether the person should be admitted. That decision remains with the client.

Any discrepancy between what was agreed and what occurred is treated by MattiMilo as a signal or matter for attention, not as proof of a breach. There may, for example, have been an authorised substitution.

Contact persons and people who may view information

A client may add trusted persons and decide what access they receive:

- **Emergency contact only**: receives an SOS notification, but does not automatically have access to care appointments;
- **May view**: may view care appointments and receive SOS notifications within the permissions granted;
- **May manage appointments**: may add or amend appointments on behalf of the client within the permissions granted.

Personal data relating to contact persons may include, for example first name, surname, relationship to the client, telephone number, e-mail address and the access permissions granted. The client may subsequently amend or withdraw these permissions.

A person supporting a client cannot independently link themselves to that client's account. Where a client wishes to add someone as a contact person, MattiMilo sends an invitation on behalf of the client to the e-mail address provided by the client. The invited person may follow the link in the e-mail to the MattiMilo app and accept or reject the invitation. Only after the invitation has been accepted is the contact person linked to the client. The extent of the contact person's access depends on the permissions granted by the client.

The Client may change the permissions within te app. A Contact Person cannot independently extend the permissions granted tot hem.

The Client may terminate the connection with a Contact Person at any time by removing that Contact Person within the app.

SOS and assistance

MattiMilo provides an SOS and assistance function for situations in which the client feels unsafe or wishes to obtain help quickly. When activating an SOS notification, the client selects from predefined options, for example "Someone needs to come to me" or "I would like someone to call me."; free text or medical

information is not required. The notification is sent to the persons designated in advance and, only where this has been lawfully agreed and configured, potentially to a care organisation. MattiMilo cannot guarantee that a recipient will see the notification immediately or respond immediately.

For the purpose of operating the SOS function, MattiMilo may process information such as the identity of the client, the relevant appointment (where necessary), the selected contact persons and the type of assistance requested, date and time, the recipients and the status of follow-up action. Earlier SOS notifications may be retained so that authorised persons can review what occurred.

A contact person designated by the client receives the SOS notification in the MattiMilo app on their telephone. In addition, a push notification with an audible alert may be sent to draw the contact person's attention to the incoming SOS notification. The technical data required to deliver the push notification to the relevant device are processed for this purpose.

MattiMilo does not use or share location data relating to the client or contact person as part of the SOS function.

Calling 112 directly

An SOS notification through MattiMilo is not the same as an emergency call to 112. MattiMilo is not an emergency dispatch centre and does not replace 112. In an acute emergency, the client may call 112 directly from the SOS environment.

9. Who can see which data?

MattiMilo operates on the basis of role-based access control. A client, emergency contact, viewer, authorised representative, employee of a care organisation and employee of a care purchaser each have different permissions. The guiding principle is that users may access only those personal data that are necessary and permitted for their role. A care purchaser will, in addition, obtain access only after the explicit consent of the relevant client and only to the extent necessary. Where appropriate, access is logged.

10. With whom do we share personal data?

Personal data are shared only where this is necessary for a particular function, where a valid legal basis exists, and where the recipient is authorised to receive them. Depending on the circumstances, recipients may include: the client, an authorised legal representative, an authorised contact person, the relevant care organisation, an authorised care purchaser, necessary technical service providers or authorised public authorities, supervisory bodies, inspection bodies or law-enforcement authorities. MattiMilo does not sell personal data.

Processors
Where technical service providers process personal data on behalf of MattiMilo, for example in connection with hosting, notifications, e-mail or SMS, MattiMilo enters into data processing agreements with those providers. MattiMilo maintains an overview of the processors and sub-processors it engages.

11. Where are data stored, and are data transferred outside the EEA?

Where personal data are processed outside the European Economic Area (EEA), this will take place only where permitted by the GDPR and where appropriate safeguards have been implemented, for example an adequacy decision or Standard Contractual Clauses.

12. How long do we retain personal data?

Personal data will be retained for a maximum of **24 months following the User's last login**, after which they will be deleted.

Where a User actively requests the deletion of their data, the relevant personal data will be deleted within a maximum of **30 days**, unless and to the extent that certain data must be retained for longer in order to comply with a legal obligation or on the basis of another valid lawful basis.

Where a Client removes a Contact Person, personal data associated with that contact connection will likewise be deleted within a maximum of **30 days**, unless and to the extent that a legal obligation or another valid lawful basis requires certain data to be retained for longer.

At the end of the applicable retention period, the data are deleted or, where appropriate, anonymised.

13. How do we secure personal data?

MattiMilo takes appropriate technical and organisational measures to protect personal data against loss, misuse, unauthorised access, unauthorised alteration and disclosure. These measures include appropriate attention to secure connections, authentication, role-based authorisation, encryption, logging, monitoring, backups, access management and procedures for security incidents.

Client

When a client signs in, a login link is sent to the registered e-mail address. The current configuration states that this login link remains valid for 15 minutes. The client may then set a six-digit PIN for access to the app.

Biometric unlocking

On a compatible iPhone or Android device, the client may use the biometric security features of their own device to open MattiMilo. MattiMilo does not process or retain biometric data for this purpose. The biometric data remain on the device.

Care organisation and care purchaser

Users of the care organisation portal and the restricted environment for care purchasers use a personal account protected by a password and mandatory two-factor authentication through an authenticator app. During setup, recovery codes are provided in case the user loses access to the authenticator app.

14. Logging and auditability

Because MattiMilo brings together information from different parties, auditability is important. Relevant actions may be logged, for example who signed in, who viewed or amended information, when a verification request was sent or answered, who issued a statement and events relating to authorisations and SOS notifications. Logging is used for security, auditability and the investigation of unauthorised access.

15. Signals and automated decision-making

A signal is not a judgement. MattiMilo may make visible, for example that a response is missing, an expiry date is approaching or according to the client, the care provided differed from what had been agreed. These are matters requiring attention: MattiMilo does not independently determine that fraud or a breach has occurred. Any further investigation is carried out by a person or organisation with the appropriate authority.

No solely automated decision-making. MattiMilo does not make decisions based solely on automated processing that produce legal effects concerning you or similarly significantly affect you within the meaning of Article 22 GDPR. Where necessary, a signal is reviewed by a human being before consequences are attached to it.

16. Privacy by design and privacy by default

Privacy forms part of the design of MattiMilo. We seek to process as few personal data as possible, including by using: no medical information, closed-response options wherever possible, no general free-text comment field and specific text fields limited to what is necessary for a particular function. We do not request copies of supporting documentation relating to care professionals and do not retain such copies. The guiding principle is always that no more personal data should be collected, displayed or retained than are necessary for the relevant function.

17. Minors and representation

MattiMilo may be used in situations in which the client is a minor or is otherwise represented.
In such cases, additional rules may apply concerning legal representation, consent, parental responsibility, access and privacy. A parent, family member or informal carer does not automatically gain access to all personal data solely by virtue of that relationship.

18. Cookies, analytics, notifications and technical services

When MattiMilo is used, technical data may be processed where necessary for the secure and proper operation of the platform, including IP address, device data; technical login data, push notification data and error messages. Where consent is required for non-essential technology, we will obtain that consent in advance. MattiMilo does not use personal data for commercial advertising profiling.

19. What are your privacy rights?

Depending on the circumstances, you may have the right to access your personal data, have inaccurate personal data corrected, have personal data erased, restrict processing, object to processing, receive or transfer your data through data portability and withdraw consent where the processing is based on consent. Not every right applies in every situation. This depends on the purpose and lawful basis of the processing.

Privacy requests may be sent to privacy@mattimilo.nl. We will generally respond within one month.
We may request additional information in order to verify that the request has been made by the correct person.

Rights of care professionals and others. Care professionals, contact persons and other individuals whose personal data appear in MattiMilo also have rights under the GDPR.
Where information has been provided by an employer or care organisation, it may be necessary to involve that organisation in assessing the request. We distinguish between factual information and the

observation or experience of a client. A difference of opinion does not automatically mean that anyone has acted unlawfully.

20. Terminating an account and deleting data

You may delete your MattiMilo account through **Settings** in the MattiMilo app by selecting "**Delete account**". Following deletion of your account, the personal data associated with your account will be deleted within a maximum of 30 days, unless certain data must continue to be retained due to a legal obligation or another valid lawful basis, for example for security, accountability, the establishment, exercise or defence of legal claims, or investigation of misuse.

Once there is no longer a valid legal basis for retaining such data, they will be deleted or, where appropriate, anonymised.

21. Personal data breaches and security incidents

Where a security incident involves personal data, MattiMilo investigates what has occurred and takes appropriate measures. Where required by the GDPR, we notify a personal data breach to the Dutch Data Protection Authority (Autoriteit Persoonsgegevens). Where a personal data breach is likely to result in a high risk to the rights and freedoms of individuals, we inform the affected individuals where required by the GDPR.

22. Privacy risks and DPIA

MattiMilo assesses privacy risks relating to its processing activities in advance. Where a Data Protection Impact Assessment (DPIA) is legally required, we carry one out before implementation. In doing so, we consider, among other things as vulnerable users, minors, different user roles, personal data relating to care professionals, verification, client feedback, signalling, involvement of care purchasers, SOS notifications and access management.

23. Changes to this Privacy Statement

MattiMilo continues to develop. Where functions are added or processing activities are changed, we assess whether this Privacy Statement must be amended. The date of the most recent version appears at the top of this Statement. Where changes have significant consequences for users, we will inform them in an appropriate manner.

24. Questions, requests or complaints

If you have any questions about this Statement or about how MattiMilo handles personal data, please contact:

Matti Caretech BV
Chamber of Commerce number: **42117759**
Correspondence address: **Burgemeester Drijbersingel 51, 8021 JB Zwolle, the Netherlands**
General e-mail address: **contact@mattimilo.nl**
Privacy e-mail address: **privacy@mattimilo.nl**
Website: **www.mattimilo.nl**

You also have the right to lodge a complaint with the Dutch Data Protection Authority (Autoriteit Persoonsgegevens).

25. Definitions

Client
The person receiving care who uses MattiMilo independently or with support.

Care professional
The person deployed by or on behalf of a care organisation to provide care.

Care organisation
The organisation responsible for deploying the relevant care professional.

Duty to verify suitability
The duty of a care provider, where applicable, to establish before deployment that a care professional is suitable. MattiMilo does not perform this duty on behalf of the care organisation.

Care purchaser
An organisation that purchases care and may impose requirements on contracted care organisations from its statutory, contractual or purchasing position.

Verification request
A request sent through MattiMilo on behalf of the client to a care organisation asking it to confirm relevant information concerning checks that have been carried out.

Contact person
A person added by the client. What this person may see and which notifications they receive depends on the permissions selected.

Emergency contact
A contact person who may receive an SOS notification without automatically having access to care appointments.

Authorised representative
A person authorised to perform certain actions on behalf of the client.

Screening
The checks carried out by the employer and/or care organisation when deploying a care professional. MattiMilo does not itself carry out these checks.

Qualified and competent
An assessment made by the responsible care organisation regarding the deployment of the care professional. MattiMilo does not make this assessment itself.

SOS notification
A notification activated by the client through which designated persons, or another authorised recipient where lawfully configured, may be asked for assistance.

Signal
A status, discrepancy or circumstance that may warrant further review. A signal does not constitute proof that anyone has acted improperly.

Personal data
Information relating directly or indirectly to an identifiable person.

Data controller
The party that determines why and how personal data are processed.

Processor
A party that processes personal data on behalf of a data controller.

Our privacy commitment

At MattiMilo, safe care and privacy go hand in hand. A client should be able to trust that the individuals providing care have been appropriately checked by the responsible care organisation. We do not, however, believe that a vulnerable client should then be expected personally to inspect diplomas, Certificates of Conduct, or personnel files. That responsibility does not belong to the client.

MattiMilo enables the client to initiate the checking process without having to perform the checks themselves — and the underlying supporting documents are not provided to MattiMilo.
This creates a chain of responsibility: the client can ask the question, the care organisation fulfils its responsibility, and, where necessary, the care purchaser can make further enquiries from within its own role and authority.

MattiMilo does not decide who is right, does not itself determine that fraud has occurred, does not screen care professionals, and does not assume the responsibilities of a care organisation, care purchaser, supervisory authority or emergency service.

We ensure that relevant questions, confirmations and signals are made visible and, where lawful, reach the appropriate persons.

More eyes. More ears. More safety.
MattiMilo – Strong for Care.