



Data Protection Declaration

Company name: SOLYDENT Kft

Last modified: 2018.05.25.

Version: v1.0

Validity from: 2018.05.

Table of Contents

1. General provisions.....	4
1.1. Purpose of the provisions	
1.2. Organisational scope of the provisions	
1.3. Scope of application of the provisions	
1.4. Legal fundamentals	
1.5. Definitions	
2. Responsibility for data management	7
3. Data management principles	7
4. Purpose of data collection	7
5. Definitions of the groups of persons.....	8
5.1. Patients	
5.2. Other persons	
6. Legal framework for the data management	9
6.1. Patient compliance	
6.2. Legal requirements	
7. Data scope and data management	9
8. Miscellaneous data management.....	10
8.1. Recording of telephone conversations	
8.2. Recording of camera images	
8.3. Preparation of documents and reproduction	
8.4. Identity management	
9. Duration of Data Management.....	11
10. Transmission of data.....	12
10.1 General rules for data transfer	
11. Managing information files.....	13
12. Data security	13
12.1 Data protection officer	

13.Data management in the clinic	14
13.1. General rules for data processing	
13.2. Miscellaneous data processing	
14.Data erasure and archiving.....	14
15.The patient, his rights and confirmations.....	15
15.1. Right to information	
15.2. Right to correction	
15.3. Right of erasure and revocation	
15.4. Patient, enforcement of patient's rights	
15.5. Patient, affected handling of complaints, liability	
16.Contacts.....	17
16.1 Data manager	
16.2 Data protection officer	
16.3 Data protection authority	

1. General provisions

1.1. Purpose of the provisions

The data protection and the relevant data protection declaration (hereinafter referred to as "declaration") are intended to ensure that the data of patients and other natural persons are treated by Solydent Kft. (hereinafter referred to as "clinic") within the legal framework and the necessary transparency. Based on Act (EU) 2016/679 2016, which is in contact with the European Parliament and the Council, adopted on 27 April 2011, and Law CXII of 2011 on Informational Self-Determination and Freedom of Information. (hereinafter referred to as "Infotv.") with due regard to the provisions of Act XLVII of 1997 on the Administration and Protection of Health and Related Personal Data Protection.

Our goal is to process personal information and health data in accordance with applicable regulations and to transparently consider our patients, their respective and other relevant interests.

1.2. Organisational scope of the provisions

The scope of this declaration extends to the clinic, all its departments and in particular to persons whose data are included in the data processing arising under this declaration, and furthermore to persons whose rights or legitimate interests are affected by the data processing.

1.3. Scope of application of the provisions

The clinic operates in accordance with the provisions set forth in the Agreement of the Infotv. on privacy and data protection statement, which secures the rights of the affected person under the law. The scope of this declaration covers the entire data management of the clinic and

- a. it includes the details of patient relations,
- b. it contains the data of the persons with whom the patient has been in contact
- c. it contains the details of the persons with whom the patient will have contact
- d. it contains the data of the persons with whom the patient is in contact, and only the data necessary for the handling of the patient's personal data

1.4 Legal fundamentals

- a. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (GDPR),
- b. the Act V of 2013, Civil Code (Civil Law)
- c. 2011 CXII. Law on self-determination and freedom of information (Infotv.),
- d. Act XLVII of 1997 on the Management and Protection of Health and Related Personal Data, and any necessary legislation that includes a mandatory data management provision.

1.5 Definitions

- a. Persons affected

Any natural person who can be identified, directly or indirectly, on the basis of personal data. With regard to the processing of data to which this declaration refers, this refers primarily to the patient, the previous patient and the persons who intend to contact the clinic, and the person whose data will be processed by the clinic in connection with the provision of the service;

b. Personal data

data relating to the individual concerned, in particular the name, identification and identity of one or more physical, physiological, mental, economic, cultural or social identities of the individual concerned and the underlying data, as appropriate;

c. Special data

- personal data relating to nationality, political opinion or party affiliation, religious or other beliefs, membership of interest groups, sex life,
- Personal data on health status, unhealthy characteristics and criminal personal information;

d. Declaration of consent

The person affected voluntarily and resolutely gives his/her consent, based on adequate information and with which he/she gives his/her unambiguous consent, to the handling of personal data covering all or part of the operations;

e. Appeal

The declaration of the affected person against whom he has objected to the processing of his personal data and demands the termination of the data processing and the cancellation of the processed data;

f. Data manager

A natural or legal person, i.e. an entity without legal personality or which, individually or jointly with others, determines the purpose of the data processing and takes decisions on the information relating to the data processing (including the equipment used) and carries it out itself or transfers it to a data manager entrusted to it.

The data controller of the clinic is responsible for the data processing that is subject to this declaration;

g. Data management

Regardless of the method used - any operation on the data or on any operation, including, but not limited to, collecting, capturing, recording, systematizing, storing, modifying, using, retrieving, transmitting, disclosing, aligning or interconnecting, locking, erasing and destroying data, preventing the continued use of data, photographing, sound or image, and recording physical characteristics capable of identifying a person - must be recorded;

h. Data forwarding

To make the data accessible to a specific third party (person);

i. Third party (person)

It is a natural or legal person or entity without a legal person, other than the data subject, data controller or data processor.

j. Disclosure

Making the data available to everyone;

k. Data erasure

Make the data unrecognizable so that recovery is no longer possible;

l. Data marking

Providing a data identification tag for differentiation;

m. Data blocking

Provision of data identification for further treatment for a specific period of time or deadline.

n. Data destruction

Complete physical destruction of data on all contained media;

o. Data processing

to perform technical tasks related to data management operations, regardless of the method and device used to perform the operations and the location of the application, provided that the technical task is performed with the data;

p. Data processor

It is a natural or legal person or entity without legal personality who processes the data on the basis of a contract concluded with the data controller, including the conclusion of a legal provision..

q. Information register

The sum of the data processed in a register;

r. Contract/Agreement

A contract/agreement between the clinic and the patient regarding the use of a service to be provided by the clinic. The contract can be concluded verbally or in writing. The conclusion of the contract can be facilitated by the treatment and cost plan as the main document describing the course and content of the treatment.

s. Health data

data on the patient's physical or mental condition, abnormal passions, morbidity, death or cause of death reported by another person or individual or supplemented, tested, measured, tracked or

derived by healthcare; and any data affecting or influencing the foregoing (e.g. behavior, environment, occupation).

2. Responsibility for data management

Solydent Kft. (head office: 9024 Győr, Kálvária utca 37., commercial register number: 08-09-003854, tax number: 11132488-1-08), which provides dental outpatient services for its clients.

3. Data management principles

As the data controller, the clinic is obliged to act in accordance with the requirements of good faith and in agreement with the parties concerned. The Clinic is obliged to exercise and fulfill its rights and obligations in accordance with its purpose. To ensure the quality of personal data during processing as long as their relationship with the affected person can be maintained. The affected person may re-establish the connection if the Data Manager has the technical facilities necessary for the re-establishment. The Data Manager shall ensure the accuracy, completeness and, if necessary, updating of the data and, if necessary for the purpose of data management, that the affected person can only be identified for the duration of the data management.

The clinic emphasizes the procedure, which contains the principles of the concept for the administration of personal data established by the DSGVO.

Personal data:

- a. the processing must be lawful, fair and transparent ('lawfulness, fairness and transparency');
- b. Data collection may only be collected for specified, explicit and legitimate purposes and may not be treated in a manner incompatible with those purposes; according to Article 89 (1), which is not incompatible with the original purpose of further data processing and for the purpose of archiving of public interest, scientific and historical research purposes or for statistical purposes ("purpose limitation");
- c. Data management must be adequate and relevant for the purposes and should be limited to needs ("information reduction");
- d. keep accurate and, where necessary, kept up to date; take all reasonable steps to delete or correct ("Accuracy") inaccurate personal data for data management purposes; irrevocably delete or correct ("Accuracy") apparently inaccurate personal data;
- e. They shall be stored in a form which permits identification of the affected person only for a specified period of time necessary for the processing of personal data. Personal data may be retained only if the personal data are processed in accordance with Article 89(1) for archiving in the public interest, for scientific and historical research purposes or for statistical purposes in accordance with the rights and provisions, subject to appropriate technical and organisational measures to protect their rights ("limited data retention");
- f. Data shall be managed in such a way as to ensure adequate security of personal data, including protection against unauthorized, unlawful, accidental loss or destruction of data ("integrity and confidentiality"), by appropriate technical or organizational measures.

4. Purpose of data collection

The Data Protection Officer manages personal data only for a specific purpose, to exercise the right and to fulfill the obligation. It must fulfill the purpose of data management at all stages of data processing. The recording and processing of data must be fair and legitimate. The Data Protection

Officer will attempt to manage only personal data that is essential for the purpose of data management. Health and personal data can only be handled to the extent and for the period of time necessary. In all cases, data processing under this Policy refers to a service provided by the Clinic as data controller, where the service is used by the affected person as a patient or is used by the data controller to receive the service or by a third party with the involvement of the affected person (e.g. its representative, its authorized representative).

Data processing within the scope of this declaration is intended for the following purposes

- a. The clinic as data controller is in charge of preparing the concluded contract, securing the conclusion and execution of a contract.;
- b. in case of separate permission, the Clinic is authorized to conduct direct marketing or market research (by letter, telephone or other electronic means and other forms of communication);
- c. after termination of the contract, the exercise of the rights arising from the contract and the fulfillment of obligations, in particular the enforcement of contractual claims.

The clinic may also manage your personal data and your health data for other purposes:

- a. Monitoring the patient's state of health;
- b. Enforcement of patients' rights;
- c. medical-professional and epidemiological investigation, analysis, planning, organisation of health care, cost planning;
- d. to promote the official or legal control of the body or person administering the health data, the work of professional associations to carry out legal supervision, if the purpose of the examination cannot be otherwise achieved and it is the task of the organisations to finance the service providers
- e. for persons who wish to receive and apply for health care under compulsory health insurance and to comply with the rules for ordering low-cost medicines, medical aids and medical care, in addition to the right to benefits provided and financed under a contract under a separate law, in addition to the settlement of price subsidy and social security benefit payments, as well as the reimbursement and reimbursement of benefits paid
- f. Determination of suitability for work, whether the activity is an employment, a public service or a public service; in a legal relationship with a public service, a state service, a professional service or any other legal relationship. The healthcare provider has the right to promote effective and safe medicines and to provide cost-effective drug therapy;
- g. Enforcement of rights relating to cross-border healthcare in the European Union

5. Definitions of the groups of persons

5.1. Patients

The clinic mainly treats the data of natural persons connected with the patient so that the service provided by the Data Manager is used on a contractual basis. The clinic also manages the data on the persons with whom you have previously been in a patient relationship (former clients).

5.2. Other persons

The clinic also manages the data of individuals with whom the clinic wishes to communicate, with the aim of enabling them to access your services. The patient relationship is not established until the conclusion of the service contract, but the persons concerned are made available to the clinic with

their data, in particular to enable the data controller to make a valid decision on the establishment of the legal relationship. The Clinic also manages the data of natural persons who are affected by the contract between the Clinic and the patients and whose data are necessary for the fulfilment of the contract (legal representative of the disabled, a lawyer for persons with limited legal capacity, carer for a disabled person).

6. Legal framework for the data management

6.1 Patient compliance

The clinic treats the patient's health and personal data primarily with the patient's consent. The person concerned provides his/her health and personal data for the conclusion of the contract and for the preparation of the contract (legal basis for the processing of personal data). In the contract with the clinic, the Patient consents to the processing of all his/her personal data necessary for the execution of the contract.

The contract cannot be executed without the processing of the data, the contract cannot be concluded without the patient's consent. However, the non-acceptance of the data protection and data processing declaration does not exclude the conclusion of a contract.

By signing the contract, the affected person consents to the processing of the data contained in this contract and in the terms and conditions of the contract, and the clinic shall determine the scope of the data to be processed in this declaration and inform the affected person of the duration of the data processing, the purpose of the use, the transmission of the data, the use of the data processing and all fundamental facts and circumstances under which affected person may voluntarily and reasonably decide whether or not to consent to data management. If the processing of the data is not necessary for the fulfillment of the contract, the clinic may only process the data if they are voluntarily provided by the patient. By filling in the forms for the collection of your data, the patient agrees to provide his/her personal data as indicated on the form. If the patient gives his/her consent in a separate declaration, the clinic will provide the person concerned with complete information on the treatment of the data in connection with the declaration.

6.2 Legal requirements

If personal data is handled legally, data management is mandatory. The clinic informs the person concerned. If a law is in force and legally binding, the clinic, as the data controller, must comply with the legal provisions. It cannot verify the appropriateness, professionalism and constitutionality of the law.

Personal data may also be processed where it is impossible or disproportionately costly to obtain the consent of the affected person and the handling of personal data is necessary for the legitimate interests of the data controller or of a third party and the enforcement of that interest is proportionate to the limitation of the right to the protection of personal data.

7. Data scope and data management

- a. Natural identity data: The purpose of this data is to treat the patient, uniquely identify those affected and contact persons. The clinic manages the patient with the following data of the person concerned: name, date of birth, nationality, address, postal address, identity card number (passport number). The legal basis for the data management is the consent of the patient in the contract and the legal provisions.

- b. The patient, telephone numbers and other contact details required for the contact in question: When patients provide the information, the clinic manages your phone numbers and e-mail addresses for that contact.
- c. information necessary to conclude a contract for the service used or to be used in order to conclude the contract, e.g. in connection with the person concerned
 - Personal data (age, gender),
 - Special information on treatment, e.g. existing cardiovascular diseases, infectious diseases, sensitisation of drugs, etc.
 - Trip organization data of the trip (if the customer requests a trip from the clinic)
 - Additional historical information for treatment and succession planning: information on alcohol consumption, smoking or drug use

These data will be processed by the clinic on the basis of the consent of the person concerned.

- d. Information generated in connection with the provision and use of the services offered
 - radiographs
 - laboratory results
 - colour of the affected tooth
 - images of the condition of a prosthesis
 - other health data generated during treatment

with the consent of the person concerned.

- e. Claims arising from contracts entered into or terminated between the clinic and the patients and their validation: Data management from contracts that have expired may be derived from applicable laws and all relevant information required to enforce the claim and from information required by law to be retained at the Clinic.
- f. Information generated during the contact with the clinic and the customer service of the clinic: This includes all information created in Customer Service and generated by the relationship between the customer and Customer Service. The processing of the data in this case refers to the procedures initiated by the party concerned and is closely linked to the contract and the performance of the contract.
- g. Telephone conversations between the patient, other affected persons and the clinic: The clinic will treat the voice recording of the patient, the affected persons and the customer service in accordance with the applicable laws and will record it in the terms agreed with the customers. The patient, the persons concerned, are always informed about the recording before the beginning of the conversation.
- h. Images captured by the clinic with an imaging device: The clinic may operate image and sound recording equipment and systems on site. Recordings that are created as such are managed by the clinic.

8. Miscellaneous data management

8.1 Recording of telephone conversations

The clinic registers a telephone call with a person who has made a call or a telephone call initiated by the clinic. These records are stored and used for handling complaints, enforcing claims, processing and quality assurance. The legal basis for the recording of sound carriers is the consent of the patient and the storage period lies at the end of the contractual relationship between the patient and the clinic.

8.2 Recording of camera images

When entering the clinic premises, the patient encounters a closed camera network. The cameras have two purposes:

- The cameras placed on the parking lot and at the reception are used for object protection. The clinic stores the data in accordance with applicable law and without use for up to 3 days.
- The cameras in the clinic's treatment rooms improve the quality of treatment and investigate possible complaints. The data recorded by these cameras are also collected by the clinic for legitimate reasons and stored for up to one year.

In every room where cameras are in operation, the clinic is obliged to draw the patient's attention to this by means of instructions.

Patient rights are enforced in the same way as described in the section "Patients and Rights and Appreciation"..

8.3 Preparation of documents and reproduction

The clinic is entitled by the patient to make available to the person concerned, for the services provided by the contracting party, documents relating to health in relation to the diseases in question and to request such information, to receive them either electronically or by telephone, to check them and to store them.

8.4 Identity management

The clinic is entitled to process the markings required for the fulfillment of legal obligations. If there is a relationship between the patient, the person concerned and the clinic in connection with the clinic's tax obligation, including the obligation to provide data, the authority is entitled to process the relevant tax identification number.

9. Duration of Data Management

The Clinic will delete the data if it is evident that the data will no longer be used in the future, i.e. the purpose of the data management will be discontinued and the relevant legislation permits this. The clinic will also delete the data if requested to do so by the affected person and if this is permitted by law. The Clinic or its suppliers may treat personal data in order to fulfil their legal obligations or to enforce legitimate interests, if the interest is asserted by limiting the right to the protection of personal data, even after the consent of the affected person has been revoked.

According to the 1997 XLVII. law, medical records must be kept for at least 30 years from the date of data collection and the final report for at least 50 years. An imaging diagnostic procedure for up to 10 years after its creation, the recorded image must be kept for 30 years after the finding. After the mandatory retention period, the data may continue to be retained for medical purposes or for scientific research, if justified. If the additional data sets are not justified, the data sets must be destroyed.

10. Transmission of data

10.1 General rules for data transfer

In any case, the data will be communicated only with the consent of the person concerned or on the basis of the consent of the law. The Clinic will transmit personal and medical data only if its legal basis is clear and expedient and if the person receiving the data is clearly defined. The clinic always documents the transmission of the data in such a way that their progress and legality can be proven. The documentation is mainly provided by properly documented documents that request or perform the data provision. Compliance with the legally prescribed data transmission is bindingly observed by the clinic as data controller. In addition, personal and health data can only be transmitted if the affected person has given his or her unambiguous consent. In order for the consent to be subsequently proven, it should be written as far as possible. The written form can be ignored if the transmission of data is of minor importance for the recipient, the purpose or the data field. In the case of data transfers which are subject to the consent of the data subject, the affected person shall state his or her declaration in the knowledge of the recipient and the purpose of the transfer. The prohibitions and restrictions listed also apply to the termination of the patient relationship.

Regular data transmissions

- The patient's personal data and medical record are forwarded to the supplier and the supplier's data processor. The patient agrees to this data management when the contract is concluded and thus releases the data manager from his confidentiality obligation. A list of the supplier categories used by the clinic can be found under "13th Section "Data Manager in the Clinic". Data may only be transferred for the purposes stated in paragraph 4 in justified cases. The data recipient may only use the data in connection with the purpose of the data transfer and may pass it on to third parties with the consent of the clinic. The data controller shall ensure that the data security and legitimate data management requirements are also met by the recipient of the data
- If the patient places an order with the Clinic that requires the data to be transmitted, the Clinic may transmit the data to the extent necessary to fulfill the order. In this case, the patient is released from the obligation of secrecy.

Transfer of data to a third country

Personal data may be transferred to the data controller for data processing in a third country or to a data processor in a third country if the patient and affected person expressly consent and the data administrator or data processor fulfils the conditions set out in paragraph V of the GDPR.

The transfer of data to the EEA States shall be deemed to be a transfer of data within Hungary.

11. Managing information files

The Clinic must ensure that the method and content of the records at all times comply with applicable laws. It is mandatory for legislative data management that patients and data subjects can request information. The clinic must ensure proper, logical separation of data management for various purposes. The Clinic shall treat electronic and paper-based records according to uniform principles and take into account the characteristics resulting from the differences in the records. The principles and obligations of this Declaration apply to both electronic and paper documents. The patient, the data contained in the relevant data and the records relating to the services provided by the Clinic will be divided appropriately to separate the data processing from its legal basis and purpose. By setting up the recording system, establishing claims and other organisational measures, the Clinic ensures that the data contained in the personnel register can only be accessed by employees and other persons acting in the interest of the Clinic who need to do so in order to perform their duties. The Clinic grants access to data to third parties involved, taking into account the data security requirements that offer services related to the processing of data in connection with data management.

The clinic's electronic records comply with data security requirements, and the records ensure that the data is intended only for the purpose and only for persons who need it to perform their duties. The Clinic will endeavour to enforce the principle of data minimization as far as possible to ensure that individual employees and other persons acting on behalf of the Clinic can only access the necessary personal data. The applicable rules and regulations apply to the management of files, their monitoring, access rights, data and the use of documentation within the organisation of the clinic. These policies and instructions are governed by this Statement and by applicable law - primarily Infotv. - the principles and provisions of the law.

12. Data security

The clinic as data administrator guarantees the security of the data. For this purpose, the necessary technical and organizational measures are taken, both for the stored IT tools and for the files stored on conventional paper media. It is ensured that the data security rules required by applicable law are enforced. It also ensures data security, takes technical and organisational measures and establishes procedural rules necessary to enforce applicable laws, data and confidentiality rules. The clinic as data administrator protects the data against unauthorized access, modification, transmission, transfer, deletion or destruction as well as accidental destruction and damage and unavailability due to a change in the technology used. In order to enforce the conditions of data security, appropriate preparation of the affected employees is guaranteed. When defining and applying data protection measures, the clinic always keeps an eye on the state of the art. It selects several possible data management solutions that offer a higher level of protection for personal data, unless this is disproportionate.

12.1 Data protection officer

In view of its activities and the data connected with them, the Clinic considers it justified to use this legal instrument in order to manage the data of the affected person more securely. The appointed Data Protection Officer shall act in matters covered by this Declaration. Affected persons may refer all matters covered by this declaration to the Data Protection Officer.

Information on the availability of the Clinic's Data Protection Officer can be found under "16 Contacts".

13. Data management in the clinic

13.1. General rules for data processing

The Clinic reserves the right to suspend a data processor permanently or at short notice during his activity. Permanent data processing may take place primarily in connection with the patient relationship, medical treatment, administration and maintenance of the IT system in connection with the provision of services. When using the data processor, the applicable laws apply, in particular Infotv. The use of a data processor can only take place on the basis of a written contract. The Clinic shall inform the data subjects of the data processor and the details of its data processing activities, in particular about the procedures carried out and the instructions given to the data processor. The rights and obligations of the data processor with regard to the processing of personal data are defined by the clinic as the data controller within the framework of the relevant legal regulations. The Clinic is responsible for the legality of the instructions for data processing. The Clinic is responsible for the processing, modification, deletion, transfer and disclosure of personal and health data within the scope of its activities and within the limits established by the Clinic. Another data processor may obtain the consent of the Clinic as part of his data processing activities. The data processor may not make any significant decisions regarding data management, process personal and health data only in accordance with the provisions of the Clinic, process data for his own purposes, and store and retain personal and health data in accordance with the provisions of the Regulation.

The Clinic shall ensure that the rights of the affected person cannot be prejudiced in the course of data processing and that the data processor cannot disclose personal data and health data, unless this is indispensable for the performance of his/her duties.

13.2. Miscellaneous data processing

The range of data processes used by the clinic may vary.

The practice typically uses the following categories of suppliers for your business:

- accredited doctors
- external laboratories
- accounting offices
- IT suppliers
- Tour operators
- interpreter

14. Data erasure and archiving

The clinic as data administrator deletes personal and health data if

- a. the processing is illegal;

- b. the patient requests the person concerned (except in the case of legally regulated data processing);
- c. the data is incomplete or inaccurate - and this status cannot be legally removed - provided that deletion is not excluded by law;
- d. the purpose of the data management has ended or the statutory period for data storage has expired;
- e. It shall be ordered by the court or the national data protection and information authority.

A deletion of the data administered by the patient can be requested by the person concerned on the basis of the voluntary consent of the patient concerned. Without the relevant deletion request by the data subject, the clinic will delete the data once the purpose of the data processing has been discontinued. In the absence of any other purpose, the Clinic shall keep the data for as long as the data can be used in a separate procedure. Instead of being deleted, the Clinic may block the data if the patient asks the person concerned or if, on the basis of the information available to him, it can be assumed that the deletion would harm the legitimate interests of the patient. The data blocked in this way can only be processed as long as there is a data processing purpose that precludes the deletion of the data. The Clinic shall disclose the data it manages if the patient or affected person questions their accuracy or precision, but the inaccuracy or inaccuracy of the data in question cannot be unequivocally established. In the case of data processing required by law, data will be deleted in accordance with the provisions of the law. In case of cancellation, the Clinic will make the data inappropriate for personal identification. If required by law, the data carrier will be destroyed. If the data are administered by the clinic despite the revocation of the consent of the person concerned, the principle of the expediency of the data administration also applies; the clinic can treat the patient's data even if the patient's consent is revoked.

In this case, the data controller shall inform the patient and the affected person of the purpose and legal basis of the data management.

15. The patient, his rights and confirmations

The GDPR records the following rights that are considered by the clinic:

- right to information
- right of access
- right to rectification
- right to erasure
- right to a restriction
- right to data storage
- right of protest
- right to information for correction, deletion or limitation
- right to object to automated decisions

15.1. Right to information

The clinic informs the person concerned before the data is processed. Information may also be provided by the clinic by publishing the statement on details of data processing and by drawing the attention of the affected person to it. The patient, the person concerned, may request information about the handling of their data. The Clinic endeavours to inform the persons concerned about the details of data management before processing the data.

At the request of the person concerned, the patient shall inform the person concerned of the data processed by the data processor treated by him or her, including their source, purpose, legal basis, duration of processing, name of the data processor, address and data management activity, and, in

the case of the transfer of personal and medical data, the person concerned shall be informed of the legal basis and addressee of the data transfer. The clinic must provide the patient with written information on request as soon as possible after receipt of the application, but not later than 30 days after submission of the application. The information is free of charge if the applicant has not yet submitted a request for information for the same request in the current year. In other cases, reimbursement may be made. The reimbursement of the reimbursement already paid should be reimbursed if the data have been unlawfully treated or if the request for information led to a rectification. In the cases laid down by law, the refusal of information may take place.

15.2 Right to correction

The patient, the person concerned, can request that the incorrectly entered personal data be corrected by the healthcare provider.

If correct data is provided on the basis of the corrected data, the clinic will inform the data manager of the data correction and the patient if a correction is necessary.

15.3 Right of erasure and revocation

The patient may request the deletion of his/her personal and health data with the exception of the data processing required by law. The clinic will inform the patient about the deletion. If the consent based data processing is a prerequisite for the establishment and maintenance of the legal relationship, the patient will be informed by the clinic about it and about the expected consequences. The Clinic may refuse the deletion of personal and health data if the data is handled lawfully and the processing is necessary to enforce the legitimate interest of the Clinic. If the request for withdrawal is rejected, the Clinic will inform the patient concerned of the cause. Based on the relevant law CXII of 2011 on the Freedom of Information Act, you can object to the legally stipulated handling of your personal data.

15.4. Patient, enforcement of patient's rights

The patient may submit a request for information, correction or deletion of the information in person or in a letter addressed to the clinic or branch of the clinic. In order to facilitate the formulation and processing of requests, the Clinic provides forms that are available on the Clinic's website (<https://solydent.hu/adatkezeles>). The Clinic reserves the right not to enforce this right until the patient has been identified as the person concerned. At the request of the patient, the person concerned may contact the Clinic's Data Protection Officer directly using the contact details provided in this statement.

15.5. Patient, affected handling of complaints, liability

If the clinic does not comply with the relevant request for correction, blocking or cancellation, it shall notify the facts of the case and the legal reason for the refusal of the request for correction, blocking or cancellation within 30 days of receipt of the request. If a request for rectification, erasure or blocking is rejected, it shall inform the person concerned of the possibility of lodging a complaint with the court and the national data protection and information authority. In the event of information, corrections, cancellations or protests, the Clinic will act in accordance with applicable law. In the event of a violation of the law, the patient may request an executive of the person acting on behalf of the Clinic and contact the Clinic's designated Privacy Officer.

If the clinic refuses the order and the request for rectification, blocking or deletion is not completed, patients may apply to the competent court and the national data protection and privacy authority. The clinic will inform the patient, on request, of the persons concerned and of the means available. The patient, the accused party, may, at his choice, bring the aforementioned action before the competent court of the place of residence or stay. For damages caused by unauthorized data

processing, the Clinic is responsible for the provisions of the applicable law. The Clinic is obliged to compensate the patient for any damage caused by the patient, unauthorized handling of the data in question or violation of data security requirements. Unlike the patient, the clinic is responsible for the damage caused by the data processor. The clinic is exempt from liability if it proves that the damage was caused by an unavoidable cause outside data management. A compensation of the damage is not necessary, as far as this is based on resolution or rough negligence of the aggrieved party. The general civil liability of the clinic is regulated in the Civil Code. In the event of a patient's request, the Clinic shall provide detailed information on the legal means of enforcing the claim.

16. Contacts

16.1 Data manager

Solydent Kft.
H-9024 Győr, Kálvária utca 37.
Phone: +36 96/416-440
Fax: +36 96/440-229
E-mail: info@solydent.hu
Web page: <https://solydent.hu>

16.2. Data protection officer

Hámori Adrienn
Phone: +36 70 623 1261
E-mail: hamori.adrienn@webflow-dental.com

16.3. Datenschutzbehörde

Nemzeti Adatvédelmi és Információszabadság Hatóság
1125 Budapest, Szilágyi Erzsébet fasor 22/C.
Levelezési cím: 1530 Budapest, Postafiók: 5.
Phone: +36 -1-391-1400
Fax: +36-1-391-1410
E-mail: ugyfelszolgalat@naih.hu
Web page: <https://naih.hu>