PRIVACY POLICY

KREATÍV-FOGKLINIKA Limited Liability Company

1141 Budapest, Vezér út 100.
1141 Budapest, Vezér út 105.
1141 Budapest, Bonyhádi utca 42.

Review date: July 31, 2024

Béla Attila Knoth
Managing Director

Table of contents

1. Introduction

The **KREATÍV-FOGKLINIKA Limited Liability Company** (registered seat: 1141 Budapest, Vezér út 100.), as controller (hereinafter referred to as the "**Controller**"), is a controller pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (EU) 2016/679 (General Data Protection Regulation) and pursuant to the Hungarian Act XLVII on the Processing and Protection of Personal Data Concerning Health and Related Matters of 1997, issues the current Privacy Policy in relation to the processing of personal data (hereinafter referred to as the "**Privacy Policy"**) to its clients, patients, visitors and website visitors interested in the Controller's services (hereinafter collectively referred to as the "**Data Subjects"**) who are interested in the services of the Controller.

The scope of the Health Data Protection Act covers

a) any organization and natural person providing healthcare services and performing professional supervision and control thereof (**healthcare network**), and any legal person, entity without legal personality or natural person processing data concerning health and personal identification data (**other data controllers**);
b) all natural persons who have been or are in contact with the healthcare network and other data controllers or who use their services, whether or not sick or healthy (**data subject**); and
c) data concerning health and personal identification data relating the data subject processed in accordance with the provisions of the currrent Act.

The Controller declares that its data processing activities are carried out in compliance with the relevant general and sectoral legal provisions and requirements, by adopting appropriate internal regulations and technical and organizational measures, and that it is committed to protecting the privacy of natural persons, including the protection of personal data or special categories of personal data that come to the knowledge of the Controller.

The primary task of the Controller is to determine the scope of personal data processed, the legal basis and purpose of data processing, the means and methods of data processing, in order to ensure compliance with the constitutional principles of data protection and the requirements of data security, to prevent unauthorized access to personal data, alteration and unauthorized disclosure of data, use of data, and in order to ensure protection against erasure, damage and destruction.

The Controller fulfils its obligation to provide information on the processing and protection of personal data in the current Privacy Policy. The regular review of the Privacy Policy, its updating, its compliance with the law and its amendment, if necessary, shall be the responsibility of the Managing Director of the Controller.

2. Governing legislation

The following laws are of particular relevance for the processing of personal data covered by the current Privacy Policy:

- 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) (hereinafter referred to as the **General Data Protection Regulation** or **GDPR**)
- Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information (hereinafter referred to as the **Informational Self-Determination Act or ISD Act**)
- Fundamental Law of Hungary (25 April 2011) (hereinafter referred to as the **Fundamental Law of Hungary**)
- Act V of 2013 on the Civil Code (hereinafter referred to as the **Civil Code**)
- Act CLIV of 1997 on Health Care (hereinafter referred to as the **Health Care Act** or **HC Act**)

- Act XLVII of 1997 on the Processing and Protection of Personal Data Concerning Health and Related Matters (hereinafter: **Health Data Protection Act or HDP Act.**)
- Act LXXXIII of 1997 on the Benefits of Compulsory Health Insurance (hereinafter referred to as the **Health Insurance Act** or **HI Act**)
- EMMI Decree No 39/2016 (XII. 21.) on the detailed rules of the National e-Health Infrastructure (hereinafter: **EESZT Decree**)
- Act C of 2000 on Accounting (hereinafter: **Accounting Act**)

3. Purpose of the Privacy Policy

The purpose of the current Privacy Policy is to provide Data Subjects with detailed, comprehensive and prior information about processing their personal data in accordance with Articles 13-14 of the GDPR.

According to Article 5(1)(a) of the GDPR, personal data must be processed fairly and lawfully and in a transparent manner for the data subject. Pursuant to Article 12 of the GDPR, the controller must take appropriate measures to provide the data subject with all information and any particulars relating to the processing of personal data in a concise, transparent, intelligible and easily accessible form, in clear and plain language.

The Controller fulfils its obligation to provide information on the processing of personal data through the current Privacy Policy. The Privacy Policy is available on the Controller's website (https://kreativdentalclinic.eu) in electronic downloadable format or in printed form at the Controller's headquarters and premises.

4. Definitions

4.1. Definitions stipulated in the GDPR

Personal data:	any information relating to the data subject.
Data subject:	an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the natural person.
Data concerning health:	personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status which include: ▪ personal data relating to the data subject which have been collected in the course of registration for or the provision of health services; ▪ a number, symbol or data allocated to the data subject for the purpose of identifying him or her individually for healthcare purposes; ▪ information obtained from the testing or examination of a body part or constituent material, including genetic data and biological samples; ▪ any information relating to, for example, the data subject's illness, disability, disease risk, medical history, clinical treatment or physiological or biomedical condition; regardless of their source, which could be a doctor or other healthcare worker, a hospital, a medical device or an in vitro diagnostic test.

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.
Biometric data:	personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.
Processing:	any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Controller:	the natural or legal person, public authority, agency or any other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Data processor:	a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.
Recipient:	a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients.
Third party:	a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data.
Consent of the data subject:	any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
Personal data breach:	a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

4.2. Definitions stipulated in the Health Care Act

Patient:	a person using or receiving health care.
Treating doctor:	the doctor or doctors who determine the plan of examination and therapy for a patient's disease or medical condition and who carry out interventions and who are responsible for the patient's medical treatment.
Health care:	a set of health care activities related to the patient's specific health condition.
Healthcare services:	the totality of healthcare activities which may be carried out under a license issued by a public health administration body or, in cases

provided for by law, on the basis of registration by a public health administration body, with the aim of preserving the health of the individual and preventing, detecting and diagnosing diseases, treatment, prevention of danger to life, improvement of the condition resulting from the disease or prevention of further deterioration of the condition, the examination and treatment of the patient, care, nursing, medical rehabilitation, reduction of pain and suffering, and the processing of the patient's examination material for the above purposes.

Healthcare provider: any individual entrepreneur, legal person or entity without legal personality authorized to provide healthcare services based on operating license issued by the public health administration regardless of the form of ownership or the person maintaining the business.

Examination: the activity aimed at assessing the patient's health condition, identifying the diseases and their risks, determining the specific disease(s), their prognosis and changes, the effectiveness of treatment, the occurrence of death and the cause thereof.

Medical records: any medical and personal identification data or information relating to a patient's treatment recorded in a notification, register or by any other means, regardless of its medium or form, which comes to the attention of a health care professional in the course of providing health care services.

Healthcare activity: any activity being a part of a health service, except for activities which do not require a health professional qualification or the professional supervision of a health professional.

4.3. Definitions stipulated in the Health Data Protection Act

Personal identification data: and personal data which identifies the data subject and which is processed by the controller together with the health-related data as part of the health record for the same purpose as, or as an integral part of, the processing of the data concerning health.

Medical treatment: any activity aimed at the preservation of health and the direct examination, treatment, care, medical rehabilitation or processing of the examination material of a person concerned for the purpose of preventing, detecting, diagnosing, treating, maintaining or correcting a disease, including the supply of medicines, medical aids, medical care, rescue and ambulance services and obstetric care.

Medical records: any medical and personal identification data or information relating to a patient's treatment recorded in a notification, register or by any other means, regardless of its medium or form, which comes to the attention of a health care professional in the course of providing health care services.

Medical confidentiality: any medical and personal identification data that have come to the knowledge of the controller in the course of treatment, as well as other data relating to necessary or ongoing treatment or treatment that has been completed, and other data obtained in connection with the treatment.

Treating doctor: the doctor or doctors who determine the plan of examination and therapy for a patient's disease or medical condition and who carry out

	interventions and who are responsible for the patient's medical treatment.
Patient care professional:	the treating doctor, the healthcare professional, the other person involved in the treatment of the patient concerned, the pharmacist.
Close relative:	the spouse, the direct relative, the adopted, step and foster child, the adopter, the step and foster parent, the brother or sister and the life partner.

5. Participants in data processing

5.1. Controller

A controller is a natural person, legal person or any other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. Basic Data of the Controller:

company name:	**KREATÍV-FOGKLINIKA Limited Liability Company**
registered seat:	1141 Budapest, Vezér út 100.
premises:	1141 Budapest, Vezér út 105. 1141 Budapest, Bonyhádi utca 42.
company registration number:	Cg. 01-09-166554
tax ID number:	10759839-2-42
represented by:	Béla Attila Knoth Managing Director
website:	www.kreativdental.eu
e-mail:	info@kreativdentalclinic.eu
phone number:	+36 1 222 0199

5.2. Data subject

For the purposes of the current Privacy Policy, data subjects are the Controller's customers, patients, visitors and website visitors interested in the Controller's services.

5.3. Data Protection Officer

Given that the Controller's main activity is the provision of outpatient healthcare (dental) services, in the course of which it obtains personal data from the data subjects and their close relatives, as well as special categories of personal data (namely data concerning health), and that the Controller obtains additional health data as a result of diagnostic tests (manual, laboratory and imaging) carried out for the provision of healthcare services, the Controller appoints a Data Protection Officer pursuant to Article 37(1)(c) of the GDPR.

Contact details of the Data Protection Officer: dpo@kreativdentalclinic.eu

5.4. Processors, recipients

In the course of processing, the Controller uses processors who process the personal data of the data subjects on behalf of the Controller. The processors are listed in point 11 and Annex 2 of the current Privacy Policy.

6. Scope of the Privacy Policy

6.1. Material scope

The material scope of the Privacy Policy covers the processing activities carried out by the Controller, except for data processing related to the employees of the Controller and to camera surveillance system, for which the Controller has created separate Privacy Policies, which shall be made available to data subjects prior to the establishment of the employment relationship and prior to access to the Controller's headquarters/premises.

6.2. Personal scope

The personal scope of the current Privacy Policy applies to natural persons. The sole entrepreneur customers and suppliers of the Controller are considered as being natural persons for the purposes of the current Privacy Policy.

7. Legal expectations regarding data processing

7.1. Clear and legitimate purposes for data processing

Personal data may only be collected for specified, explicit and legitimate purposes and may not be processed in a way incompatible with those purposes. At all stages, the processing must be compatible with the purposes for which the data are collected and processed, and the collection and processing of the data must be fair and lawful. Personal data shall be processed only in cases and to the extent necessary for the fulfilment of a legitimate purpose.

7.2. Lawfulness of the personal data processing (appropriate legal basis)

Pursuant to Article 6(1) of the General Data Protection Regulation, the processing of personal data is lawful only if and insofar as at least one of the following conditions is met:

a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
c) processing is necessary for compliance with a legal obligation to which the controller is subject;
d) processing is necessary for the protection of the vital interests of the data subject or of another natural person;
e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
f) the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where those interests are overridden by the interests or fundamental rights and freedoms of the data subject which require the protection of personal data (in particular where the data subject is a child).

The legal basis for the processing of data in the course of the Controller's activities may be:

Processing based on the consent of the data subject
[Article 6(1)(a) of the General Data Protection Regulation]
The data subject's consent is a freely given, specific, informed and unambiguous indication of his or her wishes by which you signify, by means of a declaration or an unambiguous act of affirmation, your agreement to the processing of personal data concerning you. If the processing is for more than one purpose at the same time, your consent must be given for each of the purposes for which the data are processed, and personal data will only be processed for the purposes for which you have given your consent. You have the

right to withdraw your consent at any time, but the withdrawal of consent does not affect the lawfulness of the processing prior to the withdrawal.

Processing necessary for the performance of a contract or the conclusion of a contract
[Article 6(1)(b) of the General Data Protection Regulation]
The processing is lawful if it is necessary for the performance of a contract to which you, as a data subject, are a party or if the processing is necessary to take steps at your request prior to entering into the contract.

Processing for the purposes of complying with a legal obligation to which the Controller is subject
[Article 6(1)(c) of the General Data Protection Regulation]
If the processing is carried out in the performance of a legal obligation to which the Controller is subject, in order to ensure the enforceability of that legal obligation, the processing must have a legal basis in the law of the European Union or that of a Member State.

Processing based on the legitimate interest of the Controller
[Article 6(1)(f) of the General Data Protection Regulation]
The legitimate interest of the Controller (or a third party) may provide a legal basis for processing, provided that your interests, fundamental rights and freedoms as a data subject do not override the legal interest in the processing, taking into account your reasonable expectations based on your relationship with the Controller. The Controller has carried out the necessary prior interest assessments in relation to processing based on legitimate interests and has prepared the relevant interest assessment tests, which are available at the Controller's headquarters.

7.3. Data management in accordance with the principles

Personal data are processed by the Controller in accordance with the following principles, in accordance with the General Data Protection Regulation:

a) the processing of personal data shall be lawful, fair and transparent for the data subject (**"lawfulness, fairness and transparency"**);
(b) personal data shall be collected only for specified, explicit and legitimate purposes and shall not be processed in a way incompatible with those purposes (**"purpose limitation"**);
(c) the personal data processed must be adequate, relevant and limited to what is necessary for the purposes for which they are processed (**"data minimisation"**);
(d) the personal data processed shall be accurate and, where necessary, kept up to date, and all reasonable steps shall be taken to ensure that personal data which are inaccurate for the purposes of the processing are promptly corrected or deleted by the Controller (**"accuracy"**);
(e) personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (**"storage limitation"**);
(f) personal data shall be processed in such a way as to ensure adequate security of personal data, including protection against unauthorized or unlawful processing, accidental loss, destruction or damage by implementing appropriate technical or organizational measures (**"integrity and confidentiality"**);
g) the Controller shall be responsible for compliance with the data protection principles and must be able to demonstrate compliance (**"accountability"**).

In its data management activities, the Controller also complies with the following basic provisions of the HDP Act, namely:

a) processing of personal data concerning health and personal identification data shall only be carried out for purposes specified by law;
b) for purposes other than those laid down by law, data concerning health may be processed, in whole or in part, for specific purposes only if the data subject or his or her legal representative or authorized representative has given his or her consent on the basis of adequate information, clearly expressed wishes and a credible statement of lawfulness;

c) for the purposes of processing, only so much and such health and personal identification data may be processed that is absolutely necessary for the purpose of the processing in question;
d) the security of health and personal identification data against accidental or intentional destruction, loss, alteration, damage, disclosure or access by unauthorized persons shall be ensured during the processing.

7.4. Limited period for data processing

Personal data shall be kept in a form which makes the identification of data subjects possible for no longer than is necessary for the purposes of data processing. Personal data may be processed only to the extent and for such time as is necessary for the purposes for which they are processed.

8. Processing personal data concerning health

8.1. Health data and legal basis for their processing

Special categories of personal data include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, health data and personal data concerning the sex life or sexual orientation of a natural person **(special personal data)**. As regards special categories of personal data, the Controller processes health data in the exercise of its main activities.

According to Article 9(1) of the General Data Protection Regulation, the processing of special personal data shall be prohibited, except in the cases provided for in Article 9(2):

- **the data subject has given his or her explicit consent to the processing of personal data for one or more specific purposes**, unless EU or Member State law provides that the prohibition on processing may not be lifted by the data subject's consent;
- **processing is necessary for compliance with the obligations of the controller** or the data subject **arising from legal provisions** governing employment and social security and social protection and for the exercise of his or her specific rights, where such processing is permitted by Union or Member State law or by collective agreements under national law providing adequate guarantees for the fundamental rights and interests of the data subject;
- **processing is necessary for the establishment, exercise or defense of legal claims** or when the courts are acting in their judicial role;
- **processing is necessary** for preventive health or occupational health purposes, to assess the worker's ability for work, **to make a medical diagnosis, to provide health** or social **care or treatment or to** manage health or social care systems and services, under Union or Member State law or under a contract with a health professional; for these purposes, personal data may be processed only if the processing of such data
  - is carried out by or under the responsibility of a professional **subject to the obligation of professional secrecy under** EU or Hungarian law or the rules established by the competent bodies in the Member States,
  - by another person who is **subject to a duty of confidentiality** under EU or Hungarian law or rules laid down by the competent bodies in the Member States.

8.2. Lawful purposes for processing health data

for the purposes of processing, only so much and such health and personal identification data may be processed that is absolutely necessary for the purpose of the processing in question. The purposes of processing shall be defined as follows.

Basic processing purposes

Pursuant Article 4 (1) of the HDP Act, the purposes of processing health and personal data may be: to promote the preservation, improvement and maintenance of health; to support the effective medical treatment of the patient by the health care provider, including the professional supervision; to monitor the health status of the person concerned; to take measures necessary in the interest of public health, public health and epidemiology; to enforce patients' rights; to follow the individual patient's journey.

Additional processing purposes

Article 4(2) of the HDP Act allows the processing of health and personal data also for the following purposes, among others: training of health professionals; medical-scientific and epidemiological investigation and analysis, planning, organization and cost planning of health care; statistical analysis; anonymization and scientific research for impact assessment purposes; placement and care of the data subject in a non-health care institution; for the continuous and safe supply of prescribed medicines, medical aids and medical care to persons entitled to health care; patient pathway management; assessment and development of the quality of health services, regular review and development of health services evaluation criteria; monitoring, measurement and evaluation of health system performance; enforcement of rights related to cross-border healthcare within the European Union.

For purposes other than those mentioned above, health data may only be processed in full or for specific processing activities with the explicit consent of the data subject, his or her legal representative or authorized representative, given voluntarily and with a clearly expressed and informed choice and with proof of the lawfulness of the choice.

8.3. Specific rules on health data processing

The patient has the right that information, in particular his or her medical and personal data obtained by persons involved in the provision of health care services, shall only be disclosed to the person entitled to receive it and shall be processed in accordance with the applicable legislation (medical confidentiality). The Controller and the Processor are obliged to maintain medical confidentiality. The Controller shall be exempted from the obligation of confidentiality if the transfer of the medical and personal data has been agreed in writing by the data subject or his/her legal representative within the limitations set out therein; and the transfer of the medical and personal data is required by law.

The recording of health data is part of the treatment. It is up to the treating doctor to decide which health data, in addition to the mandatory data, should be recorded in accordance with the professional rules. Other persons carrying out activities related to the treatment of the person concerned may record health data in accordance with the instructions of the treating doctor and to the extent necessary for the performance of his/her tasks.

In the case of processing for health care purposes, any health data relating to the data subject's illness which the treating doctor considers to be relevant for the purposes of treatment may be transmitted, unless the data subject has given his or her written or registered opt-out. The data subject must be informed of the current possibility before the transfer. The treating doctor shall directly inform the data subject of his or her medical data which he or she has ascertained and, unless the data subject has explicitly refused, shall transmit them to the general practitioner of the data subject's choice.

The provision of health and personal identification data by the data subject is voluntary, except for personal identification data required for the provision of health care and data required by law. In the case of a voluntary access to the healthcare network, the consent of the data subject to the processing of his/her health and personal data relating to the treatment shall be deemed to have been given, unless otherwise stated, and the data subject (legal representative) shall be informed thereof. In cases of urgency and lack of capacity of the person concerned, there should be a presumption of voluntariness.

During the treatment, apart from the doctor providing the treatment and other professionals, only those upon the patient's consent may be present. Without the consent of the data subject, and with respect for the human rights and dignity of the data subject, another person may be present only if the treatment regime requires the simultaneous treatment of several patients; the person who has previously treated the data subject for the illness concerned or to whom the head of the institution or the DPO has given authorization for professional and scientific purposes, unless the data subject has expressly objected.

When ordering medicines, medical aids and medical care, the prescription shall include the name, address, date of birth, social security number and the BNO code of the patient's disease; in the case of a prescription ordered through the National e-Health Infrastructure (EESZT), the gender of the patient and in lack of social security number, the number of the patient's identification document.

The Controller, as a healthcare provider, keeps a record of the implantation, removal and replacement of implants for the purposes of further treatment of the person concerned, monitoring of his/her health, rapid response to unexpected events and checking the suitability of the implantable medical devices, which includes the surname and first name, name at birth, date of birth, mother's name at birth, place of residence or stay, other contact details of the person concerned. The Controller shall transmit these data electronically to the Central Implant Registry at the same time as the data are entered, using the IT platform operated by the health insurance body.

8.4. Recording, storage, correction and deletion of health and personal identification data

The medical and personal data collected from the data subject for the purposes of medical treatment and their transfer shall be recorded by the Controller. The record of the transfer shall include the recipient of the transfer, the method and time of the transfer and the scope of the data transferred.

The medical records must be kept for at least 30 years from the date of recording and the final medical report for at least 50 years. After the mandatory record-keeping period, data may continue to be recorded for the purposes of medical treatment or scientific research, where appropriate. If further record-keeping is no longer appropriate, the records shall be destroyed, with regard to exceptions provided for in relevant legislation (e.g. health records of scientific interest).

Images obtained from diagnostic imaging shall be kept for 10 years from the date of its production, and diagnostic reports shall be kept for 30 years from the date of its preparation.

Incorrect health data in the medical record shall be corrected or deleted in a way that the originally recorded data can be identified.

9. Particular data processing

In Annex 1 to the current Privacy Policy, the Controller informs the data subjects in detail about the purpose, legal basis, scope of the data processed and recipients, the duration of the processing and the transfer of data.

In the case of data processing related to a legal relationship between you as a data subject and the Controller, the provision of health and personal identification data is voluntary and you are not obliged to provide your personal data. **In the event that you voluntarily contact the Controller as a healthcare provider, your consent to the processing of your health and personal identification data in relation to your medical treatment will be deemed to have been given, unless you indicate otherwise.**

Where the legal basis for the processing is your consent [Article 6(1)(a) GDPR], you may withdraw your consent at any time, but the withdrawal of consent shall not affect the lawfulness of the processing carried out on the basis of your consent prior to its withdrawal.

The provision of personal data (including sensitive personal data) is a prerequisite for the use of the Controller's services, therefore, in case of failure to provide the data, the Controller is not able to enter into a contract with you and you are not entitled to use the Controller's services. Therefore, **where the legal basis of the processing is the preparation and performance of a contract** [Article 6(1)(b) GDPR], the nature of the service means that the health service cannot be provided without the processing of personal data necessary for the use of the health service.

Where the legal basis for the processing is the legitimate interest of the controller [Article 6(1)(f) GDPR], you as the data subject may object in writing to the processing of your personal data by the controller on the basis of the legitimate interest. In such a case, the Controller may no longer process the personal data unless it can demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms or for the establishment, exercise or defense of legal claims.

10. Security of personal data

In order to comply with the principle of integrity and confidentiality, the Controller shall process personal data in such a way as to ensure adequate security thereof, including protection against unauthorized or unlawful processing, accidental loss, destruction or damage, by implementing appropriate technical or organizational measures. In this context, the Controller shall ensure the security of the personal data processed and undertakes to require any third party to whom it transfers or discloses the data, on whatever legal basis, to comply with the requirement of data security. In order to achieve data security, the Controller shall require its employees and processors to comply with the confidentiality obligation and the information security rules and applicable data protection provisions.

In order to avoid processing unnecessary data, the Controller shall ensure that the personal data processed are adequate and relevant for the purposes of the processing and that only the necessary personal data are processed, taking into account the principle of data minimization. In addition, the Controller shall ensure that the personal data are stored in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed, having regard to the principle of storage limitation.

The Controller and processors shall protect the personal data of Data Subjects against unauthorized access, loss, use or disclosure and shall ensure that personal data are processed in a secure and controlled environment.

The Controller shall implement appropriate technical and organizational measures (**data security measures**) to ensure and demonstrate that personal data are processed in accordance with the General Data Protection Regulation, taking into account the nature, scope, context and purposes of the processing (**processing context**) and the risks, of varying likelihood and severity, to the rights and freedoms of data subjects (**processing risks**). The data security measures shall be regularly reviewed and, where necessary, updated by the Controller.

12.1. Data protection by design

The Controller shall, taking into account the state of science and technology, the costs of implementation, the processing context and the processing risks, implement data security measures, both when determining the method of processing and during processing, to effectively implement the data protection principles set out in Section 5 (e.g. data minimization) and to comply with the requirements of the General Data Protection Regulation, further to incorporate into the process the necessary safeguards to protect the rights of data subjects.

12.2. Data protection by default

The Controller implements data security measures to ensure that, by default, only personal data that is necessary for the specific purpose of the processing are processed. This applies to the amount of personal data collected, the extent to which they are processed, the duration of their storage and access to personal data. The data security measures for data protection by default ensure that personal data cannot be made available to an indefinite number of persons without the intervention of the data subject.

12.3. Security of processing

The Controller shall implement appropriate data security measures, taking into account the state of science and technology, the costs of implementation, the processing context and the processing risks, in order to ensure a level of data security appropriate to the level of risk. In this context, the Controller shall, inter alia, ensure the continued confidentiality, integrity, availability and resilience of the systems and services used to process personal data; shall ensure the ability to restore access to and availability of personal data in the event of a physical or technical incident in a timely manner; and shall regularly test, assess and evaluate the effectiveness of the technical and organisational measures taken to ensure the security of processing. When determining the appropriate level of security, the Controller shall take into account the risks, arising from the processing, which may result from, amongst others, the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed.

The Controller takes the following measures to ensure that personal data processed cannot be accessed, disclosed, transmitted, modified or deleted by unauthorized persons:

- the personal data processed (with special regard to personal data concerning health) may only be disclosed to the extent and scope necessary for the purposes of the activities of the Controller, its authorized employees and the processors used for the processing;
- firewalls its IT systems to ensure their security, and uses anti-virus software to prevent external and internal data loss;
- classifies personal and health-related personal data as confidential and treats it accordingly;
- requires employees who process personal data and health data in the course of their duties to respect the confidentiality thereof;
- carries out electronic data processing and record-keeping using a software that meets the requirements of data security;
- ensures that access to the data is limited to those persons who need it for the performance of their tasks, under controlled conditions and for a specific purpose;
- ensures the security of incoming and outgoing electronic communications to protect personal data;
- stipulates that only the competent employees (administrators) have access to documents in the process of being processed;
- files containing personal data and personal data concerning health, medical records must be kept securely locked away;
- ensures adequate physical protection of data and the devices and documents that carry them;
- ensures the logging and analysis of IT systems for accesses and access attempts.

11. Data transmission, data processors

The Controller does not transfer personal data to third countries or international organizations.

In the course of its data processing activities, the Controller uses the processors listed in Annex 2, to whom personal data are transferred. The Controller keeps a record of the transfer of data.

12. Rights of the data subject

You, as the data subject, have the rights listed in the current section in relation to data processing.

12.1. Right to prior information

The Controller fulfils its obligation to provide you with prior information before starting processing the personal data in the current Privacy Policy, by providing you with the following information:

- the person and contact data of the Controller;
- the contact data of the Data Protection Officer (if any);
- the purposes and legal basis for the intended processing of personal data and the legitimate interests of the Controller (third party) in case of processing based on Article 6(1)(f) GDPR;
- the recipients of the personal data;
- the purpose of transferring personal data to a third country or to international organization and the basis and guarantees for the transfer;
- the duration of the storage of personal data;
- the content of the rights the data subject may exercise;
- the right to withdraw consent and the consequences of such withdrawal where the legal basis for processing is the data subject's consent;
- the right to file a complaint with the supervisory authority;
- if the provision of personal data is based on a legal or contractual obligation, whether the data subject is obliged to provide such personal data and the possible consequences of not providing them;
- automated decision-making and profiling (if any);
- if the personal data are not obtained from the data subject: the categories of such data processed and the source thereof.

12.2. Right of access by data subject

You shall have the right to obtain from the Controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

- the purposes of the processing;
- the categories of personal data concerned;
- the recipients or categories thereof to whom the personal data have been or will be disclosed;
- where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- the existence of the right to request from the Controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
- the right to lodge a complaint with a supervisory authority;
- where the personal data are not collected from the data subject, any available information as to their source;
- the existence of automated decision-making, including profiling, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject;
- where personal data are transferred to a third country or to an international organization, the appropriate safeguards to the transfer.

The Controller shall provide a copy of the personal data subject to the processing upon your request. The Controller may charge a reasonable fee based on administrative costs for any additional copies requested by you. The right to request a copy shall not adversely affect the rights and freedoms of others. If you have submitted the request by electronic means, the Controller will provide you with the information in electronic format, unless requested otherwise.

12.3. Right to rectification

You shall have the right to obtain from the Controller without undue delay the rectification of inaccurate personal data concerning you. Taking into account the purposes of the processing, you shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

12.4. Right to erasure

You may request the Controller to erase your personal data. The Controller shall erase the personal data concerning you without undue delay where one of the following grounds applies:

- the personal data are no longer necessary for the purposes for which they were collected;
- you object to the processing and there are no overriding legitimate grounds for the processing;
- personal data have been unlawfully processed by the Controller without a legitimate purpose or legal basis for the processing;
- the personal data must be erased in order to comply with a legal obligation to which the Controller is subject.

The Controller may refuse to comply with your request for erasure, amongst others, if the processing is necessary

- for exercising the right to freedom of expression and information;
- to comply with a legal obligation to which the Controller is subject;
- for the establishment, exercise or defense of legal claims.

12.5. Right to restriction of processing

You may request the Controller to restrict processing your personal data if

a) you contest the accuracy of the personal data (the restriction applies for the period of time that allows the Controller to verify the accuracy of the personal data);
b) the processing is unlawful, but you oppose the erasure of the personal data and request the restriction of their use instead;
c) the Controller no longer needs the personal data for the purposes of the processing, but you request them for the establishment, exercise or defense of legal claims; or
d) you have objected to the processing (the restriction applies for a period of time until it is determined whether the legitimate grounds of the Controller override your legitimate grounds).

If processing is restricted based on your request, such personal data may be processed, except for storage, only with your consent or for the establishment, exercise or defense of legal claims or for the protection of the rights of another natural or legal person. The Controller shall inform you in advance of the lifting of the restriction on processing.

12.6. Right to data portability

As a data subject, you have the right to receive personal data concerning you which you have provided to the Controller in a structured, commonly used, machine-readable format and the right to transmit such data to another controller without hindrance by the Controller, if the processing is based on consent or a contract and the processing is automated. In exercising the right to data portability, you have the right to request, where technically feasible, the direct transfer of personal data between controllers.

12.7. The right to object

As a data subject, you may object in writing to the processing of your personal data if the legal basis is the legitimate interests of the Controller or a third party. In such a case, the Controller may no longer process

the personal data unless it can demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms or for the establishment, exercise or defense of legal claims.

12.8. Right to lodge a complaint and seek judicial redress

As a data subject, you have the right to lodge a complaint with the supervisory authority or seek judicial remedy if you consider that the Controller is in breach of the law on the processing of personal data concerning you.

If you have any questions or doubts about the personal data processed by the Controller, or if you wish to obtain information about your personal data, you can do so at any time by sending an e-mail to dpo@kreativdentalclinic.eu or by post to the Controller's headquarters. We are at your disposal to clarify any issues related to the processing of your personal data and will do our utmost to clarify and resolve the situation as soon as possible.

Irrespective of the above, you have the right to contact the National Authority for Data Protection and Freedom of Information at any time (address: 1055 Budapest, Falk Miksa utca 9-11.; website: http://naih.hu; postal address: 1363 Budapest, Pf.; telephone: +36 1 391 1400; fax: +36 1 391 1410; e-mail: ugyfelszolgalat@naih.hu), if you consider that your rights have been infringed or there is an imminent threat of such infringement in connection with the processing of your personal data, in particular if you consider that the Controller is restricting the exercise of your rights under the current Privacy Policy or is refusing your request for the exercise of your rights without justification, and if the Controller or a data processor to whom it has delegated the processing of your personal data infringes the legal provisions on the processing of personal data.

You are entitled to judicial remedy if you consider that the Controller or Processor is processing your personal data in breach of the applicable legal provisions. The judicial proceedings are subject to the jurisdiction of the courts, which may, at your option, be brought before the competent court in your place of residence or domicile.

13. Measures taken at the request of the data subject

The Controller shall facilitate the exercise of your rights and shall not refuse to comply with your requests unless the Controller proves that it is unable to identify the applicant as the data subject. The Controller may, where it has reasonable doubts as to the identity of the natural person making the request, request you to provide additional information necessary to confirm your identity as the data subject.

Your requests will be examined, fulfilled and dealt with, or in certain cases rejected, within one month of the date of your request. If necessary, taking into account the complexity of your request and the number of data subjects' requests submitted to the Controller, the Controller may extend the current time limit for a further two months, which the Controller will inform you of within one month of receipt of the request.

If the Controller does not take action on your request, it will inform you without delay and at the latest within one month of receipt of the request of the reasons for the failure to act and of your right to lodge a complaint or exercise your right to judicial remedy.

If you submit your request electronically, the Controller will provide the information electronically where possible, unless you request otherwise.

The Controller shall provide information on data processing and shall comply with requests generally free of charge. Where your request is obviously unfounded or excessive, in particular because of its repetitive nature, the Controller may charge a reasonable fee, taking into account the administrative costs of providing the information or information requested or of taking the action requested, or may refuse to act on the request.

If the Controller has reasonable doubts about your identity, it may request additional information necessary to confirm your identity.

14. Handling data breaches

A data breach is a breach of security that results in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed (e.g. loss of notebook or mobile phone, unsecure storage of personal data, unsecure transmission of such data, unauthorized copying or transmission of customer and partner lists, attacks against servers). The prevention and handling of data breaches and compliance with applicable legal requirements are the responsibility of the Managing Director.

When a data breach is reported or becomes known, the administrator, with the involvement of the DPO, will immediately initiate an investigation: identify the circumstances of the data breach and determine whether it is a genuine incident or a false alert. The current should include an investigation and a determination:

- the time and place of the data breach;
- a description of the data breach, its circumstances, its effects;
- the scope and quantity of data involved in the data breach;
- the natural persons and personal data concerned by the data breach;
- a description of the measures taken to deal with the data breach;
- a description of the measures taken to prevent, remedy or reduce the damage.

In the event of a data breach, the systems, people and data involved must be contained, isolated and the evidence supporting the data breach must be collected and preserved. Damage restoration and return to lawful operations can then begin. The Controller shall keep a record of the data breaches, indicating the facts relating to the data breach, its effects and the measures taken to remedy it.

The Controller shall notify data breaches to the supervisory authority without undue delay (preferably within 72 hours of becoming aware of the breach at the latest), unless the data breach is unlikely to pose a risk to the rights and freedoms of natural persons.

If the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the Controller shall inform the data subject of the personal data breach without undue delay. The information provided to the data subject shall describe the nature of the personal data breach and shall inform the data subject of

- the name and contact details of the Data Protection Officer or other contact person who can provide further information;
- the likely consequences of a data breach;
- the measures taken or envisaged by the controller to remedy the personal data breach, including, where appropriate, measures to mitigate any adverse consequences of the personal data breach.

The data subject need not be informed of the personal data breach if:

- the Controller has implemented appropriate technical and organizational protection measures and these measures have been applied to the data affected by the personal data breach, in particular measures, such as the use of encryption, which render the data unintelligible to persons not authorized to access the personal data; or
- the controller has taken further measures following the personal data breach to ensure that the high risk to the rights and freedoms of the data subject is no longer likely to materialize; or
- the provision of information would require a disproportionate effort; in such cases, the data subjects shall be informed by means of publicly disclosed information or by a similar measure ensuring that the data subjects are informed in an equally effective manner.

If the controller has not yet notified the data subject of the personal data breach, the supervisory authority may, after having considered whether the personal data breach is likely to present a high risk, order the data subject to be informed.

15. Amendments to the Privacy Policy

The Controller reserves the right to amend or update the current Privacy Policy at any time without prior notice. The Controller will publish the Privacy Policy on its website without delay after any modification.

16. Governing language

The English version of the Privacy Policy is mainly for information purposes. In case of any question of interpretation or doubt, the Hungarian version of the Privacy Policy shall prevail.

Annex 1: Particular data processing

Name of processing	Purpose of processing	Scope of data processed / categories of data	Legal basis for processing	Source of data	Recipient / processor	Duration of processing
1. Contact						
1.1. contact via website initiated by the patient	by providing a contact form on the website, to make it possible that interested parties and prospective patients can contact the Controller in order to receive services (to make an appointment)	name, e-mail address, telephone number, other personal data and health-related data voluntarily provided by the patient	consent of the data subject GDPR 6 (1)(a) explicit consent of the data subject GDPR 9 (2)(a)	data subject	Webflow Ltd. SOS Informatika Ltd. Tiofris Bt.	until consent is withdrawn, but no later than 3 months
1.2. contact via telephone initiated by the patient	patients have the possibility to contact the Controller by telephone in order to receive services (to make an appointment)	name, telephone number, other personal data and health-related data voluntarily provided by the patient	consent of the data subject GDPR 6 (1)(a) explicit consent of the data subject GDPR 9 (2)(a)	data subject	Webflow Ltd. SOS Informatika Ltd. Tiofris Bt.	until consent is withdrawn, but no later than 3 months
1.3. contact via e-mail initiated by the patient	patients have the possibility to contact the Controller by e-mail in order to receive services (to make an appointment)	name, e-mail address, other personal data and health-related data voluntarily provided by the patient	consent of the data subject GDPR 6 (1)(a) explicit consent of the data subject GDPR 9 (2)(a)	data subject	Webflow Ltd. SOS Informatika Ltd. Tiofris Bt.	until consent is withdrawn, but no later than 3 months
1.4. contact through an agent initiated by the patient	foreign patients have the possibility to contact the Controller through a foreign regional representative (agent) in the patient's country for the purpose of receiving services (to make an appointment)	name, e-mail address, telephone number, other personal data and medical data voluntarily provided by the patient	consent of the data subject GDPR 6 (1)(a) explicit consent of the data subject GDPR 9 (2)(a)	data subject	Webflow Ltd. SOS Informatika Ltd. Tiofris Bt.	until consent is withdrawn, but no later than 6 months
1.5. contact with the patient during medical or dental hygiene treatments	maintaining contact with patients to arrange consultations, appointments, cancellations	name, e-mail address, telephone number	performance of the contract GDPR 6 (1)(b)	data subject	Webflow Ltd. SOS Informatika Ltd. Tiofris Bt.	until completion of the contract (end of treatment)
2. Registration at the Clinic						

Name of processing	Purpose of processing	Scope of data processed / categories of data	Legal basis for processing	Source of data	Recipient / processor	Duration of processing
2.1. patient registration at the clinic	at the first visit to the clinic or it has been a longer time since the previous treatment, the patient shall fill in a paper-based anamnesis form, the main purpose of which is to record the patient's data necessary for treatments	name, date of birth, mother's name, address, social security number (if any), telephone number, e-mail address, information on sensitivity to medicines, allergies, primary or infectious diseases, medical history, other voluntarily provided personal data	complying with a legal obligation to which the Controller is subject GDPR 6 (1)(c) HC Act 136.§ making a medical diagnosis and providing medical care and treatment GDPR 9 (2)(h)	data subject	Webflow Ltd. SOS Informatika Ltd. Tiofris Bt.	medical records: 30 years; final report: 50 years; diagnostic imaging: 10 years; diagnostic imaging findings: 30 years [Eüaktv. § 30]
3. Travel management						
3.1. organizing travel for patients between their place of residence and the Clinic	at the patient's request, the Controller (or the agent representing the Controller) arrange the patient's travel to Hungary and his or her return to the home country (airline ticket reservation)	name, telephone number, e-mail address, travel information, travel document number, arrival and departure times, flight number	performance of the contract GDPR 6 (1)(b)	data subject	agent SOS Informatika Ltd. Tiofris Bt.	until completion of the contract (end of treatment)
3.2. receiving patients from abroad at the airport	patient coordination, reception and transfer of patients from abroad and provision of airport assistance,	name, telephone number, arrival and departure times, flight number	performance of the contract GDPR 6 (1)(b)	data subject	SOS Informatika Ltd. Tiofris Bt.	until completion of the contract (end of treatment)
3.3. transfer service for foreign patients	transport of foreign patients between the airport and the surgery and accommodation	name, telephone number, arrival and departure times, flight number, treatment times	performance of the contract GDPR 6 (1)(b)	data subject	transfer service provider SOS Informatika Ltd. Tiofris Bt.	until completion of the contract (end of treatment)
3.4. accommodation (hotel) reservations	booking accommodation at hotels contracted with the Controller, if requested by the patient.	name, telephone number, arrival and departure times, lifestyle data	performance of the contract GDPR 6 (1)(b)	data subject	hotel service provider SOS Informatika Ltd. Tiofris Bt.	until completion of the contract (end of treatment)
4. Consultation and price quote						
4.1. personal consultation with a dentist, health check, demand assessment	a personal consultation between the dentist and the patient, during which the patient's oral health is assessed, his/her dentition, teeth and oral cavity are examined, and the treatments required by the	name, medical condition data, medical data obtained from laboratory and diagnostic imaging	complying with a legal obligation to which the Controller is subject GDPR 6 (1)(c) HC Act 136.§	data subject, treating doctor	diagnostic service provider Webflow Ltd. SOS Informatika Ltd.	medical records: 30 years; final report: 50 years; diagnostic imaging: 10 years; diagnostic imaging findings: 30 years [Eüaktv. § 30]

Name of processing	Purpose of processing	Scope of data processed / categories of data	Legal basis for processing	Source of data	Recipient / processor	Duration of processing
	patient or those medically necessary are agreed		making a medical diagnosis and providing medical care and treatment GDPR 9 (2)(h)			
4.2. preparation of treatment plan	on the basis of the assessed state of health and the patient's needs, the treating doctor draws up a treatment plan for the patient	name, details of medical condition disclosed, medical conclusions and recommendations, photographs of the denture, details of proposed treatment	complying with a legal obligation to which the Controller is subject GDPR 6 (1)(c) HC Act 136.§ making a medical diagnosis and providing medical care and treatment GDPR 9 (2)(h)	treating doctor	Webflow Ltd. SOS Informatika Ltd.	medical records: 30 years; final report: 50 years; diagnostic imaging: 10 years; diagnostic imaging findings: 30 years [Eüaktv. § 30]
4.3. preparing a price offer, acceptance of price offer	making a price offer to the patient on the basis of the treatment plan and acceptance of the price by the patient	name, details of medical condition disclosed, medical conclusions and recommendations, photographs of the denture, details of proposed treatment, payment method and payment schedule	contract preparation GDPR 6 (1)(b) making a medical diagnosis and providing medical care and treatment GDPR 9 (2)(h)	treating doctor data subject	Webflow Ltd. SOS Informatika Ltd.	5 years from the completion of the contract
4.4. verbal interpretation services during treatments at the patient's request	where necessary in the course of the services, the Controller provides interpretation services to the patient during the assessment, referral, consultation and treatment	information on medical conditions and treatment during treatment	consent of the data subject GDPR 6 (1)(a) explicit consent of the data subject GDPR 9 (2)(a)	doctor data subject	interpretation service provider	-
5. Medical and dental hygiene care						
5.1. dental treatment, aesthetic, dental hygiene treatment	the patient attends treatment according to an agreed treatment plan, for which medical data are collected and recorded in the medical record	name, medical condition data, medical data obtained from laboratory and diagnostic imaging procedures, medical conclusions and recommendations, treatment data, pre- and post-operative photographs	complying with a legal obligation to which the Controller is subject GDPR 6 (1)(c) HC Act 136.§ making a medical diagnosis and providing medical care and treatment GDPR 9 (2)(h)	data subject, treating doctor	Webflow Ltd. SOS Informatika Ltd.	medical records: 30 years; final report: 50 years; diagnostic imaging: 10 years; diagnostic imaging findings: 30 years [Eüaktv. § 30]

Name of processing	Purpose of processing	Scope of data processed / categories of data	Legal basis for processing	Source of data	Recipient / processor	Duration of processing
5.2. keeping medical records during treatments	the Controller records the data relating to the examination and treatment of the patient and the entire process of care in a medical record pursuant to § 136 of the HC Act	personal identification data, medical condition data, medical history, diagnosis, test results, diagnosed diseases, treatment data, drug sensitivity data, medical findings, treatment records, medical data obtained from laboratory and diagnostic imaging procedures, medical conclusions and recommendations, treatment data, pre- and post-intervention photographs	complying with a legal obligation to which the Controller is subject GDPR 6 (1)(c) HC Act 136.§ making a medical diagnosis and providing medical care and treatment GDPR 9 (2)(h)	data subject, treating doctor	Webflow Ltd. SOS Informatika Ltd.	medical records: 30 years; final report: 50 years; diagnostic imaging: 10 years; diagnostic imaging findings: 30 years [Eüaktv. § 30]
5.3. handling a patient's change request	the patient may change his/her needs during the course of treatment, which may require a new treatment plan (price quote) and a change in the treatment process	name, details of medical condition disclosed, medical conclusions and recommendations, photographs of the denture, details of proposed treatment	complying with a legal obligation to which the Controller is subject GDPR 6 (1)(c) HC Act 136.§ making a medical diagnosis and providing medical care and treatment GDPR 9 (2)(h)	data subject, treating doctor	Webflow Ltd. SOS Informatika Kft.	medical records: 30 years; final report: 50 years; diagnostic imaging: 10 years; diagnostic imaging findings: 30 years [Eüaktv. § 30]
5.4. ordering a medical prescription	the treating doctor may prescribe medication for the patient in connection with the treatments, for which the doctor shall include personal data on the prescription	name and surname, place of residence, date of birth, social security number (identity document number)	complying with a legal obligation to which the Controller is subject GDPR 6 (1)(c) Eüaktv. 14/A.§ making a medical diagnosis and providing medical care and treatment GDPR 9 (2)(h)	data subject	State Health Care Centre Webflow Ltd. SOS Informatika Ltd.	medical records: 30 years [30.§ Eüaktv.]
6. Diagnostic testing						
6.1. laboratory diagnostic tests	laboratory diagnostic tests may be necessary to determine the patient's treatment plan and to carry	laboratory test results as health data	complying with a legal obligation to which the Controller is subject GDPR 6 (1)(c)	treating doctor	Webflow Ltd. SOS Informatika Ltd.	medical records: 30 years; final report: 50 years; diagnostic imaging: 10 years;

Name of processing	Purpose of processing	Scope of data processed / categories of data	Legal basis for processing	Source of data	Recipient / processor	Duration of processing
	out the treatment in order to ensure that the patient receives medical care appropriate to his or her medical condition		HC Act 136.§ making a medical diagnosis and providing medical care and treatment GDPR 9 (2)(h)			diagnostic imaging findings: 30 years [Eüaktv. § 30]
6.2. diagnostic imaging tests (X-rays, CT scans)	imaging diagnostic tests (X-rays, CT scans) may be necessary to determine the patient's treatment plan and to carry out the treatment in order to ensure that the patient receives medical care appropriate to his/her medical condition	images from diagnostic imaging tests as health data	complying with a legal obligation to which the Controller is subject GDPR 6 (1)(c) HC Act 136.§ making a medical diagnosis and providing medical care and treatment GDPR 9 (2)(h)	treating doctor	Webflow Ltd. SOS Informatika Ltd.	medical records: 30 years; final report: 50 years; diagnostic imaging: 10 years; diagnostic imaging findings: 30 years [Eüaktv. § 30]
7. Billing, accounting and financial transactions						
7.1. issuing invoices, keeping supporting documents	the Controller issues an invoice to the patient on the fees of the services provided; the personal data on the invoice are processed by the Controller in order to fulfil tax declaration obligations and the obligation to keep accounting records	name, address	complying with a legal obligation to which the Controller is subject GDPR 6 (1)(c) VAT Act § 159 (1), Accounting Act § 169 (1)-(2)	data subject	accounting service provider National Tax and Customs Office Webflow Ltd. SOS Informatika Ltd.	by the end of the 8th year after the invoice is issued
7.2. handling incoming bank transfers	the patient may settle the invoices issued by the Controller by bank transfer, in which case the Controller shall keep the patient's bank account number in bank statements and analytical records in order to ensure the verification of payment obligations	name, bank account number	performance of the contract GDPR 6 (1)(b)	data subject	accounting service provider account-holding bank	5 years from the completion of the contract
7.3. processing payment transactions by credit card	the patient may settle the invoices issued by the Controller by using a credit card, in which case the	name, last four digits of credit card	performance of the contract GDPR 6 (1)(b)	data subject	accounting service provider account-holding bank	5 years from the completion of the contract

Name of processing	Purpose of processing	Scope of data processed / categories of data	Legal basis for processing	Source of data	Recipient / processor	Duration of processing
	Controller shall - in order to ensure the verification of payment obligations - process the last four digits of the patient's bank card number in his/her bank statements and analytical records				financial service provider operating a credit card terminal	
8. Complaints handling, legal claims						
8.1. handling of patient complaints	the patient has the right to lodge a complaint with the Controller in relation to the healthcare services provided, in accordance with the provisions of the HC Act; the Controller is obliged to investigate the complaint and to inform the patient in writing of the outcome thereof as soon as possible, but not later than within 30 working days	name, personal and medical data indicated in the complaint, photographs taken of the person before and after the procedure or sent by the person concerned, X-rays taken during the procedure, CT scans, medical records	complying with a legal obligation to which the Controller is subject GDPR 6 (1)(c) HC Act § 29. presentation, enforcement and defense of legal claims GDPR 9 (2)(f)	data subject	Webflow Ltd. SOS Informatika Kft.	5 years from the closure of the complaint
8.2. complaints handling, warranty claims settlement, legal claims	the patient's requests for post-treatment complaints or warranty claims can be made to the Controller in person, by telephone or by e-mail, which the Controller will assess and, if the conditions are met, will fulfil the warranty claim, or, if the conditions are not met, will reject the warranty claim	name, personal and medical data indicated in the complaint, guarantee claim, photograph taken of the data subject before and after the intervention or sent by the data subject, X-ray, CT scan, medical records taken during the treatment	legitimate interest of the controller GDPR 6 (1)(f) the legitimate interest of the Controller (complaint handling, legal proceedings or ethics procedure) is to document and prove ex post that the services received by the patient were provided in accordance with professional rules, that no professional errors were made in the provision of the services, and to whom the problem that arose ex post was attributable presentation, enforcement and defense of legal claims	data subject	Webflow Ltd. SOS Informatika Kft.	5 years from the completion of the contract

Name of processing	Purpose of processing	Scope of data processed / categories of data	Legal basis for processing	Source of data	Recipient / processor	Duration of processing
			GDPR 9 (2)(f)			
9. Mandatory reporting to public authorities						
9.1. forwarding the data on the invoice to the tax authorities (NTCA online reporting)	the Controller is obliged to transfer the data of invoices issued electronically to the National Tax and Customs Administration in accordance with the legal provisions in force	name, address	complying with a legal obligation to which the Controller is subject GDPR 6 (1)(c) 23/2014 (VI.30.) NGM Decree § 13/A.	data subject	National Tax and Customs Office Webflow Ltd. SOS Informatika Ltd.	by the end of the 8th year after the invoice is issued
9.2. mandatory data reporting to the Electronic Health Service Space (EESZT)	the Controller is obliged to provide data on the services and interventions provided to the Electronic Health Service Provider Space (EESZT) in accordance with the legal provisions in force	Social security number (or, in the absence of such number, identity document number), date of birth, sex, nationality, EESZT identifier, indication of the care event, type, date and duration, medical data relating to the intervention, medical records	complying with a legal obligation to which the Controller is subject GDPR 6 (1)(c) HDP Act § 35/F.§, 35/J., 35/K.	data subject	Webflow Ltd. State Health Care Centre	medical records: 30 years; final report: 50 years; diagnostic imaging: 10 years; diagnostic imaging findings: 30 years [Eüaktv. § 30]
9.3. registration and mandatory data reporting to the Central Implant Registry	the implantation, removal and replacement of implants for the further treatment of the person concerned, the monitoring of his/her health, the rapid response to unexpected events and the verification of the suitability of the implantable medical devices, the Controller as a healthcare provider keeps records and provides data to the Central Implant Registry	the surname and forename, name at birth, date of birth, mother's name at birth, place of residence or stay, contact details of the person concerned	complying with a legal obligation to which the Controller is subject GDPR 6 (1)(c) HC Act § 101/C., HDP Act § 22/B.	data subject	Webflow Ltd. State Health Care Centre Central implant register	50 years
10. Processing for scientific and marketing purposes						
10.1. processing of photographs related to dental procedures and services for scientific publication purposes	use photographs of the data subject before and after the treatment, preferably without revealing the face of the data subject, in order to demonstrate the medical	a photograph taken of the patient before and after the treatment (if possible, without the face and any special features)	consent of the data subject GDPR 6 (1)(a) explicit consent of the data subject	data subject	readers and viewers of the printed professional press, professional magazines, professional reports, participants in professional lectures	until consent is withdrawn

Name of processing	Purpose of processing	Scope of data processed / categories of data	Legal basis for processing	Source of data	Recipient / processor	Duration of processing
	procedures of the Controller, for scientific presentation purposes in the printed professional press, professional magazines, professional reports, professional lecture material		GDPR 9 (2)(a)			
10.2. processing of photographs related to dental procedures and services for marketing and reference purposes	use photographs taken before and after the treatment for the purposes of presenting, promoting and advertising of the Controller's services on its website, social media profiles, in the printed press, magazines and in reports	a photograph taken of the patient before and after the treatment (if possible, without the face and any special features)	consent of the data subject GDPR 6 (1)(a) explicit consent of the data subject GDPR 9 (2)(a)	data subject	visitors to the Controller's website, social media profiles, readers of the printed press, magazines, readers and viewers of reports	until consent is withdrawn
10.3. data processing on social media sites	The Controller creates its own profile on social media sites (Facebook, Instagram, TikTok) in order to provide information about its activities and services to interested parties, to present its activities, to promote its services. The Controller does not process personal data in relation to social networking sites, personal data only appears in connection with the Controller's site if the visitor of the social media profile voluntarily consents to a published material or post, and thereby places his/her personal data[1]	the name and picture of the data subject's profile and personal data voluntarily provided by the data subject on the Community site	consent of the data subject GDPR 6 (1)(a)	data subject	interested parties visiting social networking sites	until consent is withdrawn (the data subject has the right to delete the posted comment himself/herself or to request the Controller to delete it)

[1] The privacy policies of social networking sites are available at the links below:
Facebook, Messenger, Instagram (Meta): https://www.facebook.com/privacy/policy/?entry_point=data_policy_redirect&entry=0

TikTok: https://www.tiktok.com/legal/page/eea/privacy-policy/hu-HU

Annex 2: Processors, personal data transferred

Name, address of data processor	Activity carried out by the data processor	Personal data processed by a data processor
Webflow Ltd. [1117 Budapest, Bogdánfy utca 7. 3. em. 15.]	operating the Webflow Dental software, which provides IT support for the outpatient specialist care service process, and also provides an e-mail server	personal identification data, contact data, health data, health data provided by patients and generated in the course of providing services, stored in the Webflow Dental software
SOS Informatika Kft. [1162 Budapest, Csoport utca 39.]	IT and system administrator services, IT operations, server operation and maintenance, camera surveillance system operation and maintenance, IP telephone exchange operation and maintenance	personal identification data, contact data, health data, health data provided by patients and generated in the course of providing services, stored on the server, images captured by the camera system during the provision of the service
Tiofris Bt. [9027 Győr, Ipar utca 30/b. 3. em. 2.]	CRM system and website operation and maintenance	personal identification data stored in the CRM system, contact details, medical data provided by patients and those included in the treatment plan for foreign patients
Denmark: Anne Precht [Viermosevej 1DK3600 Frederikssund] **Finland**: Nina Amanpour, Kari Amanpour [Eagle Ego Oy Valokaari 10, 00750 Helsinki] **France**: Dr. Onody Consulting Kft. [1055 Budapest, Falk Miksa utca 6. II. emelet 4B. ajtó] / Kreativ Dental Clinic Belgique-France-Suisse / 798 281 358 R C S Nanterre, Sirene: 798 281 358 / Siret:798 281 358 00019, 10 rue Penthieve 75008 Paris] **Germany**: René Herrmann, Kreativ Dental Serviceagentur Herrmann & Sieradz GbR [Ursula str. 5. 67434 Neustadt, Deutschland] **Icelad**: Grímur Axelsson [1132 Budapest, Visegrádi u. 18A] **ireland**: Mary Flanagan, Kreativ Dental Ireland [Clontarf, Dublin 3 Ireland]	as a foreign representative of the Controller, provides information to prospective and existing patients about the services of the Controller, maintains contact with them, participates in the organization of travels, and in the complaint handling process in the event of a patient's enquiry	name, telephone number, e-mail address, travel-related data, health data voluntarily provided by the data subject (only for contacts from the country of activity)
EDIMART Tolmács- és Fordítóiroda Kft. [1061 Budapest, Király u. 14. 3/1.]	interpretation and translation services for the services used	personal and health data related to the treatment and information changed during the treatments
Úri Sándor [2373 Dabas, Kossuth Lajos út 106.] **Ódor László** [1195 Budapest, Kossuth Lajos u. 29.] **Müller Péter** [2315 Szigethalom, Petőfi utca 11/a.] **Rózsa Sándor** [1171 Budapest, Nagyszentmiklósi út 42.]	patient transport between the airport, accommodation and the surgery	name, travel details, accommodation data, dates of treatments
Danubius Hotel Aréna [1148 Budapest, Ifjúság útja 1-3.] **Danubius Hotel Hélia** [1133 Budapest, Kárpát u. 62-64.]	providing hotel services for patients	name, phone number, e-mail address, arrival and departure times, special lifestyle information (food sensitivities, other requests)
State Health Care Centre [1085 Budapest, Horánszky u. 15.]	Operation of the Electronic Health Service Space (EESZT), registration of health data in accordance with the provisions of the Eüaktv.	personal data on a medical prescription, personal and medical data in medical records
Central Implant Register [https://impreg.neak.gov.hu/]	record data on implant procedures in case of urgent need for intervention, rapid response to unexpected events	the surname and forename, name at birth, date of birth, mother's name at birth, place of residence or stay, contact details of the person concerned

Name, address of data processor	Activity carried out by the data processor	Personal data processed by a data processor
Tax Advisor Agency Kft. [1051 Budapest, Hercegprímás utca 11. 2/1.]	accounting and payroll services	information on the invoice: first name and surname (billing name), place of residence (billing address), e-mail address (if the invoice is sent electronically)
National Tax and Customs Office [1054 Budapest, Széchenyi utca 2.]	state taxation tasks	information on the invoice: surname and first name (billing name), place of residence (billing address)
CIB Bank Zrt. [1024 Budapest, Petrezselyem utca 2-8.]	banking services, making and receiving transfers, credit card terminal services	name, bank account number, last four digits of the credit card
UniCredit Bank Zrt. [1054 Budapest, Szabadság tér 5-6.]	credit card terminal service	name, last four digits of credit card
Dr. Koletár András Kázmér Law Firm [1118 Budapest, Budaörsi út 62.]	legal representation	data necessary for the exercise of legal representation, the exercise of legal claims or the handling of complaints
Dr. Sándor Lilian Law Firm [1039 Budapest, Hollós Korvin Lajos u. 13. 3/10.]	acting as Data Protection Officer, responding to requests from data subjects, liaising with the data protection authority, responding to requests from the authority	personal data necessary to comply with a request from a data subject or a public authority