Privacy statement for Heltti's private customers

Updated 30.12.2024

This privacy statement provides information on the processing of personal data of private customers at Heltti in accordance with data protection legislation.

1. Data Controller

Heltti Oy (Business ID 2544593-8)
Mannerheimintie 12 A, 00100 Helsinki

The patient registry at Heltti is jointly used by Heltti and independent service providers operating at Heltti, either as self-employed professionals or through external companies.

For occupational health services, Heltti Oy acts as an independent data controller.

2. Contact Information

Data Protection Officer Juulia Kaipiainen
privacy@heltti.fi

Heltti Oy / Data Protection Officer
Mannerheimintie 12 A, 00100 Helsinki

3. Purposes and Legal Basis for Processing Personal Data

Personal data is processed for the following purposes and on the following legal bases:

- To provide occupational health services on the basis of law or consent
- To provide healthcare services on the basis of law
- To assess needs for work ability and wellness services, and to allocate and provide services on the basis of an agreement between the customer and Heltti, the law, or Heltti's legitimate interest
- To ensure the quality and conduct of healthcare professionals on the basis of the law
- For marketing and/or communication purposes on the basis of customer's consent, agreements, or Heltti's legitimate interest

- To plan, develop, manage, monitor, and report on Heltti's operations and services, as well as to ensure quality and knowledge management on the basis of law or Heltti's legitimate interest
- For research and statistical purposes on the basis of consent, law, public interest, or Heltti's legitimate interest
- To handle customer contacts, feedback, official clarification requests, and incident reports on the basis of law or Heltti's legitimate interest
- To provide digital services for logged-in customers on the basis of law, agreement between the customer and Heltti, or the customer's consent
- For billing, payment, and debt collection on the basis of law or agreement between the customer and Heltti
- To investigate and resolve technical errors in digital services (e.g. online services, applications) or devices on the basis of Heltti's legitimate interest
- To monitor user's online behavior and the use of digital services on the basis of
- legitimate interest or the customer's consent
- To ensure the legal protection of Heltti and the customers as well as to meet statutory or other obligations based on regulations and guidelines issued by authorities, to verify misuse and usage on the basis of law or legitimate interest

More details on the purposes of processing

Personal data is processed for the provision of healthcare and occupational health services relating to:

- Organizing, planning, implementing, monitoring, and supervising patient care
- Managing appointment bookings, including profiling when required by occupational health services (profiling is only implemented on the basis of customer consent)
- Evaluating the work ability of an occupational health customer.
- Planning and implementing occupational health action plans.
- Invoicing services.
- Statutory and/or group level reporting to customer organizations.
- As part of the implementation of occupational health services, Heltti may analyze health data generated in connection with a patient's healthcare service use and implementation of care in an automated manner for healthcare purposes, such as assessing the state of health, evaluating work ability needs, and promoting health (profiling).

Personal data is processed for the provision of work ability and wellbeing services relating to:

- Providing work ability coaching.
- Providing wellbeing services.

Personal data is processed to ensure the quality of healthcare professional's operations and work relating to:

- Ensuring the proper use of patient records and other personal data.

Personal data is processed for communication and marketing purposes relating to:

- Managing customer relationships, including appointment reminders, referrals, and renewals of prescriptions and vaccinations.
- Collecting, monitoring and analyzing data regarding customer interests, preferences on services and clinics, and customer satisfaction for the development of the related customer services.
- Registering and marketing loyalty program activities and benefits.
- Addressing customer preferences and tailoring offerings.
- Communicating and marketing products and services.
- Targeting communications, marketing and services
- Conducting market research and opinion surveys.
- Analyzing, profiling, segmenting, and reporting for the above purposes.

Personal data is processed for handling customer inquiries, feedback, official clarification requests and incidents relating to:

- Addressing customer contacts and feedback.
- Handling notifications and complaints pursuant to the Patient Act.
- Processing official requests for clarification.
- Processing incident reports.
- Communications between customers and Heltti's customer service may be recorded for service verification, ensuring the quality of the service, for development purposes as well as to ensure the legal protection of the parties involved.

Personal data is processed for the provision of digital services for logged-in customers (e.g. MyHeltti application and online service) relating to:

- Managing contact information and consents of a registered user and for reviewing health information.
- Receiving feedback and customer satisfaction data, as well as conducting, monitoring and analyzing research and opinion surveys.
- Managing appointments.
- Using remote services.
- Facilitating communication and information exchange between Heltti and a customer.
- Processing payments related to the use of services.
- Offering, analyzing, and marketing products and services of the data controller or its cooperation partners.
- Sending reminders and recommendations related to health.
- Collecting, monitoring and analyzing data regarding registered users' interests, preferences on services and clinics, and customer satisfaction for the development of the related customer services.

4. Categories of Personal Data Processed

Heltti may process the following categories of personal data:

- **Basic information**, such as name, personal identity number, date of birth, contact details, preferred language, occupation and other required identification information (e.g. copy of a passport), next of kin or other contact person specified by the patient, guardians or other legal representatives of underaged patients with their contact details, legal representative assigned to the patient with their contact details.
- **Health information**, including information required for purposes of organizing, planning, implementing and monitoring the treatment of the patient (e.g. patient records, photographs, video- and audio records, referrals, statements, certificates and forms); health and self-care data provided by the patient; information on laboratory tests, imaging studies, and other examinations; prescriptions and associated notes; information related to physiotherapy and occupational physiotherapy as well as information related to the employer (e.g. workplace visits)
- **Work ability data**, including information related to assessment of work ability and customer data used in work ability coaching services.
- **Wellbeing data**, such as replies to questionnaires, follow-up data and analyses; measurement data produced or submitted by the customer; information on use of wellbeing services
- **Employer information** of occupational health customers, such as department or unit, job title, superior-subordinate information, sickness fund membership, the employer's insurance company details.
- **Appointment information**, including customer information, date, time, place and the person for whom the appointment was made as well as the person who made the appointment and date of the booking, appointment history.
- **Information and recordings of customer service events**, such as communications between Heltti and the customer, telephone number of the caller, identifier of the recipient, date and time, recording of the conversation; chat recording, parties to the chat, date and time.
- **Invoicing and payment information**, such as invoicing and payment information regarding the treatment and other services; payer information regarding the treatment (e.g. insurance company and insurance information); order, payment and payer information related to online store.
- **Digital service data of logged-in users** (e.g. MyHeltti application and online service), including information on health; vaccination information; payment related information, communication between Heltti and the customer; information required for arranging remote care services; information related to the use of identification and authentication devices and services and other identification information; usage log and measures taken by the user in the digital services.
- **Information of customer contacts, feedback, official clarification requests, and incidents**, such as customer contact, feedback or clarification request and the replies to them; contact information provided by the customer or the feedback provider; and incident description and the report provided to the person concerned.

- **Other information related to the provided service**, such as name and title of the person who made the patient record as well as date and time of the recording; customer data of social care provided for purposes of organizing and implementing health service; information on customer satisfaction on certain service of the data controller; user preferences and information on services the user wishes to have; market research and opinion survey responses; contact history; information recorded from a third party register with the user's explicit consent.
- **Data related to the use of our website and digital services, online behaviour and analytics**, including access right and login information; IP address and information concerning the user's network connection; information on the user's end device, browser and operating system; session ID, timestamp and other corresponding information; information on the use of applications and other digital services (e.g. log data, data collected by using cookies and other corresponding monitoring technologies, web analytics); website behaviour during the session.
- **Consents, refusals and declarations of will**, such as consents to data sharing, and other consents and prohibitions in Kanta-service; organ donations will, living will and other declarations of will by a patient; the customer's consent and refusal information regarding direct marketing and the processing of personal data.

5. Storage time of personal data

Heltti only stores personal data that is necessary for Heltti's operations and for the purposes the personal data in question is processed and has a legal basis for the processing. Storage time is determined on the basis of the purpose the personal data in question is processed and/or the personal data in question. Storage time is also affected by legal obligations concerning storing of personal data as well as other limits for different legal actions, such as the period of filing a suit or expiration of time limit for the right to institute criminal proceedings.

Patient data is stored in accordance with the Act on Processing of Client Data in Healthcare and Social Welfare (Fi. *asiakastietolaki*, Client Data Act), mainly for a period of 12 years after the patient's death or for 120 years after the patient's date of birth.

Recordings of customer service events are in general stored for a period of six months.

Outdated and unnecessary data may be deleted or anonymized even during the customer relationship, such as data relating to marketing and use of online services. Personal data which is outdated, or no longer necessary for the purposes they were processed, or for which there is no longer a legal basis to process, is anonymised or securely destroyed.

6. Data Sources

Data is primarily collected directly from the customer, their guardians or other legal representatives, or medical staff and healthcare professionals. Data may also be collected

from events relating to the customer relationship, use of services, communications as well as provision of services.

With the patient's consent, information may also be obtained from other healthcare units or professionals, for example, through Kanta-services. Information may also be obtained from other healthcare providers on the basis of the patient's consent or law. The disclosure permissions (consents) and refusals may be managed through Kela's MyKanta service or through a healthcare service provider. The basic information of the customer may be updated from the Digital and Population Data Services Agency's Population Information System.

In occupational health care, a patient's basic information and the workplace's contact information as well as changes to them are received from the employer. Data may also be received from insurance companies or pension insurance companies.

7. Processing and Disclosure of Personal Data

The patient data recorded in Heltti's patient register is confidential, and Heltti's personnel are obligated to maintain confidentiality regarding this data.

Except for occupational healthcare services, Heltti's patient register is shared among Heltti and various service providers operating there, who act as independent practitioners or through external companies. A patient may give their consent for the disclosure of their patient data between healthcare service providers operating at Heltti who are involved in the patient's care.

The processing of personal data may be outsourced to external service providers who process personal data on behalf of Heltti. Personal data may be transferred outside the EU or EEA to the extent permitted by law. In such cases, the transfer shall be carried out using the European Commission's standard contractual clauses or other transfer mechanisms permitted by data protection legislation. The patient data systems used by Heltti are always located within the EU or EEA.

In certain situations, personal data may be disclosed to service providers acting as independent data controllers, such as providers of payment, financing, or debt collection services (e.g., MobilePay, Visma Amili Oy, Visma Payments, PayPal).

Personal data is disclosed to the following entities based on law or the customer's consent:

Kela's Kanta Services

- Patient data is stored electronically in accordance with the law in the national information system services for healthcare and social welfare maintained by Kela, such as the client data repository.
- The Information Management Service composes up-to-date patient information from patient records essential for the implementation of healthcare and produces summaries of them for the implementation of

patient care. Each healthcare service provider and Kela are joint controllers of the Information Management Service. Kela acts as the contact point for data subjects, responsible for the disclosure of data stored in the service.

- Electronic prescriptions and other information possibly related to medication are stored in the Prescription Center. Each service provider issuing electronic prescriptions, Kela, pharmacies, and other independent prescribers are joint controllers of the Prescription Center. Kela acts as the contact point for data subjects, responsible for the disclosure of data stored in the service.
- The Declaration of Will Service stores information on the information provided to the data subject in accordance with the Client Data Act and the Prescription Act, as well as the data subject's granted permissions, consents, and prohibitions regarding the disclosure of customer data. Each healthcare service provider and Kela are joint controllers of the Declaration of Will Service. Kela acts as the contact point for data subjects, responsible for the disclosure of data stored in the service.

Another healthcare service provider

- With the patient's consent or permission, patient data may be disclosed to another healthcare service provider, for example, in the case of follow-up care, or in accordance with the permissions or prohibitions of Kanta Services.
- Information necessary for the organization or implementation of the data subject's examination and treatment may also be disclosed to another Finnish or foreign healthcare unit or healthcare professional without the data subject's consent if the data subject, due to a mental disorder, intellectual disability, or other similar reason, does not have the capacity to assess the significance of the consent given and does not have a legal representative, or if consent cannot be obtained due to the data subject's unconsciousness or other similar reason.

Insurance companies

- Necessary information may be disclosed to insurance companies with the data subject's written consent or based on law.

Authorities

- Information may be disclosed to authorities or communities with a statutory right of access based on a written and individualized request in the form and extent required by the matter, or based on the customer's consent.

Next of kin

- Information may be disclosed to the data subject's guardian, other legal representative, or next of kin if the data subject has given their consent to the disclosure. However, if an underaged patient is capable of making decisions regarding their care in view of their age and level of development, they have the right to prohibit the disclosure of information concerning their health and care to their guardian or other legal representative.

- If an adult patient, due to a mental disorder, intellectual disability, or other similar reason, is unable to make decisions regarding their care, the patient's legal representative, next of kin, or other close relative has the right to receive information regarding the patient's health condition that is necessary for being heard and giving consent to important treatment decisions.
- In addition, information about the data subject and their health status may be provided to the next of kin or other close relative of the data subject who is being treated due to unconsciousness or other comparable reason, unless there is reason to believe that the data subject would prohibit such a procedure.

Research organizations

- Information contained in patient records may be disclosed to research organizations based on the consent of the individual customer in accordance with legislation.

In the case of death, the obligation of confidentiality and privacy continues, so information cannot be disclosed without explicit legislation.

Based on the Communicable Diseases Act, information necessary for the detection, investigation, and tracing of epidemics may be disclosed to the National Institute for Health and Welfare (THL) and the wellbeing services county/HUS Group.

8. Principles of Personal Data Protection

Heltti takes appropriate physical, technical, and organizational measures to protect personal data from misuse. Any manual material is stored in a locked location that is only accessible to separately authorized personnel.

Access to electronically processed material is restricted to authorized employees, practitioners, or partners through their personal username and password. Access rights are tiered, and each user is granted the minimum necessary access required to perform their duties.

Heltti carefully selects its subcontractors and ensures through contracts and other arrangements that data is also processed by subcontractors in accordance with legislation, Heltti's instructions, and good data protection practices.

9. Data Subject's Rights

Right of Access

The data subject has the right to know whether their personal data is being processed and to inspect the data concerning them. The data subject may also make a request to inspect their personal data. With regard to patient data, the data subject may also view and access their data in the OmaKanta service (kanta.fi/omakanta).

Right to Rectification and Erasure

The data subject has the right to request the rectification of inaccurate and incomplete data. Heltti must also rectify inaccurate or incomplete data on its own initiative without undue delay.

The data subject also has the right to request the erasure of their personal data. The erasure request is implemented in accordance with applicable law. In the case of health data, Heltti has a statutory obligation to retain data in accordance with the Client Data Act.

Right to Object to or Restrict Processing

In certain situations, the data subject has the right to object to the processing of their personal data on grounds relating to their particular situation.

The data subject also has the right to restrict the processing of personal data in certain situations, for example, when the data subject is awaiting Heltti's response to a request of rectification or erasure of their data. Heltti has the right to refuse the data subject's request if restricting the processing could cause a serious risk to the data subject's health or care, or to the rights of the data subject or another person.

Right Not to Be Subject to an Automated Decision-Making

The data subject has the right not to be subject to a decision based solely on automated processing, such as profiling, which produces legal effects concerning them or significantly affects them in a similar way. There are exceptions to this prohibition.

Withdrawal of Consent

If the processing of personal data is based on consent, the data subject may withdraw their consent at any time. Consent can be withdrawn in the service based on consent in the manner instructed or by contacting HelttiLinja.

Right to refer a Matter to a Supervisory Authority

The data subject has the right to refer a matter to the supervisory authority (in Finland, the Office of the Data Protection Ombudsman) if the data subject considers that the data controller has failed to comply with applicable data protection legislation. Instructions on how to file a complaint can be found on the website of the Office of the Data Protection Ombudsman: tietosuoja.fi.

Requests regarding the data subject's rights must be primarily made in writing at Heltti's office or in a digital service intended for customers through strong identification. The data subject's identity is verified in a reliable manner with each request. These measures ensure the confidentiality and appropriate handling of personal data.