

Data protection policy

Published 18.02.2026

INTRODUCTION

Meliva's data protection policy describes the terms and conditions of the processing of personal data by all Meliva branded service providers. Depending on the service chosen by the customer, Meliva may impose specific conditions on the service, including the conditions for processing personal data.

Please read the data protection policy carefully and if you have any questions about how we process your personal data or if you wish to make any requests to exercise your rights in relation to the processing of your personal data, please contact us using the contact details in the contact section below.

Meliva may change this data protection policy from time to time. The current data protection policy is published on Meliva's website.

1. DEFINITIONS

"data protection policy"

This data protection policy, which describes the terms and conditions of the processing of personal data by Meliva branded service providers.

"digital clinic app"

The provision of a healthcare service or service that is delivered through the digital clinic app.

"GDPR"

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

"personal data"

Any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification code, location data, a network identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Examples of personal data are your name, personal identification number, e-mail address, health information.

"existing law"

All applicable European Union legislation and all applicable legislation of the Republic of Estonia, including, but not limited to, the Personal Data Protection Act or other national implementing legislation of the GDPR and legislation regulating

	the provision of health care services .
"patient", "client", or "data subject".	A natural person who applies or has applied to Meliva for a service.
"Meliva"	Any Meliva branded service provider. At the time of the adoption of the Privacy Policy: Meliva AS (registry code 10303948, address Rävala pst 5, 10143, Tallinn).
"Meliva's health protection"	Voluntary health insurance provided by a partner insurer of Meliva, offered to the policyholder's employees and under which Meliva provides health care to the policyholder's employees.
"service provider"	A Meliva-branded company, a Meliva employee or other representative, or a Meliva legal or natural partner used in the provision of a service and/or who is a provider of a service or healthcare.
"service"	Any service that is not a health service, such as nutritional advice, rehabilitation or any other service that is not considered a health service.
"health service"	All healthcare services provided to the client by Meliva (including the remote digital clinic service). Meliva provides various health services under the Health Services Organisation Act, for example, Meliva issues occupational health certificates under the Occupational Health and Safety at Work Act and provides other services in accordance with applicable law. A list of Meliva's services can be found at http://www.meliva.ee .
"processing"	An automated or non-automated operation or set of automated or non-automated operations on personal data or on sets of personal data, such as collection, recording, organisation, structuring, storage, adaptation and alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
"controller"	A natural or legal person, public authority, agency or other body which alone or jointly with others determines the purposes and means of the processing of personal data. For the purposes of this Data Protection Clause, the data controller of a customer's personal data is the service provider providing the service. For the purposes of this Privacy Policy , this means Meliva's service providers.

"processor"

A natural or legal person, public authority, agency or other body that processes personal data on behalf of a controller.

2. OVERVIEW

- 2.1. The data protection policy applies when you contact Meliva for a service provision.
- 2.2. The Data Protection Policy sets out the general principles of Meliva's processing of personal data.
- 2.3. Meliva ensures that patients' personal data is processed in accordance with applicable law. The most important legal acts Meliva follows when processing the personal data of its customers are the Health Care Services Organisation Act, the Health Insurance Act, the Medicinal Products Act, the Occupational Health and Safety Act, the Personal Data Protection Act and the GDPR.

3. WHEN AND FOR WHAT PURPOSES DO WE PROCESS PERSONAL DATA?

- 3.1. Meliva processes patients' personal data only for specified purposes on the basis of applicable law. A more detailed overview of the personal data processed can be found in Chapter 4.

Processing of personal data for the performance of a contract

- 3.2. If you seek healthcare from Meliva, we will process your personal data for the purpose of providing you with specific healthcare and/or preparing for the provision of healthcare. In such cases, the processing of personal data will be carried out on the basis of the Healthcare Services Act and the contract we have with you for the purpose of providing the healthcare you have ordered. We will also process your personal data for the purpose of providing healthcare if you contact us through the digital clinic App and use the digital clinic app.
- 3.3. If you contact Meliva for healthcare at the referral of your employer or another person, we will process your personal data for the purposes of providing healthcare to you and/or preparing healthcare for you under a contract with your employer or other person, the Health Services Organisation Act and the Health and Safety at Work Act.
- 3.4. When you contact Meliva for a service, we process your personal data for the purpose of providing the service you have requested. We will also process your personal data for the purposes of providing the service if you contact us through the Digital clinic app and use the digital clinic app.
- 3.5. Please note that if you have cancelled your appointment only on the day before or on the day of your visit, Meliva may have already processed your personal data in order to properly prepare for your visit. Processing of personal data for the performance of a contract may also take place, for example, in a situation where we send you a reminder of a visit.
- 3.6. For the purpose of analysing and evaluating patient satisfaction, Melia has the right to ask for your feedback on the services provided. If the patient is a minor, feedback will be sought from the patient's parent or guardian.
- 3.7. In the cases outlined in points 3.2 to 3.4, the legal basis for the processing of personal data is Article 6(1)(b) of the GDPR, i.e. the processing of personal data is necessary for the performance of a health care service or service contract relating to a client.

Processing of personal data to fulfil a legal obligation

- 3.8. We will also process personal data where it is necessary to comply with our legal obligations. For example, where Melinda requests personal data from a court on the basis of a valid court order or judgment, or where personal data are requested by a law enforcement authority on the basis of a valid regulation. Similarly, if Meliva is required to retain Personal Data under, for example, an accounting law or other applicable law. The legal basis for the processing of Personal Data for such processing is Article 6(1)(c) of the GDPR.

Processing of personal data based on consent

- 3.9. If you have given us your explicit consent to process your personal data, the legal basis for the processing of your personal data is your consent. In this case, we will process your personal data for the purposes and to the extent specified in the consent. For example, this may include marketing communications, including special offers, campaigns, health-related news, etc. Such communications may be sent via email, SMS, mobile applications or on the web, depending on which channel you have chosen. The legal basis for the processing of personal data for such processing is Article 6(1)(a) of the GDPR.
- 3.10. Please note that once you have given us your consent to process your personal data, you have the right to withdraw your consent at any time. The most convenient way to manage your consents is directly through your Meliva account, where you can see which notifications you have agreed to receive and change them at any time, including withdrawing them.

Processing of personal data based on legitimate interest

- 3.11. In certain cases, we may process personal data where it is necessary for Meliva's legitimate interest to do so. The legal basis for the processing of personal data in such cases is Article 6(1)(f) of the GDPR. We will only process personal data on the basis of legitimate interest where such processing is not overridden by the interests of the customer or the fundamental rights and freedoms for which the personal data must be protected. Processing on the basis of legitimate interest is only carried out on data which has been obtained from the data subject or which has arisen in the course of the performance of a contract. For example, we may have a legitimate interest in processing personal data where it is necessary for the establishment, exercise or defence of legal claims. Similarly, we may have a legitimate interest in processing personal data where it is necessary to ensure the technical functionality of our website. In addition, we also process personal data on the basis of a legitimate interest where it is necessary for the monitoring of quality requirements and for the supervision of the provision (documentation) of healthcare.
- 3.12. On a regular basis, but no more frequently than monthly, Meliva will use the contact details of the legal entity you provide to us to share occupational health and safety news and best practices and know-how. The representative of such a legal entity will have the right to opt-out of receiving informative communications by email or by informing their Meliva contact as set out in the guidelines.

Job applications

- 3.13. We process your personal data when you apply for a job at Meliva. Meliva processes job applicants' personal data as part of the recruitment process, for the purpose of assessing the candidate's suitability for the position offered by Meliva. In connection with the job application, Meliva processes the data that the candidate voluntarily provides in their CV and/or cover letter. If the candidate is selected, Meliva uses the data to conclude an employment contract and may request additional information if necessary.

Processing of non-personal data

- 3.14. Meliva also processes non-personalised patient data for statistical and analytical purposes, including quality assessment and the preparation of reports. Such non-personally identifiable data processed for statistical purposes include, inter alia, the nationality and/or country of residence of the patient. The data collected for statistical purposes cannot be directly or indirectly attributed to a patient.

4. AN OVERVIEW OF THE PERSONAL DATA PROCESSED

Depending on the legal relationship between you and Meliva, Meliva may process the following data about you:

Purpose	Categories of personal data collected	Personal data collected	Legal basis	Retention period
Provision of health care (documentation)	Health data (evidence of healthcare provision)	Evidence of healthcare may include, for example, a referral letter, a reply to a referral letter, a medical history, a dental card. These also contain general personal data (such as first name, surname, personal identification number) that allow the patient to be identified.	Article 6(1)(b) of the GDPR, after termination of the Agreement Article 6(1)(c) of the GDPR.	According to the Act on the Organisation of Health Care Services (Section 4 ² (4) of the Health Care Services Organisation Act), the data certifying the provision of outpatient and inpatient health care services are usually stored for 30 years from the date of confirmation of the service provided to the patient. Dental records are kept for 15 years (Section 59 ¹ (5) of the Health Care Services Organisation Act).
Provision of health care (provision of a quality service)	Health data (evidence of healthcare and other data necessary for the provision of healthcare).	Health questionnaires, declarations. Depending on the healthcare service provided, we may ask the patient to complete a health questionnaire during or before the visit, the composition of which will depend on the specific questionnaire. The health data to be processed in this case may include the history or presence of a disease, as well	Article 6(1)(b) of the GDPR, after termination of the Agreement Article 6(1)(c) of the GDPR.	Health questionnaires collected on paper are destroyed within 1 month of the visit at the latest. To the extent that the data provided in the questionnaire are necessary for documenting the provision of health care services, under the Health Care Services Organisation Act (Section 4²(4) of the Health Care Services Organisation Act), the data certifying the provision of outpatient and inpatient health care services are, as a rule, retained for 30 years from the date of confirmation of

		as information on any previous procedures.		the service provided to the patient.
Organising and providing healthcare or other services (making and managing bookings, contacting clients to provide information about services).	Identification details, contact details, health data (including health insurance data), service provision data.	Identifying information is the name, personal identification number (or, in the absence of this, date of birth). Contact details are e-mail address, telephone, address. Data relating to the provision of the service may include the time, place, content and name of the service provider (for example, which doctor the client has visited or wishes to visit), as well as information on the medicines used and clinical images taken of the client. The composition of the health data that Meliva processes in a particular case depends on the healthcare service provided. In particular, the health insurance data processed by Meliva include information on whether the customer has health insurance.	Article 6(1)(b) of the GDPR, after termination of the Agreement Article 6(1)(f) of the GDPR.	5 years from the date of the provision of the health care or service (Section 771 of Law of Obligations Act).
Offering a digital clinic app	Identification details, contact details, health data (including	Name, personal identification number, e-mail address, telephone	Article 6(1)(b) of the GDPR, after termination	According to the Act on the Organisation of Health Care Services (Section 4 ² (4) of the Health Care Services

	health insurance data), voice or video recording	number, address, details of the client's medical condition (for example, which doctor the client has visited or wishes to visit), as well as details of the medicines taken and clinical images of the client. In addition, information collected from the customer by phone, web chat or video call. The composition of the health data that Meliva processes in a particular case depends on the healthcare service provided. In particular, the health insurance data processed by Meliva include information on whether the customer has health insurance.	of the Agreement Article 6(1)(c) or Article 6(1)(f) of the GDPR.	Organisation Act), the data certifying the provision of outpatient and inpatient health care services are usually stored for 30 years from the date of confirmation of the service provided to the patient. Other data are kept for up to 5 years after the provision of the health care or service (Section 771 of Law of Obligations Act) or accounting data for 7 years (see below).
Patient satisfaction assessment	Patient feedback	Patient feedback	Article 6(1)(b) of the GDPR, after termination of the Agreement Article 6(1)(f) of the GDPR.	Feedback collected to assess patient satisfaction is kept for 1 year from the date of feedback.
Ensuring quality of service	Customer complaints and suggestions	Information related to the complaint or suggestion made by the client (health care or service number, provider information such	Article 6(1)(c) of the GDPR, after the expiry of the Agreement Article 6(1)(f) of the GDPR.	Complaints and suggestions received to ensure the quality of the service will be kept for 3 years from the date of receipt.

		as first and last name).		
Dispute resolution	Data relating to a specific dispute	Data and documents relating to the specific dispute	Article 6(1)(f) of the GDPR.	3-10 years based on the provisions of § 146(1), (4) of the Civil Procedure Code and § 771 of the LOA, depending on the specific legal dispute and its content.
Payment and billing for health care or service provision	Payment details	Billing information related to the health care or service, such as contact details, cost of the service, bank account details.	Article 6(1)(b) of the GDPR, after termination of the Agreement Article 6(1)(f) of the GDPR.	Data related to invoices are stored for up to 7 years in accordance with the Accounting Act (in particular § 12 of the RPS.
Other accounting documents	Accounting data	Documents needed to comply with a legal obligation.	Article 6(1)(c) of the GDPR.	Under the Accounting Act, we keep accounting documents for 7 years (Section 12 of the Accounting Act).
Job applications	First and last name; contact details (phone number, email address); data provided by the applicant in their CV and motivation letter (e.g., education, qualifications, further training, etc.)	Data directly provided by the job applicant to Meliva during the application process	GDPR Article 6(1)(a)	Under the Equal Treatment Act (Section § 25) and legitimate interest under the GDPR, up to 1 year after the recruitment decision.
Job applications	Publicly available sources, including information shared by the candidate in professional or public environments (e.g., LinkedIn, professional portals, public appearances or publications)	Data published by the candidate themselves, collected by Meliva from public sources	GDPR Article 6(1)(f)	Under the Equal Treatment Act (Section § 25) and legitimate interest under the GDPR, up to 1 year after the recruitment decision.
Data collected through cookies	Read separately			

5. USE OF VIDEO CAMERAS

- 5.1. Under applicable law, Meliva has the right to use surveillance equipment in its clinics for the purpose of protecting persons and property. Meliva uses video cameras in its clinics, in connection with which we also process personal data. The legal basis for the use of security cameras is legitimate interest within the meaning of Article 6(1)(f) of the GDPR. Meliva does not use video cameras in every clinic, and before deploying cameras, Meliva has carefully considered the existence of a legitimate interest as the basis for using the cameras.
- 5.2. The use of video cameras is necessary primarily to ensure the security of property and persons in Meliva's clinics, including the safety of Meliva's clients and employees. Video cameras are also used for the purpose of preventing potential violations and investigating violations after they occur.
- 5.3. Meliva's surveillance equipment consists of cameras installed in the clinics, which are stationary and do not record audio. Meliva uses cameras in common areas of the clinics, particularly near the entrances and exits.
- 5.4. Video cameras are never installed in areas where Meliva employees, clients or other persons who may enter the camera's field of view may expect complete privacy. For example, video cameras are not installed near toilets. When video cameras are in use, a sign with a camera image and/or the word "VIDEO SURVEILLANCE" is always placed in the camera surveillance area.
- 5.5. As a rule, Meliva does not transfer camera recordings to third parties, except where Meliva is entitled or obliged to do so under applicable law. For example, Meliva may transfer recordings to authorities under applicable law, for example where necessary for the investigation of offences or other incidents by persons authorised under applicable law, such as the Police and Border Guard Board.
- 5.6. Access to video camera recordings is restricted to a limited number of persons who need access strictly in connection with the performance of their duties. Meliva employees are not able to monitor the video camera feed, and recordings are only reviewed when an incident occurs that requires clarification of the circumstances by reviewing the video recordings. Meliva applies reasonable organisational and technical security measures when storing camera recordings to protect personal data from unintentional, unauthorised processing or disclosure. Camera recordings are not transferred outside the European Union.
- 5.7. Meliva retains camera recordings for up to 180 days from the date the recording was made, unless proceedings have been initiated during that period to investigate an offence or other incident that occurred during the same period, in connection with which it is necessary to retain a specific recording for a longer retention period. This retention period is necessary for the detection or investigation of possible incidents or offences that occurred during this period.
- 5.8. All Meliva employees, clients or other third parties who are at Meliva's clinics where video cameras are used and whose image has been recorded by Meliva have the right to review the recording containing their image. Meliva is unable to provide the employee or third party with the camera recording if the recording has been deleted by the time the request to review the recording is received. In addition, please note that in order to protect the rights and interests of other persons captured in the recording, we must make their image unidentifiable, which means that we cannot provide access immediately.

6. TRANSFERS OF PERSONAL DATA AND USE OF PROCESSORS

- 6.1. Meliva will not disclose your personal data to third parties, except where it has a legal right to do so under applicable law. For example, Meliva may transfer personal data to third party processors or independent controllers where the transfer is required by law or where the transfer is necessary for the provision of a service.
- 6.2. Meliva has the right under applicable law to use processors for the processing of personal data. In limited cases, Meliva's processors may process patients' personal data. Meliva will only use as processors those cooperation partners who have committed to process personal data in accordance with this data protection policy and applicable law. Meliva's processors referred to in this Chapter are not limited and Meliva may also use persons not referred to in this Chapter as processors. In particular, Meliva uses as processors various health service partners (e.g. optometrists, general practitioners or specialist partners used by Meliva to provide services to patients, as well as, for example, dental and blood laboratories), IT partners (various server service providers, IT support service providers, communication service providers, other IT service providers), marketing partners, payment service providers and other service providers or partners. In connection with the provision of the digital clinic service, Meliva uses BeeHealthy Oy as a partner to provide maintenance, data storage and technical support services for the digital clinic digital platform.
- 6.3. When providing you with health care, Meliva transfers your health data to the e-health patient portal information system located on the website <https://id.digilugu.ee/> and processed by the Centre for Health and Welfare Information Systems (registration code 70009770, address Pärnu mnt 132, 11317 Tallinn, Estonia). If you have any questions about the Patient Portal, you can contact the Health and Welfare Information Systems Centre's helpdesk on +372 794 3943 or by e-mail at abi@tehik.ee.
- 6.4. When providing healthcare to you, Meliva may transfer and/or receive your health data as necessary under applicable law through the Prescription Centre, the controller of which is the Health and Welfare Information Systems Centre (registered at 70009770, Pärnu mnt 132, 11317 Tallinn), if this is necessary for the provision of healthcare to you. If you have any questions about the Prescription Centre, you can contact the Helpdesk of the Health and Welfare Information Systems Centre on +372 794 3943 or by e-mail at abi@tehik.ee.
- 6.5. When providing healthcare to you, Meliva may transfer and/or receive your health data as necessary under applicable law through an image bank, the controller of which is the Estonian Health Care Image Bank Foundation (registered at 90007945, Puusepa 8, 51014 Tartu, Estonia), if this is necessary for the provision of healthcare to you. If you have any questions about the Image Bank, you can contact the helpdesk of the Centre for Health and Welfare Information Systems on +372 5331 8888 or by e-mail at abi@pildipank.ee.
- 6.6. When providing you with health care services in connection with the issuance of a medical certificate for drivers of motor vehicles, we may transfer your health data (medical certificate) to the digital environment of the Transport Board, the controller of which is the Transport Board (registration code 70001490, address Valge tn 4, 11413 Tallinn). If you have any questions regarding the processing of your data by the Transport Board, please contact the Transport Board by phone +372 620 1200 or by e-mail at info@transpordiamet.ee.
- 6.7. When providing you with health care, we may transfer your treatment data to the Health Insurance Fund (Tervisekassa, registration code 74000091, address Lastekodu tn 48, 10144 Tallinn) if your treatment bill is paid in part or in full by the Health Insurance Fund to health care institutions. If you have any questions about the Health Insurance Fund, you can contact the Health Insurance Fund by phone +372 669 6630 or by e-mail at info@tervisekassa.ee.
- 6.8. In certain cases, Meliva is obliged to transfer personal data under applicable law, for example to courts or law enforcement authorities on the basis of an order issued by the relevant body

under applicable law or, for example, where the transfer of personal data is mandatory under the Insurance Activities Act in connection with an inquiry made by an insurer. We may also, for example, pass on to your employer the decision of your medical examination under the Health and Safety at Work Act, but not any further health information about you or the results of any tests or analyses carried out. In addition, for example, when a health care service is provided or a prescription is renewed through the digital clinic, Meliva is required by applicable law to transfer information related to the provision of the service to the Patient Portal or the prescription center.

In all such cases, Meliva will only transfer personal data where required to do so by applicable law and in compliance with all applicable principles for the processing of personal data, including the principle of minimisation.

- 6.9. In certain cases, Meliva may also involve third parties in the processing of personal data who may be considered as independent controllers. Such independent data controllers may include insurers. Meliva will transfer personal data to the insurer only to the extent necessary for the provision of the service under Meliva's health protection, in compliance with all applicable principles for the processing of personal data, including the principle of minimality. Meliva will only transfer personal data of the customer to the insurer if the transfer of such personal data is mandatory under the Insurance Activities Act.

7. YOUR DATA SUBJECT RIGHTS

- 7.1. You have all the rights under applicable law to the processing of your personal data.

- 7.2. You have the following rights when processing personal data:

- 7.2.1. right of access: you have the right to ask Meliva at any time whether or not Meliva holds personal data about you and to be informed about what personal data Meliva is processing about you;
- 7.2.2. right to rectification of personal data: you have the right to request Melinda to clarify or rectify your personal data if it is insufficient, incomplete or incorrect;
- 7.2.3. right to object: you have the right to object to Meliva processing your personal data, for example, where Meliva has a legitimate interest in the processing of your personal data;
- 7.2.4. the right to request the deletion of personal data: you have the right to request the deletion of personal data, for example, where personal data is processed with your consent and you have withdrawn your consent;
- 7.2.5. right to restriction of processing: you have the right to request Meliva to restrict the processing of your personal data on the basis of applicable law, for example if Meliva no longer needs your personal data for the purposes of the processing or if you have objected to the processing of your personal data;
- 7.2.6. the right to withdraw your consent to the processing of personal data: where the processing of personal data is based on your consent, you have the right to withdraw your consent to Meliva at any time;

- 7.2.7. right to data portability: you have the right to obtain from Meliva, in writing or in a commonly used electronic format, personal data that you have provided to Meliva and that are processed on the basis of your consent or in performance of a contract with Meliva, and, where technically feasible, to request Meliva to transfer such data to a third party service provider;
- 7.2.8. the right to lodge a complaint: if you believe that your rights have been infringed by the processing of your personal data, you have the right to lodge a claim or complaint with the Data Protection Inspectorate or a court.
- 7.3. Your rights in relation to the processing of personal data listed in this chapter are not exhaustive. In certain cases, the rights of other data subjects or Meliva's legal obligations may limit the rights of the data subject.
- 7.4. In order to exercise your rights in relation to the processing of your personal data or to make a request in relation to the processing of your personal data, please contact us using the contact details in the "Contact" section below.

8. SECURITY OF PERSONAL DATA

- 8.1. Meliva undertakes to ensure the security of the processing of personal data in order to protect personal data against accidental or unauthorised processing, disclosure or destruction.
- 8.2. Taking into account the latest developments in science and technology and the costs of their implementation, the nature, scope, context and purposes of the processing of personal data, as well as the varying likelihood of the risks to the rights and freedoms of natural persons arising from the processing, Meliva will implement appropriate technical and organisational measures to ensure the security of personal data when processing personal data.

9. CONTACT

If you have any questions about the processing of your personal data, or if you wish to make a request regarding the processing of your personal data, please contact us by phone, email or post. You can also contact our Data Protection Officer by e-mail.

Our contact details are:

Address: Rävala pst 5, Tallinn
10143
Phone: +372 605 1550
E-mail: meliva@meliva.ee

The contact details of the Meliva's Data Protection Officer are:

E-mail: andmekaitse@meliva.ee