DATA PROTECTION TERMS

1. GENERAL PROVISIONS

1.1. The data protection terms regulate the processing of personal data at Unimed Kliinikud OÜ (Unimed), by Unimed employees and processors. The purpose of the data protection terms is to inform Unimed patients about the processing of personal data at Unimed, including what kind of data is processed by Unimed, how this data is processed and what are the rights of the person in relation to the processing of personal data by Unimed.

1.2. The data protection terms comply with the obligation to notify a person arising from Article 12 of 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) (Regulation).

1.3. Unimed processes personal data in accordance with the principles set out in the General Data Protection Regulation, Personal Data Protection Act, Health Services Organisation Act, the guidelines of the Estonian Data Protection Inspectorate and these data protection terms.

1.4. Unimed adheres to the following principles when processing personal data:

1.4.1. Lawfulness, fairness and transparency.

1.4.2. Principle of purpose limitation – Unimed processes personal data for specified, explicit and legitimate purposes.

1.4.3. Principle of data minimisation – Unimed collects and processes only such personal data that are necessary to achieve the purpose of the processing.

1.4.4. Principle of accuracy – Unimed takes appropriate steps to ensure the accuracy of the data being processed, inaccurate and redundant data are rectified or erased at the first opportunity.

1.4.5. Principle of storage limitation – Unimed stores personal data only as long as it is necessary for the purposeful processing of personal data or to fulfil an obligation arising from law.

1.4.6. Principle of integrity and confidentiality – Unimed has adopted physical, organisational and technological security measures to ensure the lawful processing and protection of personal data.

1.5. Unimed has the right to unilaterally amend these data protection terms at any time by giving notification thereof on the Unimed website.

2. PERSONAL DATA CONTROLLER

2.1. The controller of personal data is Unimed Kliinikud OÜ,
registry code 10569340;
address Lelle 24, 11318 Tallinn;
phone number +372 677 6800; email address andmekaitse@unimed.ee.

2.2. The data protection officer at Unimed is Kristina Viznovitš, email address kristina.viznovits@pallo.ee.

3. DEFINITIONS

3.1. **Personal data** – any information relating to an identified or identifiable natural person. Personal data also includes special categories of personal data.
3.2. **Special categories of personal data** – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, health data, or data concerning a natural person's sex life or sexual orientation.
3.3. **Genetic data** – personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.
3.4. **Biometric data** – personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.
3.5. **Health data** – personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about their health status.
3.6. **Service** – services provided by Unimed such as dental care, face and jaw surgery, orthodontics and braces.
3.7. **Data subject** – a natural person whose personal data Unimed is processing. The data subjects are primarily Unimed patients and their legal representatives, as well as persons who visit the Unimed website and persons who visit the Unimed clinic, Unimed employees, employees' close relatives and job applicants, as well as Unimed contract partners who are natural persons and the employees of the contract partners.
3.8. **Patient** – a natural person to whom Unimed provides healthcare services.
3.9. **Contractual partner** – a natural or legal person who provides services to Unimed (eg accounting service provider, IT service provider etc).
3.10. **Processing (of personal data)** – any operation or set of operations which is(are) performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
3.11. **Personal data breach** – a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

4. CATEGORIES OF PERSONAL DATA BEING PROCESSED

4.1. Unimed processes the following categories of personal data:
4.1.1. data enabling the identification of a person (first and last name, personal identification code, date of birth);
4.1.2. contact details (phone number, email address, place of residence);
4.1.3. health data (patient diagnosis, performed and planned treatment, operation, examinations and their results etc);
4.1.4. data on the existence of health insurance;
4.1.5. patient profile data (gender, age);

4.1.6. network identifiers (IP addresses, cookies);
4.1.7. financial data of the patient (loans, leases, income);
4.1.8. data necessary to fulfil obligations arising from employment contract (bank account, tax data, vacation data, sick days data, name and birthday of an underage child, contact person data);
4.1.9. data necessary for recruitment (education, qualifications, hobbies, language skills);
4.1.10. personal data captured by the security camera (appearance, face image, externally visible disability etc of clinic visitors, employees, transaction partners etc).

5. SOURCES OF PERSONAL DATA

5.1. Unimed receives the personal data specified in clause 4:
5.1.1. directly from the data subject, including on site at the clinic, via phone or email;
5.1.2. directly from the data subject's legal representative, including on-site at the clinic, via phone or email;
5.1.3. from institutions and databases which Unimed employees have access to (eg Health Insurance Fund, Pildipank, health information system etc);
5.1.4. from the web browser used by the data subject;
5.1.5. from the security cameras installed in the clinic.

6. PURPOSES AND LEGAL BASIS OF PERSONAL DATA PROCESSING

6.1. Unimed provides dental care services to patients. Unimed processes the patient's contact details and health data for the purpose of providing healthcare services to the patient. The legal basis for the processing comprise Articles 6(1)(b) and Article 9(2)(a) of the Regulation and subsection 1 of § 41 of the Health Services Organisation Act. Health data is transmitted to the dental laboratory for the purpose of providing health care service to the patient and is managed in cloud-based X-ray programs. Unimed has the right to consult with another health care provider on topics regarding the patient's health. Part of the health care service provision is to remind the patient by email or SMS of the approaching appointment time if the patient has submitted these contact details to Unimed.
6.2. Pursuant to § 769 of the Law of Obligations Act, Unimed has the obligation to document the provision of health care services. For the purpose of documenting the provision of health care services, Unimed stores the patient's health data and the history of the provision of health care services in the treatment management program and transmits the data to national databases (Digilugu and Digipilt). Data related to the provision of health care services are stored for 110 years from the date of the patient's birth.
6.3. For the purpose of analysing and evaluating patient satisfaction, Unimed has the right to ask the patient for feedback on the services provided. If the patient is a minor, their parent or guardian is asked for feedback. Received feedback is stored for five years from the date of receiving the feedback.
6.4. In the event that the Estonian Health Insurance Fund takes over the obligation to pay for the provision of health care services, Unimed will provide the Estonian Health Insurance Fund with the necessary data for record keeping.
6.5. If the provision of health care service is paid for by the patient themselves or if the patient pays the appointment fee, Unimed processes the invoicing information for the purpose of enabling payment. Pursuant to the Accounting Act, invoices are stored for seven years. If it is not possible to reach a payment agreement with the patient regarding unpaid invoices, Unimed has the right to use debt collection services and for this purpose to forward the invoice information to the debt collection service provider, as well as the right to turn to qualified legal assistance (lawyer, advocate) and the court.

6.6. If Unimed is approached for data by a court or a state authority (police, prosecutor's office, security agency), Unimed is obliged to provide them with data in accordance with the requirements arising from legislation. For each request, the legal basis for the request for data release is determined.
6.7. If a person inquires from Unimed about Unimed services and discloses their personal data in the process, Unimed directs the person to an appointment with a suitable specialist to receive health care services. Inquiries and correspondence containing personal data are stored for ten years from the date of their occurrence, regardless of whether Unimed develops a medical treatment relationship with the person.
6.8. If the data necessary for the provision of the health care service is not provided, Unimed has the right to refuse to provide the service.

7. DATA PROTECTION RIGHTS OF A NATURAL PERSON

7.1. The right to access your personal data
- 7.1.1. A person has the right to receive confirmation as to whether Unimed is processing their data.
- 7.1.2. If Unimed has processed or is processing a person's personal data, the person has the right to access their personal data, including the composition of the data and the persons or categories of persons to whom the data has been transmitted.
- 7.1.3. In particular, a person has the opportunity to personally access their data processed by Unimed on the national Patient Portal Digilugu www.digilugu.ee.
- 7.1.4. If a person does not have the opportunity to access the data on Digilugu, the procedure for accessing personal data is as follows:
  - 7.1.4.1. the person submits a digitally signed application for accessing their personal data by email to andmekaitse@unimed.ee or a signed application on paper.
  - 7.1.4.2. Unimed confirms the receipt of the application and ascertains what kind of data the patient wants exactly (for example, a time period or treatment guide) and in what format does he want them (electronically or on paper).
  - 7.1.4.3. Unimed issues the personal data requested by the patient. Data on paper are handed over to the applicant personally on the basis of the patient's identity document or on the basis of a power of attorney to another person on the basis of their identity document. Electronically, the data is transmitted as encrypted to the patient's personal identification code to the email address provided by the patient or to the personal identification code of the person authorised by the patient.
  - 7.1.4.4. Unimed does not hand over data on paper format if there is a reasonable suspicion that the person who came to collect the data is not the same person as they claim to be on the basis of the identity document. In this case, Unimed issues the requested data only as electronically encrypted to the patient's personal code.
- 7.1.5. Unimed provides the first copy of the data at its own expense, and has the right to charge a reasonable fee for additional copies.

7.2. Right to data portability
- 7.2.1. A person has the right to demand the transmission of data to another personal data controller (another legal or natural person).
- 7.2.2. The procedure for transmitting data at the request of a person is as follows:
  - 7.2.2.1. A person submits a digitally signed application for the transmission of their personal data by email to andmekaitse@unimed.ee or a signed application on paper. In order to protect this right from abuse by unauthorised persons, the patient must hand over the signed application on paper personally at Unimed's place of business and must identify themselves with an identity document.
  - 7.2.2.2. The application must contain the following data of the personal data controller to whom the patient wishes to transmit their data:

name (legal or natural person); registry or personal identification code;

7.2.2.3. name, personal identification code and email address of the legal person's contact person to whom the data transfer is requested.

7.2.2.4. Unimed confirms the receipt of the application and ascertains what kind of data the patient wants exactly to be transmitted (for example, a time period or treatment guide).

7.2.2.5. Unimed transmits the requested data in an encrypted format to the personal identification code of the contact person provided by the patient to the email address provided by the patient.

7.3. Right to rectification of data

7.3.1. A person has the right to demand that Unimed rectifies inaccurate personal data concerning them, or if it is necessary based on the purpose of the processing, to complete incomplete personal data.

7.3.2. The procedure for rectification of data at the request of a person is as follows:

7.3.2.1. the person submits a digitally signed application for the rectification of their personal data by email to andmekaitse@unimed.ee or a signed application on paper. In order to protect this right from abuse by unauthorised persons, the person must hand over the signed application on paper personally at Unimed's place of business and must identify themselves with an identity document.

7.3.2.2. When submitting an application to rectify or complete data, the person is required to prove that the data about the person in Unimed's possession are inaccurate or incomplete.

7.3.2.3. Unimed confirms receipt of the application and ascertains whether the application is justified.

7.3.3. If the application is justified, Unimed will rectify or complete the patient's data.

7.4. Right to be forgotten

7.4.1. According to the Regulation, a person has the right to demand the erasure of data if:

7.4.1.1. the personal data is no longer necessary for the purpose for which it was originally collected or processed;

7.4.1.2. personal data has been processed unlawfully;

7.4.1.3. the person has objected and there are no overriding legitimate grounds for the processing to continue;

7.4.1.4. the person has prohibited data processing for direct marketing purposes; or

7.4.1.5. the obligation to erase arises from the law of the European Union or a Member State directly applicable to Unimed.

7.4.2. Regardless of the existence of a legal basis for the request for erasure, Unimed refuses to erase the data if it is necessary:

7.4.2.1. for fulfilling a task in the public interest or an obligation arising to Unimed from the law of the European Union or a Member State providing for the processing of personal data;

7.4.2.2. for reasons related to public interest in the field of public health;

7.4.2.3. for archiving, scientific or historical research or statistical purposes in the public interest; or

7.4.2.4. for preparing, presenting or defending legal claims.

7.4.3. Unimed may not erase data related to the provision of health care services, because Unimed is required to store this data under the Law of Obligations Act.

7.4.4. The procedure for erasure of data at the request of a person is as follows:

7.4.4.1. the person submits a digitally signed application for the erasure of their personal data by email to andmekaitse@unimed.ee or a signed application on paper. In order to protect this right from abuse by unauthorised persons, the person must hand over the signed application on paper personally at Unimed's place of business and must identify themselves with an identity document.

7.4.4.2. Unimed confirms receipt of the application and ascertains whether and to what extent the application is justified. If the application is justified, Unimed will erase the person's data to the extent requested and permitted by legislation.

7.5. Right to restrict the processing of data

7.5.1. A person has the right to request restriction of data processing if:

7.5.1.1. the person has contested the accuracy of the personal data, for a period that allows for the verification of the accuracy of the personal data;

7.5.1.2. the person has objected to the existence of a legitimate interest or public interest underlying the processing, for a period until the existence of a legal basis is verified;

7.5.1.3. the processing of personal data is unlawful and the person does not request erasure; or

7.5.1.4. Unimed does not need personal data for the purpose of processing, but a person needs them for the establishment, exercise or defence of legal claims.

7.5.2. The procedure to restrict the processing of one's data is as follows:

7.5.2.1. the person submits a digitally signed application for the restriction of the processing of their personal data by email to andmekaitse@unimed.ee or a signed application on paper. In order to protect this right from abuse by unauthorised persons, the person must hand over the signed application on paper personally at Unimed's place of business and must identify themselves with an identity document.

7.5.2.2. When submitting an application to restrict the processing of data, the person is required to prove that the restriction is necessary.

7.5.2.3. Unimed confirms receipt of the application and ascertains whether the application is justified.

7.5.3. If the application is justified, Unimed will restrict the processing of data in a way requested by the patient.

7.6. Right to the protection of one's rights

7.6.1. If a person finds that Unimed has violated their rights when processing personal data, they have the right to have recourse to the Estonian Data Protection Inspectorate and the court. The contact details of the Estonian Data Protection Inspectorate are as follows: phone +372 627 4135; email info@aki.ee; address Tatari 39, Tallinn 10134.

7.7. Time schedule for responding to data protection applications

7.7.1. Unimed informs the person about the measures taken at the latter's application within one month from the receipt of the application.

7.7.2. If a person submitted an application for the rectification, erasure or restriction of processing of personal data, Unimed also informs the persons to whom the personal data has been disclosed, unless this proves impossible or would require disproportionate efforts.

7.7.3. If it is not possible to fulfil the person's application within one month, Unimed may extend the deadline by two months, informing the person of the extension of the deadline and the reason for this within one month of submission of the application.

7.7.4. If Unimed does not fulfil the person's application, Unimed will provide the person with a reasoned answer of refusal within one month.

7.7.5. If Unimed has doubts about the identity of the person who submitted the application, Unimed may ask for additional information to establish the person's identity.