PRIVACY POLICY

DENTAL HOLIDAY BP. KORLÁTOLT FELELŐSSÉGŰ TÁRSASÁG

(DENTAL HOLIDAY BP. LIMITED LIABILITY COMPANY)

H-2030 ÉRD, BUDAI ÚT 20. 1. EM. 14.

Tata, 25 October 2018

Content

1. General part

1.1 The purpose of the Privacy Policy

The purpose of this Privacy Policy (hereinafter: Policy) is to ensure that the data of the clients and other natural persons connected to Dental Holiday Bp. Kft (hereinafter: the Company) are processed under lawful conditions, in a transparent manner, in accordance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, and Act CXII of 2011 on Informational Self-Determination and the Freedom of Information (hereinafter: Act on Privacy), particularly taking into account the provisions of Act XLVII of 1997 on the management and protection of health and related personal data.

Our goal is that the personal and health data in our possession is properly processed according to the relevant legislation, while considering and balancing the relevant interests of our clients, our own, and other stakeholders in a transparent manner.

1.2 The organizational scope of the Privacy Policy

The scope of this Policy covers the Company, its organizational units, the persons whose data is processed under this Policy, and the persons whose rights or legitimate interests are concerned by the data processing.

1.3 The material scope of the Privacy Policy

In accordance with the provisions of the Act on Privacy, the Company undertakes to prepare a Data Protection and Data Security Policy, which more effectively ensures the statutory rights of the concerned persons. The scope of this Policy covers all data processing of the Company that:

a. contains the data of persons that are in a client relationship with the Company;
b. contains the data of persons that were in a client relationship with the Company;
c. contains the data of persons with whom the Company intends to establish a client relationship;
d. contains the data of persons related to persons in a client relationship with the Company in a way that the processing of their personal data is necessary for the Company's service provision.

1.4 Legislative background

a. Regulation (EU) 2016/679 of the European Parliament and of the Council adopted on 27 April 2016 (GDPR),
b. Act V of 2013 on the Civil Code (the Hungarian Civil Code),
c. Act CXII of 2011 on Informational Self-Determination and the Freedom of Information (Act on Privacy),
d. Act XLVII of 1997 on the management and protection of health and related personal data, and
e. all legislations that contain applicable statutory data management provisions.

1.5 Terms

a. Data subject
Any – directly or indirectly – identified or identifiable natural person to whom personal data relates. With regard to the data processing under this Policy, the data subject is primarily the Company's client, ex client, and those persons that intend to establish a client relationship with the Company, and the person whose data is managed by the Company relating to the service provision;

b. Personal data
Any information relating to the data subject – in particular the data subject's name, identification number, or one or more factors specific to the physical, physiological, mental, economic, cultural or social identity of that natural person or any conclusions to be drawn from such data regarding the data subject;

c. Sensitive Data
- Personal data concerning racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, or data concerning sex life,
- personal data concerning health status, abnormal passions or criminal personal data;

d. Consent

Voluntary and determined expression of the data subject's intent based on appropriately informed decision by which he or she unambiguously signifies consent to the processing of personal data – to full scope or for certain operations – relating to him or her;

e. **Objection**
The data subject's declaration by which data subject objects to the processing of his/her personal data, and requests that the data processing is cancelled, and the processed data are deleted;

f. **Data controller**
The natural or legal person, or organization without legal personality, which or who alone or jointly with others determines the purposes and means of the processing of personal data, makes decisions relating to data management (including the used tool) and implements them, or have them performed by the delegated data processor. The Company is the data controller with respect to any data processing under this Policy;

g. **Data management**
Irrespective of the method used, any operation or set of operations which is performed on personal data, in particular the collection, recording, organization, storage, alteration, use, retrieval, forwarding, disclosure, alignment or combination, restriction, erasure or destruction, preventing further uses, photo - voice or video recording, as well as recording the person's identifying physical characteristics;

h. **Data transfer**
The making available of data to specific third parties;

i. **Third Party**
A natural or legal person or organization with no legal personality other than the data subject, the controller and the processor;

j. **Disclosure**
The making available of data to anyone;

k. **Erasure of data**
Rendering data unrecognizable in such a way that its restoration is no longer possible;

l. **Destruction of data**
Complete physical destruction of the data carrier;

m. **Data processing**
Technical tasks related to the data management operation, regardless of the method and device used for the operations and the place of application, provided that the technical tasks are performed on the data;

n. **Data processor**
A natural or legal person or organization with no legal personality who or which, based on a contract concluded with the data controller – including contracting on the basis of legislative provisions – performs the processing of data;

o. **Contract**
An agreement concluded between the Company and the client for the purpose of using a service provided by the Company. The Contract may be concluded orally or in writing;

p. **Data concerning health**
Data concerning the data subject's physical, intellectual, spiritual condition, abnormal passions, and data relating to the circumstances of disease and death, the cause of death disclosed by the data subject or another person about the data subject or detected, examined, measured, mapped or derived by the healthcare network, as well as all data relatable to and affecting the foregoing (e.g. behaviour, environment, profession).

2. The data controller

Dental Holiday Bp. Kft (registered office: H-2030 Érd, Budai út 20. 1. em. 14.; company registration number: 13-09-191429; tax number: 25768259-2-13; represented by: Kornél Fülöp executive director).

3. Principles of data management

The Company as data controller shall act in accordance with the requirements of good faith and integrity, in cooperation with the data subjects. The Company shall enforce its rights and comply with its obligations pursuant to their intended purpose. During data management all data remains to be regarded as personal data until its relationship with the data subject is restorable. The relationship with the data subject is restorable if the data controller is in possession of the technical conditions that are required for the restoration. The data controller ensures that the data are accurate, complete and – if required for the purpose of the data management – up-to-date, and that the data subject can only be identified for the time required for data management purposes.

The Company puts emphasis on the personal data management principles set forth by Regulation (EU) 2016/679 (GDPR).

For this purpose, the Company manages personal data in accordance with the principles of lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality.

4. Purpose of data management

The data controller shall exclusively manage personal data for the specified purpose, in order to exercise rights and perform obligations. Every phase of the data management shall be in compliance with the purpose of the data management. Data shall be recorded and managed in a fair and lawful manner. The data controller shall endeavour to handle only personal data that is essential for the purpose of the data management to achieve the purpose, and which is suitable for this purpose. Health and personal data shall only be managed to the extent and duration necessary for the realization of the purpose. Data management falling under the scope of this Policy is always connected to a service provided by the Company as data controller, where the service is or was used by the data subject as client or with the purpose of obtaining such data the data controller established contact with the Company, or which service is provided by the Company to third parties with the cooperation or personal involvement of the data subject (e.g. representative or proxy of the data subject).

Data management falling under the scope of this Policy serve the following purposes

a. preparation, conclusion and execution of the contract concluded with the Company as data controller;
b. subject to specific consent, direct contacts by the Company with business acquisition and market research purposes (via mail, telephone, or other, electronic and other communication means);
c. following the termination of the contract, exercising rights and fulfilling obligations arising from the contract, particularly the enforcement of contract-based claims.

5. The data subjects

5.1 Clients

The Company primarily manages the data of natural persons with whom it is in a client relationship, therefore under the contract they use the service provided by the data controller. The Company also manages the data of the persons that used to be in a client relationship with the Company (ex-clients);

5.2 Other data subjects

In addition, the Company manages the data of natural persons that intend to establish a client relationship with the Company and contact the Company with the purpose of using its services. No client relationship is established until the contract is concluded for the service, however, the data subjects provide the Company with their data, primarily to enable the data controller to make an informed decision about establishing the legal relationship. Moreover, the Company also manages the data of natural persons that are affected by the contract between the Company and its clients, and whose data is required to be processed to perform the contract (legal representative of minor of limited legal capacity or incapacity, guardian of those incapacitated or with limited legal capacity).

6. Legal basis of data management

6.1 Consent of the client as data subject

The Company primarily manages the client's health and personal data based on the client's consent. The data subject implicitly provides health and personal data to the Company for the purpose of preparing and concluding the contract (legal basis for processing personal data). In the contract concluded with the Company the client consents to manage all personal data the handling of which is necessary to perform the contract.

If without managing the data the contract cannot be performed, in the absence of consent the contract may not be concluded. Failure to accept the Data Protection and Data Management Policy does not exclude concluding the contract.

The scope of data to be managed shall be specified by the Company in this Policy, in addition to information provided about the length of data processing, the transfer of data, engagement of a data processor and every fundamental fact and circumstance based on which the data subject is able to make an informed decision about whether to consent to the data management. By signing the Contract, the data subject consents to the data management specified under the Contract and in this governing Policy. If the management of the data is not necessary to perform the contract, the Company may only manage the data if it is voluntarily provided to it by the client. By completing the forms to record client's data, client provides consent to the management of his/her personal data as specified on the form. If client provides consent by way of a separate declaration, the Company shall provide the data subject exhaustive information regarding the declaration about the management of data.

6.2 Legislative provisions

If personal data management is prescribed by legislation, data management is obligatory. The Company shall inform the data subject about this fact.

Personal data can also be managed if it is impossible to obtain consent from the data subject or it would incur disproportionate costs and the management of personal data is necessary to enforce the legitimate interest of the data controller or a third party, and the enforcement of such interest is in proportion to the limitation of personal data protection rights.

7. Scope and management of data

a. Natural person's identification data: the aim of managing such data is to clearly identify the client, the data subject and keep contact. The Company manages the following data of the client, the data subject: name, date of birth, nationality, address, postal address, personal ID card (passport) number. Legal basis of data management is the consent provided by the client – primarily under contract - or a legal provision.
b. Telephone numbers and other contact details required to communicate with the client, the data subject: If provided by the client, the Company manages the client's telephone numbers and electronic mail addresses for communication purposes.
c. Data required for the conclusion of or decision about the contract for the service used or intended to be used, e.g. concerning the data subject.
    - Personal data (age and gender of the data subject),
    - Data relating to travel organization (if client requests travel agency services from the Company)
d. The following, generated in the context of service provision and use:
    - X-rays
    - Laboratory evidences
    - Photos taken of the status of teeth
e. Data relating to claims arising from contracts existing or terminated between the Company and its clients, and the enforcement of such claims: Based on the applicable legislation, claims may arise from contracts that have already been terminated; data relating to such claims and the eventual enforcement of such claims, and data to be statutorily retained are managed by the Company.
f. Data generated at the Company during establishing contact with customer services: All such data that are generated at customer services and in the course of the communication between customer services and the data subject. In this case, the processed data is related to the procedure initiated by the data subject, and to the contract, and are in close connection with contractual performance.
g. Phone conversation executed between the client, other data subject, and the Company: The Company may record the conversation between the client, the data subject and the customer service and in light of the governing law and the contract concluded with the clients, it may

process such voice recording. The client, the data subject is always informed about any recording prior to the conversation. Such voice recordings are stored and used by the Company for complaint handling, claims enforcement, settlement and quality assurance purposes. The legal basis for voice recording is the client's consent, and storage time is up to the end of the contractual relationship between the client and the Company.

8. The duration of data management

The Company shall delete the data when it becomes obvious that they will not be used in the future, so the purpose of processing the data ceased, and it is permitted by the related legislation. The Company shall also delete the data where it is requested by the data subject and erasure is permitted by legislation. The Company and its suppliers may keep processing personal data after the withdrawal of the consent by the data subject in order to perform their obligations or enforce their legitimate interest, provided that the enforcement of the legitimate interest is in proportion with the limitation of data protection rights.

In light of Act XLVII of 1997, health documentation shall be retained for 30 years after data recording, recordings made by diagnostic imaging procedures shall be retained for 10 years after making, evidence made from the recording shall be retained for 30 years after making. If further record keeping is not justified, the records shall be destructed.

9. Data transfer

9.1 General rules of data transfer

Data is only transferred based on the consent of the data subject or authorization provided by legislation. The Company shall only transfer personal or health data, where its legal basis in unambiguous, and its purpose as well as the recipient of the transferred data is clearly defined. The Company shall document the data transfer in any case, in a way that enables the justification of the procedure and its lawfulness. Documentation is primarily served by properly issued data requesting documents and those establishing fulfilment. Statutory data transfer shall be performed by the Company as data controller. In addition to the above, personal or health data may only be transferred with the express consent of the data subject. For the consent to be subsequently justified, it must be provided in writing. Written form can be omitted if the data transfer is of minor significance with regard to its recipient, purpose, or scope of data. Where the data transfer is subject to consent by the data subject, the declaration of consent shall be provided by the data subject in knowledge of the recipient and purpose of the data transfer. The prohibitions and limitations above are governing even where the client relationship is terminated.

Regular data transfers

- The Company, the data controller shall transfer the client's personal and health data to its suppliers; the client consents to this data management upon contract conclusion and waives the data controller from the obligation of confidentiality in this regard. The suppliers engaged by the Company are listed in chapter "12 Data processors of the Company". Data shall exclusively be transferred for the purposes specified in point 4, where appropriate. The recipient shall only use the transferred data for the purpose of the data transfer, and only transfer the data to third parties with the Company's consent. The data controller shall ensure that the data security requirement and the conditions for lawful data management are provided at the recipient of the data as well.
- Where the client gives such an assignment to the Company based on which the data transfer is required, the Company may transfer the data to the extent necessary to fulfil the assignment and waives the data controller from the obligation of confidentiality in this regard.

Data transfer to third countries

- The Company may transfer data to data controllers managing data in third countries or to data processors processing data in third countries provided that the client, the data subject expressly consented to such data transfer and the data controller or data processor meets the requirements set forth by Chapter V of Regulation (EU) 2016/679 (GDPR).

Data transfers to EEA-states shall be regarded as data transfer within the territory of Hungary.

10. Management of data files

The Company shall ensure that the method and data content of the records are in accordance with the current legislation in force. Legislation-based data processing is obligatory, the clients, data subjects may request information in this regard. The Company shall ensure that data processed for other purposes are properly and logically separated. The Company shall handle the electronic and paper-based records according to standard principles, taking into account the differences resulting from the different media of the data records. The principles and obligations under this Policy are applicable to both electronic and paper-based records. The Company ensures by way of the records system structure, the definition of entitlements and other organisational measures that data included in the personnel records may only be disclosed to such employees and other persons acting in the interest of the Company who require them in order to perform their scope of work and responsibilities. In compliance with the data security requirements, access to the records is ensured by the Company to such third parties cooperating as data processors that provide a service to the Company relating to the management of data.

The Company's electronic records comply with the data security requirements; the records ensure that the data can only be accessed for limited purposes, and by persons for whom it is required to perform their responsibilities. Where possible, the Company seeks to enforce the principle of minimum data so that the individual employees and other persons acting in the interest of the Company can only access the necessary personal data. For the management of data files, their secure storage, the access rights and the use of data and documentation, the policies and instructions in force within the Company's organisation shall be appropriately governing. These policies and instructions serve the enforcement of the principles and provisions of this Policy and the governing legislations, primarily those of the Act on Privacy.

11. Data security

The Company as data controller ensures data security. For this purpose, it shall take the necessary technical and organizational measures with regard to data files stored by IT devices and traditional, paper-based data media. It shall provide that the data security rules prescribed by the relevant legislations are enforced. It shall also provide data security, take all the technical and organizational measures and establish procedural rules that are necessary to enforce governing legislations and the data protection and confidentiality regulations. The Company as data controller shall protect the data by the appropriate measures against unauthorized access, alteration, transfer, disclosure, erasure or destruction, as well as unintentional destruction or damage, and becoming inaccessible due to any alteration in the technique used. Provides the proper relevant preparation of the concerned employees in order to enforce the conditions for data security. When determining and applying the data security measures, the Company considers the current development level of technology. From multiple data management options, it shall select the one that provides the highest level of personal data protection, except where it would mean unproportionate difficulties.

12. The Company's data processors

12.1 General rules of data processing

The Company reserves the right to engage data processors based on permanent or ad hoc assignment. Permanent type of data processing may be primarily required to perform administrative tasks relating to client relations and service provision, and to maintain the information system. For engaging a data processor, the relevant legislative provisions, primarily those of the Act on Privacy, are governing. Data processors shall only be engaged subject to a written agreement. Upon request the Company shall notify the data subjects about the person of the data processor and the details of the data processing activity, in particular, the performed operations and the instructions given to the data processor. The rights and obligations of the data processor relating to the processing of personal data are determined by the Company as data controller under the scope of the relevant legislations. The Company shall be held liable for the lawfulness of the operation instructions relevant to data processing. Within the scope of its activities, and within the framework provided by the Company, the data processor shall be liable for the

processing, alteration, erasure, transfer and disclosure of personal and health data. During performing its activity, the data processor may assign other data processors with the Company's consent. The data processor shall not make substantive decisions concerning the data management, it shall only process the acquired personal or health data according to the Company's commands, it shall not perform data processing for own purposes, and shall store and retain personal and health data in accordance with the Company's orders. By establishing the appropriate contractual conditions and organizational and technical measures, the Company ensures that the rights of data subjects are not violated during the data processor's activity, and that the data processor can only acquire personal and health data if it is indispensable to carry out its task.

12.2 Scope of data processing

The scope of data processors engaged by the Company can change.

The Company typically applies the following suppler categories:

- Healthcare companies supplementing the Company's provision of services
- External laboratories
- Accountants
- IT contractors
- Accommodation providers in partnership with the Company

13. Erasure and archiving of data

The Company as data controller shall delete the personal and health data, if

a. processing is unlawful;
b. it is requested by the client, the data subject (with the exception of statutory data management);
c. the data is incomplete or incorrect – and this state cannot be lawfully remedied –, provided that erasure is not excluded by law;
d. the purpose of data management has ceased, or the statutory data storage period has expired;
e. it was ordered by the court or by the Hungarian National Authority for Data Protection and Freedom of Information.

The client, the data subject may request the erasure of the personal data managed based on voluntarily provided consent. In the absence of a request by the client, the data subject, the Company shall delete the data when the purpose of the data management has ceased. In the absence of any other purpose, the Company shall keep records of the data as long as their use may be required in a separate procedure. Instead of deletion the Company shall lock the data where it is requested by the client, the data subject, or where based on the available information it can be assumed that erasure would violate the legitimate interests of the client, the data subject. The locked data shall only be managed while the purpose of the data management – excluding the erasure of the data – prevails. The Company shall mark the processed data where the client, the data subject disputes their correctness or accuracy, but the incorrectness or inaccuracy of the data cannot be established unambiguously. In case of statutory data management, the provisions prescribed by legislation shall be governing for the erasure of data. In case of erasure, the Company shall make the data impossible to be used for personal identification. Where prescribed by legislation, it shall destruct the medium containing the data. Where the Company remains entitled to manage the data despite the withdrawal of the data subject's consent, the purpose limitation principle of the data management also prevails, and the Company may process the data even where the consent of the data subject is withdrawn. In such cases the data controller shall provide information to the client, the data subject about the purpose and legal basis of data management.

14. The rights of the client and the data subject, and enforcement of such rights

The client, the data subject is entitled to:

- the right to information

The Company shall inform the data subject about this fact prior to processing the data. The information may be provided by way of disclosure of the Policy about the detailed rules of data management by the Company and calling the attention of the data subject to this. Data subjects may request information about the management of their data. Upon request of the client, the data subject, the Company shall provide information about the data subject's data managed by the Company or data processed by the engaged data processor, the sources of such data, the purpose of data management, its legal basis, duration, and the data processor's name, address and activity in connection with the processing of the data; in addition – where the personal and health data of the client, the data subject is transferred – the legal basis and recipient of the data transfer. The Company shall provide the information within the shortest possible time after the submission of the client's, the data subject's relevant request, but within 30 days the latest, in an understandable form in writing. Information provision is free of charge, provided that no request for the same scope of data was submitted in the current year. In other cases, a fee can be applied. Any fees paid shall be reimbursed where data was unlawfully processed, or the request for information resulted in rectification. Information provision may be denied in cases specified under legislation.

- right of access
- right of rectification
  The client, the data subject may request that the Company rectifies any incorrectly recorded personal data. Provided that based on the data to be rectified, permanent data provision is generated, if necessary, the Company shall notify the recipient of the provided data and calls the attention of the client, the data subject to the fact that the rectification must be initiated at other data controllers as well.
- right to erasure
  The client, the data subject may request the erasure of his/her personal and health data with the exception of statutory data management. The Company shall inform the client, the data subject about the erasure. Where data management based on consent is a condition to establishing and maintaining a legal relationship, the Company shall inform the client, the data subject of this fact and the expected consequences. The Company is entitled to reject the erasure of personal and health data where the management of data is based on legislation and required for the enforcement of the Company's legitimate interest. In the event of rejecting to fulfil the erasure request, the Company shall inform the client, the data subject about the reason for the rejection.
- the right of limitation
- the right of data portability
- the right of objection
  The data subject is entitled to object to the management of his/her personal data under the provisions of Act CXII of 2011 on Informational Self-Determination and the Freedom of Information.
- right to be informed about rectification, erasure or restriction
- right of objection to automated decision-making

14.1 Enforcement of the right of the client, the data subject

The client, the data subject is entitled to submit a request for information, rectification or erasure to the Company in person, or by a letter addressed to the Company's registered office or site. The Company reserves the right to only perform the requested right enforcement following the identification of the client, the data subject.

14.2. Complaint handling of the client, the data subject and liability of damages

Where the Company does not perform the concerned request for rectification, locking, or erasure, it shall provide written information within 30 days of receiving the request for rectification, locking, or erasure about the factual and legal grounds for the rejection. In case of rejecting the request for rectification, erasure or locking, it shall inform the data subject about the possibility to seek legal remedy at court, or at the Hungarian National Authority for Data Protection and Freedom of Information. In the event of information provision, rectification, erasure or objection the Company shall act in accordance with the governing legislative provisions. In case of impairment of rights of the client, the data subject,

they are entitled to request examination by a manager superior to the person acting on behalf of the Company.

Where the Company rejects the information provision, and fails to complete the request for rectification, erasure or locking, the client, the data subject is entitled to seek remedy at the relevant competent court or at the Hungarian National Authority for Data Protection and Freedom of Information. Upon request the Company shall inform the client or data subject about the available legal remedy measures. For any damage caused as a result of unlawful data management, the Company shall be held liable in accordance with the relevant laws. The Company shall indemnify for any damage caused by the unlawful processing of the client's or data subject's data or beaching the data security requirements. The Company shall be held liable for any damage caused by the data processor against the client or data subject. The Company shall be waived from any liability if it can prove that the damage was caused by unavoidable cause falling outside the scope of data management. Damages are irrecoverable to the extent they arise from the intentional or seriously negligent conduct of the damaged party. For the general, civil liability of the Company the rules of the Civil Code are governing. The Company shall inform the client, the data subject about the right enforcement options.

15. Contact information

15.1 Data controller

Dental Holiday Bp. Kft.

H-2030 Érd, Budai út 20. 1. em. 14.

Telephone: +44 20 396 647 85

E-mail: office@dentalbp.com

Website: www.dentalbp.com

15.2 Data Protection Authority

Hungarian National Authority for Data Protection and Freedom of Information

H-1125 Budapest, Szilágyi Erzsébet fasor 22/C.

Postal address: H-1530 Budapest, P.O. Box: 5.

Telephone: +36 1 391 1400

Fax: +36 1 391 1410

E-mail: ugyfelszolgalat@naih.hu

Website: https://naih.hu