GENERAL DATA MANAGEMENT INFORMATION

1 DATA CONTROLLER DETAILS, CONTACT DETAILS:

1.1 Supplier: DENTAL PALACE Limited Liability Company

Company registration number: Cg.: 01-09-912523

Headquarters: 1037 Budapest, Toboz utca 6.

TAX number: 14627000-2-41

Tel.: 061/250 9086

E-mail: info@dentalpalace.hu

2 GENERAL INFORMATION

2.1 The purpose of health data management:

The purpose of the processing of health and personal identification data (Section 4 (1) of the Eüak Act):

- promoting the preservation, improvement and maintenance of health,
- promoting the patient's effective treatment activities, including specialist supervision,
- monitoring the health status of the person concerned,
- taking measures necessary in the interests of public health, public health and epidemiology,
- enforcement of patients' rights
- transmission of data to social security in the case of an OEP-funded service.

Health and personal identification data can be found on Eüak tv. Pursuant to Section 4 (2), in addition to the above, in the cases specified by law, it may be treated for the following purposes:

- training of health professionals,
- medical-professional and epidemiological examination, analysis, planning and organization of health care, cost planning,
- statistical analysis,
- nonymisation for impact assessment, scientific research,

- the work of organizations carrying out official or legality control, professional or legality supervision of the body or person handling health data elősegítése, ha az ellenőrzés its purpose cannot be achieved in any other way and to perform the tasks of organizations financing health care,
- determination of social security or social benefits, if it is based on health status,
- examining the ordering and provision of services available to those entitled to health care at the expense of compulsory health insurance and compliance with the rules for ordering economical medical aids and medical care,
- in addition, the financing of the benefits provided to the beneficiaries on the basis of a contract according to a separate legal regulation, and the settlement of the price subsidy,
- law enforcement, as well as Act XXXIV of 1994 on the police. crime prevention within the scope of authorization to perform tasks specified by law,
- Act CXXV of 1995 on National Security Services. performing tasks specified by law,
- infringement proceedings,
- prosecution proceedings,
- court proceedings,
- placement and care of the data subject in a non-medical institution,
- determination of fitness for work, regardless of whether this activity:
    - employment,
    - civil servant and civil service legal relationship,
    - in the course of a professional or other employment relationship,
- determining the suitability for education or training for public education, higher education and vocational training,
- determination of suitability for military service or fulfillment of personal defense obligations,
- unemployment benefits, employment promotion and related control.

For purposes other than those set out above, health and personal data may be processed with the written consent of the data subject or his or her legal or authorized representative (hereinafter together: the legal representative), based on appropriate information. For the purposes of data processing defined above, only as much and such health or personal data as are strictly necessary for the fulfillment of the purpose of data processing may be processed.

2.2 Legal basis for data management:

The legal basis for data management is the Eüak Act and the Eü Act. and 39/2016. (XII. 21.) of the EMMI (Article 6 (1) of the GDPR) fulfillment of a legal obligation under point (c).

Otherwise, performance of the contract with the Data Controller as a healthcare provider pursuant to Article 6 (1) (b) of the GDPR Regulation.

The data management of e-mail addresses managed for the purpose of subscribing to the newsletter is based on the consent of the data subject, while the legal basis of the use of cameras located in the Data Controller's office is the Data Controller's legitimate interest in property security under Article 6 (1) (f) GDPR.

2.3 Definitions:

Data subject: a natural person who has come into contact with or comes into contact with the Data Controller or uses its services, regardless of whether he or she is ill or healthy.

Health data: information on the physical, mental and mental condition, pathological condition of the person concerned, the circumstances of illness or death, the cause of death, communicated by him or her or by another person, or detected, examined, measured or imaged by the health care network. derived data; and any data that may be related to the above and that affect them (eg behavior, environment, occupation).

Personal identification data: surname and first name, maiden name, sex, place and time of birth, mother's maiden name and forename, place of residence, place of residence, social security number (hereinafter: TAJ number) together or any of these , if it is or may be suitable for the identification of the data subject.

Therapeutic treatment: any activity aimed at the direct examination, treatment, care, medical rehabilitation or, in order to prevent including the processing of medicines, medical aids, spa care, rescue and ambulance services, and obstetric care.

Medical secret: health and personal data that came to the attention of the data controller during the treatment, as well as other information about the required or ongoing or completed treatment, as well as other information about the treatment.

Medical records: records, records or any other recorded information, regardless of its medium or form, containing medical and personally identifiable information that comes to the care of the patient during treatment.

Patient caregiver: the doctor performing the treatment, the health care professional, any other person performing activities related to the treatment of the person concerned.

Health care network: an organization and a natural person that provides health care and carries out its professional supervision and control.

Close relative: spouse, direct relative, adopted, stepchild and foster child, adoptive parent, stepfather and foster parent, and brother and partner.

Third party: any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor or persons who have been authorized to process personal data under the direct control of the controller or processor.

Urgent need: a sudden change in his or her state of health which, in the absence of immediate health care, would put the person concerned in immediate danger of life or cause serious or permanent damage to his or her health.

Data Management: Any operation or set of operations on personal data or files, whether automated or non-automated, such as collecting, recording, organizing, sorting, storing, transforming or altering, retrieving, viewing, using, communicating, transmitting, distributing or otherwise harmonization, interconnection, restriction, deletion or destruction.

Data processing: the performance of technical operations related to data management operations, regardless of the method and means used to perform the operations and the place of application.

Data transfer: when the data is made available to a specific third party.

Media: any material or device capable of recording, storing and retrieving data.

Data controller: The healthcare provider, its manager, the staff employed by the service provider, who alone or together with others is entitled to process health and related personal or personal data for data processing purposes, and who determines the purpose of data processing, including the device used) and implements it with the data controller.

Data processor: a natural or legal person, an organization without legal personality, who, or on behalf of the data controller, also processes personal data on behalf of the data controller.

2.4 Managed data sets

2.4.1 Providing appointments, contact and information transfer:

Appointment, dental treatment, advance notification via email and phone, SMS date notification.

Legal basis for data management: Consent of the data subject

Scope of data managed:

- Name
- Permanent address
- Phone
- E-mail address,
- Type of treatment
- Dental problem
- Year of birth

2.4.2 Provision of dental services to and in connection with natural persons:

Identification of the User, differentiation from other customers and interested users, registration.

Storage of patient diary, medical history, preparation.

Legal basis of data management: Statutory

Scope of data managed:

- Name
- Permanent address
- Phone
- History
- Finds
- Year of birth
- Unique identifier

- Patient Diary

2.4.3 Invoicing for dental services

Legal basis of data management: Statutory

Scope of data managed:

- Name
- Adress
- Health Fund Settlement
- Health fund card number and address of and provider name.
- Cardholder's name
- Signature,
- EP card number

Legal basis of data management: legitimate interest - The Organization has a legitimate interest in settling accounts with the Health Insurance Fund provider

2.4.4 Advertising of service (s), provision of information to registered users about new or renewed services, direct business acquisition and marketing inquiries with advertising content customer satisfaction measurement.

Legal basis for data management: Consent of the data subject

Scope of data managed:

- Name
- E-mail address
- Additional information provided by the user

2.4.5 Operation of an electronic monitoring system to protect:

Security of the Data Controller's site

Protection of the Data Controller's assets

Protecting the physical integrity and property of the Data Controller's employees and visitors

Investigation of the circumstances of possible accidents and crimes

Legal basis of data management: The consent of the data subject, which in this case is expressed in action, i.e. enters the Data Management area despite the call for camera surveillance, as well as a legitimate interest in property protection.

Scope of data managed:

- Recording the image, motion picture and sound of a natural person (hereinafter together recording)

3 RIGHTS OF STAKEHOLDERS AND THEIR ENFORCEMENT

3.1 Rights of the data subject vis-à-vis the Data Controller:

- request information on the handling of your personal data,
- request the correction or deletion of your data, with the exception of mandatory data processing required by law,
- object to the processing of your personal data,
- you can go to court if your rights are violated.

3.2 Right to information:

At the request of the data subject, the Data Controller shall provide information on the data processed by the data subject or processed by the data processor entrusted by him or her or at his / her disposal, their source, the purpose, legal basis, duration of the data processing and whether the data processing is in progress. The Data Controller shall inform about the name, address and activities related to the data processing, the circumstances, effects and measures taken to prevent the data protection incident, and, in case of transfer of the data subject's personal data, the legal basis and recipient of the transfer.

The Data Controller is obliged to provide the information in writing in a comprehensible form as soon as possible after the submission of the request, but no later than within 30 days. The information is free of charge if the person requesting the information has not yet submitted a request for information to the data controller for the same data set in the current year. In other cases, reimbursement may be established. The Data Controller may only refuse the information in accordance with the provisions of the data protection legislation in force at any time.

3.3 Correction and erasure:

The data subject shall have the right, at his request, to have inaccurate personal data concerning him rectified without undue delay. Taking into account the purpose of the data processing, the data subject has the right to request that the incomplete personal data be supplemented, inter alia, by means of a supplementary statement.

Personal data must be deleted:

- if your handling is illegal,
- the data subject requests or
- withdraw your consent to the processing of the data, unless the processing is required by law,
- incomplete or incorrect - and this condition cannot be legally corrected, provided that cancellation is not precluded by law,
- the purpose of data processing has ceased or the data storage period has expired,
- personal data has been processed unlawfully, ordered by a court or the Data Protection Commissioner.

The rectification or erasure shall be notified to the data subject or to those to whom the data have previously been transmitted, unless this would harm the data subject's legitimate interests.

3.4 Right to protest:

The data subject may object to the processing of his or her personal data if:

- the processing and transmission of personal data is necessary only for the enforcement of the data controller's, data recipient's right or legitimate interest, unless the data processing is ordered by law,
- if the use or transfer of personal data is for the purpose of direct business acquisition, public opinion polling or scientific research
- the exercise of the right to protest is otherwise permitted by law.

Despite the protest of the data subject, the Data Controller may only continue to process the data of the data subject if it is required to do so by law.

3.5 Right to restrict data processing:

The data subject has the right to restrict the data processing at the request of the Data Controller if any of the following is met:

- the data subject disputes the accuracy of the personal data, in which case the restriction applies to the period of time that allows the controller to verify the accuracy of the personal data,
- the processing is unlawful and the data subject opposes the deletion of the data and instead requests that their use be restricted,
- the data controller no longer needs the personal data for the purpose of data processing, but the data subject requests them in order to submit, enforce or protect legal claims,
- the data subject has objected to the processing; in that case, the restriction shall apply for as long as it is established whether the legitimate reasons of the controller take precedence over the legitimate reasons of the data subject.

Where data processing is restricted, such personal data may be processed, with the exception of storage, only with the consent of the data subject or for the purpose of bringing, enforcing or protecting legal claims or protecting the rights of another natural or legal person or in the important public interest of the Union or a Member State. The Data Controller shall inform the data subject at whose request the data processing has been restricted in advance of the lifting of the data processing restriction.

3.6 Right to data portability:

The data subject shall have the right to receive the personal data concerning him or her made available to the Data Controller in a structured, widely used machine-readable format and to transfer such data to another data controller without being hindered by the data controller whose provided the personal data to him.

3.7 Judicial enforcement:

In case of violation of the rights of the data subject, he / she may take legal action against the data controller. The court is acting out of turn in the case. The data controller is obliged to prove that the data processing complies with the provisions of the law.

3.8 Compensation, damages:

If the data controller causes damage to another person by unlawfully processing the data subject's data or by violating data security requirements, he / she is obliged to compensate it.

If the data controller violates the data subject's right to privacy by unlawfully processing the data subject's data or by violating data security requirements, the data subject may claim damages from the data controller.

The data controller is liable to the data subject for the damage caused by the data processor and the data controller is also obliged to pay the data subject damages in the event of a personal data breach caused by the data processor.

The data controller shall be released from liability for the damage caused and the obligation to pay damages if he proves that the damage or the violation of the data subject's personal rights was caused by an unavoidable cause outside the scope of data processing. There is no need to compensate for the damage and no claim for damages to the extent that the damage was caused by the intentional or grossly negligent conduct of the injured party or the violation of the right to privacy.

4 METHOD OF DATA MANAGEMENT

4.1 They are entitled to data management:

The following are entitled to process health and personal data:

- the person caring for the patient,
- the head of the health care provider, or
- a person authorized by the head of the service provider.

When handling health and personal data, the security of the data must be ensured against accidental or deliberate destruction or destruction, alteration, damage, disclosure, and that they cannot be accessed by unauthorized persons.

4.2 Data recording:

The Data Controller records and stores the personal data provided by the data subject (name, date of birth, mother's name, address) as well as the health data recorded before or during the treatment in an electronic database.

In the case of a child under the age of 16, the processing of children's personal data is lawful only if and to the extent that the consent has been given or authorized by the person exercising parental supervision over the child (legal representative).

4.3 Data deletion:

Data can only be deleted in accordance with the relevant legislation. Deletion must comply with data protection rules, in particular with regard to unauthorized access. During deletion, manually processed data must be physically destroyed, and in the case of electronically stored data, they must be irreparably altered. Deletion of data may be performed with the permission of the Head of the Data Controller. The video and audio material recorded during the camera recordings will be automatically deleted after a maximum of 30 days, unless it serves as evidence as a basis for infringement or criminal proceedings, in which case the Data Controller may only forward the video and audio material to the investigating authority.

4.4 Data transmission:

The data controller does not transfer data outside the European Economic Area.

4.5 Data management for dental care:

During dental and oral surgery, the Data Controller records the personal data of the person (concerned) receiving the treatment and the health data necessary for the professional conduct of the treatment. The data subject or his / her legal representative shall provide the Data Controller with the health and personal identification data in order to fulfill the contract concluded with the Data Controller as a health care provider.

The data subject (legal representative) is obliged to provide his / her health and personal data at the request of the patient care provider, if

- is probable or confirmed to be infected by a pathogen of a disease or to poisoning of infectious origin, or
- suffer from an infectious disease if prescribed
- required for screening and suitability tests,
- in the case of acute poisoning, if the person concerned is likely to have an occupational disease if
- the provision of data is necessary for the treatment, preservation or protection of the health of the minor child, if
- for law enforcement, crime prevention, prosecution, court, infringement or administrative proceedings, the competent body has ordered the investigation if
- the provision of data is required for the purpose of control under the National Security Services Act.

During treatment, data in accordance with professional rules should be recorded in the medical records. The dentist performing the treatment decides which health data is required in accordance with professional rules, in addition to the mandatory data. Data collection that is not directly related to the patient's treatment should be avoided during data collection. During treatment, the procedure for handling medical records should be designed in such a way that the records and the patient's personal data can be accessed by those who treat the treated person.

Dental technicians employed by the Data Controller or acting as contracted subcontractors are entitled to get to know the patient data to the extent necessary for the preparation of the dental

unit. In the case of a subcontracting relationship, in order to ensure the legality of the data processing of the dental technician, it is necessary to conclude a data processing contract.

4.6 Protection of medical secrecy:

The patient care provider and any other person with an employment relationship with the service provider (Data Controller) shall be bound by the obligation of confidentiality with regard to the data related to the patient's state of health, as well as other data obtained in connection with work. The obligation of confidentiality is independent of the way in which the data was disclosed. The caregiver is also bound by the obligation of confidentiality vis-à-vis the caregiver who did not participate in the patient's treatment, unless the data are necessary for the further treatment of the treated person.

The patient or the statutory obligation to provide information may waive the obligation of confidentiality in writing. In order to protect medical secrecy, it is necessary that all employees of the service provider undertake to maintain medical secrecy. The obligation must be included in or attached to the employee's job description. The data subject (patient) has the right to declare who can be informed about his / her illness, its expected outcome, or who is excluded from partial or complete knowledge of his / her health data. The medical data of the patient concerned shall be provided without his or her consent, if this is the case

- ordered by law,
- necessitates the protection of the life, physical integrity and health of others.

4.7 Persons present during treatment:

The patient has the right to be present during the examination and medical treatment only by those persons whose participation in the care is necessary or by those whose presence the patient has consented to, unless otherwise provided by law. With the consent of the data subject, the following may be present without respect for the data subject's human rights and dignity:

- another person, if the treatment regimen requires the simultaneous care of several patients,
- a professional member of the police, if the treatment is provided to a detainee,
- a member of the penitentiary service, if the treatment is provided to a person who is serving a custodial sentence in a penitentiary institution and this is necessary for the safety of the medical care provider or to prevent escape,
- if the patient's personal safety justifies it for law enforcement purposes and the patient is unable to make a statement.

In addition to the above,

- who has already treated the patient for the disease,
- who has been licensed by the head of the healthcare provider for professional reasons. The express protest of the person treated must be upheld in this case.

For the purpose of training a health professional, a doctor, medical student, health professional, health college, health vocational school or student of a health vocational high school may be present during the treatment with the consent of the data subject (legal

representative). The consent of the person being treated may also be given orally to the treating dentist.

4.8 Right to information, information giving and obligation, patient's right to information:

Prior to initiating patient care, the patient should be informed of the provider's privacy policy. It is the duty of the dentist performing the treatment to inform the patient about the data protection. The patient confirms the provision of the information by signing the service contract. The patient's documentation must be accompanied by any patient's restrictive statement. Information on the treatment of the person being treated is provided by the dentist treating the patient. The healthcare professional who cares for the patient can also provide information about the nursing aspects of the patient's treatment. A specialist or other employee may not provide information about the patient's treatment, unless the dentist treating the patient has authorized it for that patient. The information is provided in person.

The treating physician shall inform the data subject directly of the health data established by him or her. In the case of a person with a mental illness, the patient's right to access the medical records may exceptionally be restricted if there are reasonable grounds for believing that access to the medical records would seriously jeopardize the patient's recovery or the privacy of another person. Only the dentist has the right to order the restriction. The patient's legal representative and the patient's legal or authorized representative must be notified immediately of the imposition of the restriction.

4.9 Informing a relative and another person:

The patient may decide at the time of registration with the service provider or later which persons may be given partial or complete information about his / her illness, its expected outcome, changes in his / her state of health, and who should be excluded from it. The patient should be informed of the possibility of disposal.

4.10 Right of access to medical records:

The patient (or his / her legal representative) has the right to be informed of his / her personal identification and medical data and has the right to inspect the medical records. The medical documentation is available to the healthcare provider, and the data contained therein is available to the patient.

The patient is eligible

- receive information on the handling of your treatment-related data,
- get to know the health data concerning him,
- inspect the medical records and make an extract or copy thereof or obtain a copy at your own expense.

5 IMPLANT REGISTER

5.1 Information on the legal obligations related to the implant register:

If an implant is implanted, removed or replaced in connection with the patient concerned during the treatment, the Data Controller shall comply with the provisions of Act CLIV of 1997 on Health Care. According to Act 101 / C. § (1) The data of the register containing the data shall be forwarded to the central implant register kept for the purpose of further treatment, monitoring of the state of health, rapid response to an unexpected event and verification of the conformity of implantable medical devices.

The health insurance body that operates the central implant register generates a contact code for personal identification data. The contact code shall be established by the health insurance body on the basis of the same coding method for all personal data, so as not to allow decryption of personal data and for all data transmissions to the same patient, regardless of the healthcare provider performing the intervention.

The contact code according to the above is sent by the health insurance body to the healthcare provider keeping the register via the IT application operated by it. The contact code should be included in the medical documentation, including in the final report provided to the patient. The body designated to perform official tasks related to medical devices may access non-personally identifiable data with a contact code in the central implant register for the purpose of performing official tasks related to medical devices.

The health insurance body shall provide information on non-personally identifiable data stored in the central implant register with a contact code to the public health administration body and the body responsible for professional quality assessment without delay upon request within 8 days or, if necessary to protect the health of implant wearers.

At the request of the healthcare provider containing the contact code indicated in the patient documentation, the health insurance body shall immediately provide information on the data stored in the central implant register with a contact code in connection with the implant intervention previously performed by the healthcare provider.

If it is necessary to prevent or remedy an urgent or endangered condition for the implanter and the last implantable healthcare provider has ceased to exist without a legal successor or the medical records cannot be obtained or are not significantly delayed, the body designated to perform official medical device tasks you can get to know Eütv. 101 / C. § (1) a) in order to contact the data subject and inform him / her about the actions necessary for the protection of his / her health.

The following personal and health data must be handled:

- among the personal identification data specified in the Act on the Handling and Protection of Health and Related Personal Data, the surname and first name, birth name, date of birth, mother's birth name, place of residence or stay, other contact details of the person involved in the intervention,
- the date of implantation, removal or replacement,
- the reason for implantation, removal or replacement,
- in relation to the implant implanted or removed

  - the name, type and batch number of the implant, if available, with the serial number,
  - the name of the manufacturer,
  - the name and registered office of the distributor from whom the implant was obtained by the healthcare provider,
- the name and number of the implanting doctor,
- the name of the implanting health care provider and the number of its operating license.

The data stored in the central implant register shall be deleted 50 years after the last transmission of the data subject.

6 RECORD OF HEALTH AND PERSONAL IDENTIFICATION DATA

6.1 Registration obligation:

The health and personal data collected from the data subject for the purpose of medical treatment and their transmission shall be recorded. The record of the transfer must contain the recipient, method, date of the transfer and the scope of the data transferred. The means of registration may be any means of storage which ensures that the data are protected against deliberate destruction, destruction, alteration, damage, disclosure and that they cannot be accessed by unauthorized persons. The patient caregiver's own records are part of the record.

6.2 Procedure for storing and archiving health records:

Data related to the examination and treatment of the patient are included in the medical records. Medical records should be maintained in a way that accurately reflects the process of care.

The health record must indicate:

- the patient's personal identification data,
- in the case of a patient with legal capacity, the name, address and contact details of the person to be notified, in the case of a minor or a patient under guardianship,
- medical history, medical history,
- the result of the first test,
- the test results on which the diagnosis and care plan are based, the date on which the tests were performed,
- the name of the illness justifying the care, the underlying illness, comorbidities and complications,
- an indication of other illnesses or risk factors that do not directly justify the benefit,
- the time of the interventions carried out and their results,
- patient hypersensitivity data,
- the name of the healthcare professional who registered and the date of registration,
- recording the content of the information provided to the patient or other person entitled to information,
- the fact of consent or refusal and their date,
- any other data and facts that may affect the patient's recovery.

The following must be kept as part of the medical file:

- findings from each study,
- documents generated during medical treatment and consultation,
- recordings of imaging diagnostic procedures.

7 DATA PROTECTION, DATA SECURITY

7.1 Data security, data protection:

The data shall be protected in particular against unauthorized access, alteration, transmission, disclosure, deletion or destruction, and against accidental destruction or damage. In order to ensure the technical protection of personal data, special protection measures must be taken by the data controller, the data processor or the operator of the telecommunications or IT device if the personal data is transmitted over a network or other IT means.

Within the health care provider, the head of the institution handling the data is responsible for the protection of health and personal identification data and the preservation of the register.

8 DATA PROCESSING FOR PUBLIC HEALTH AND EPIDEMIOLOGICAL PURPOSES

The patient care provider shall immediately forward the health and personal identification data to the state health administration body if an infectious disease is detected or suspected. The urban institute of ÁNTSZ may request the personal identification data of the person concerned on the grounds of public health or epidemiological public interest.

9 DATA CONTROLLER DETAILS, CONTACT DETAILS

Supplier: DENTAL PALACE Limited Liability Company

Company registration number: 01-09-912523

Tax number: 14627000-2-41

Headquarters: 1037 Budapest, Toboz utca 6.

Tel .: +36 1 250 9086

WEB:

http://www.dentalpalace.hu/

http://www.dentalpalacehongrie.fr/

http://www.dentalpalace.nl/

E-mail:

info@dentalpalace.hu;

info@dentalpalace.nl;

info@dentalpalacehongrie.fr

10 DATA PROCESSING

10.1 Use of data processor:

The rights and obligations of the data processor in relation to the processing of personal data are determined by the data controller within the framework of separate laws on data processing. The data controller is responsible for the legality of the instructions given by him. The data processor may not make a substantive decision concerning data management, may process personal data obtained only in accordance with the provisions of the data controller, may not process data for its own purposes, and is obliged to store and preserve personal data in accordance with the data controller's provisions.

10.1.1 Patient record IT environment:

The Health Service Provider, as the Data Controller, uses a data processor to manage the data - to perform various sub-tasks. The Data Processor provides the Data Controller with the software used to record the patient documentation in the electronic database and to keep the IT environment up to date. The data controller and any person acting under the control of the data controller or the data processor who has access to personal data may only process such data in accordance with the data controller's instructions, unless otherwise required by law to deviate from it.

10.1.2 Invoicing

In addition to the above, the Data Controller employs an additional data processor for the performance of accounting tasks only in order to fulfill the tax obligations on the invoice issued for the healthcare service fee. The data processor only gets to know the personal data of the patients, which are indicated on the invoice issued for the service fee (name, address). The legal basis for the data processing or data processing in this case is the fulfillment of a legal obligation under Article 6 (1) (c) of the GDPR Regulation. The period of data storage for accounting records is set by law at 10 years.

10.1.3 Ancillary health service

If, during the medical treatment, the patient requires vigilant sedation (anesthesiology) for an intervention, the Data Controller implements this service with the help of an external service provider, during which a separate medical data is collected with the anesthesiologist and a statement of consent is signed. by the patient. The sole purpose of this data collection is to obtain information and health data that may affect the work of the anesthesiologist. The anesthesiologist acts as a data processor for data processing purposes, the legal basis for data processing is the performance of a contract with the Data Controller as a healthcare provider pursuant to Article 6 (1) (b) of the GDPR Regulation.

11 COMPLAINTS, REMEDIES

The Data Controller fully respects the rights and freedom of self-determination of the data subjects. In order to avoid various conflicts of interest and to increase the protection and

security of the personal data of the data subjects, the Data Controller employs a Data Protection Officer within the framework of a mandated legal relationship.

The Data Protection Officer is the internal guardian of the rights and freedom of self-determination of data subjects. Your opinion must be sought before introducing any new data sets or data management. In the case of complaints and notifications related to data protection and data security, your support must be requested in order to ensure proper administration.

11.1 Contact details of the Data Protection Officer:

CONSILIS DATA KFT. (JÓZSEF DR. CSABA)

Cím: 2051 Biatorbágy, Arany János u. 29.

WEB: https://consilisdata.hu/

e-mail: info@consilisdata.hu

The data subject may initiate the relevant procedure or investigation against the Data Controller at the National Data Protection and Freedom of Information Authority if he / she is harmed in connection with the processing of his / her data.

11.2 Contact details of the authority:

National Authority for Data Protection and Freedom of Information (NAIH)

Address: 1125 Budapest, Szilágyi Erzsébet avenue 22 / c

Phone: +36 (1) 391-1400

Fax: +36 (1) 391-1410

www: http://www.naih.hu

e-mail: ugyfelszolgalat@naih.hu