PRIVACY AND COOKIES POLICY OF HÁROMSZÁZHATVAN DENTAL KFT.

Our dentistry (Háromszázhatvan Dental Kft.) is committed to protect the personal information that you provide us when you visit our clinic in person or our sites www.360dental.hu or www.fogaszatictbudapest.hu (the "Site"). This Privacy and Cookies Policy describes how your personal information is collected, used, protected and shared when you visit our website - both anonymous data and personally identifying data- or engage with us in other related ways, including any sales, marketing or medical threatments.
During the processing of any personal data we respect the legal requirements and ensure the closed management of the data. We comply with the provisions of the current Data Management Act and, based on this, we reserve the right to comply with this at any time without prior notice due to possible changes in the law.

Data controller

Name:	**Háromszázhatvan Dental Kft.**
Headquarter:	1135 Budapest, Kerekes utca 1/A II/2.
E-mail:	haromhatvandental@gmail.com
Telephone:	+3630-2439-995
Websites:	www.360dental.hu, www.fogaszatictbudapest.hu
Tax number:	27538034-2-41
Company registration number:	01-09-393779
Data protection officer (DPO):	Dr.Bedő Zsombor, CEO
Creator of the privacy policy:	Forgon Anikó (official DPO)
Effective date of the regulation:	2023.03.15.

This data protection policy can only be used in relation to our institutions and its use elsewhere in whole or in part without the permission of the owner is prohibited and will result in legal proceedings.

Guidelines applied during data management

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

Regulations and laws used during data management

We apply the following legislation in relation to the care of our patients:

- Regulation (EU) 2016/679 of the European Parliament (April 27, 2016) on the protection of natural persons with regard to the processing of personal data and on the free flow of such data,
- CLIV law of 1997 on healthcare (hereinafter: Eütv.),
- XLVII law of 1997 on the management and protection of healthcare related personal data,
- CXII law of 2011 on the right to information self-determination and freedom of information.

Our organization units, where your data is processed:

Due to the complexity of our activities, we have several organizational units, which will manage the data. This policy applies to all our units.

Our organizational units:

- Reception
- Outpatient treatment
- Accounting & finance
- Human resources
- Marketing
- Administrative

Priority data management areas

Data management related to the provision of healthcare services.
Legal basis for data management:
The Data Controller, as a healthcare provider, has a data management obligation. Due to the nature of our institution, the affected parties contact us on a voluntary basis (consent), so the provision of personal data is also done on a voluntary basis and is therefore considered consent to the regulated use.

Personal information we collect may include the following provided by you during booking (via online site – foglaljorvost.hu or via email or mobile call):

- First- & last name (identification)
- Mobile number (to keep in touch)
- E-mail (to keep in touch)
- Date of appointment (service provision)

The data gathered and processed at the time of patient admission are as follows:

- First- & last name
- Birth name
- Maiden name
- Birthplace & -time
- Your mother's name
- Billing address
- Possible place of residence
- Social security identification number (TAJ in Hungary)
- Mobile number
- Contact or authentication data
- E-mail address
- Information revealing job position, religious belief and ethnic origin, **if it is relevant for the provision of health care services**

In addition to the list above list, the following information might be collected according to different reasons:
- In relation to medical care (sensitive information):

- The data required for the anamnesis with the discretion of the attending doctor like medical history, health data, genetic data, family background, possible sensitivities, allergies, etc.
- People to be notified in case of urgency

- In relation to non-medical care:

- Copies of documents and certificates required to establish an employment relationship
- Contracts and other documents related to other economic operators

-In relation with marketing activities:

- Email addresses for use in the database related to newsletters

-In relation with billing activities:

- Tax number of economical partner
- Bank account number of economical partner
- Patient's health fund identifier

In addition to the above, we only provide any data upon official request, but here also for regularity (legally verified request, participation of only authorized persons in the transfer, regularity of data transmission).
The people providing the data have the right to request information about the management of their personal data at any time. Furthermore, they have the right to update, modify, or request deletion of their personal data, except for information, that is required by other legally regulated retention obligations, or if they are regulated in regulations, for example employment data (Labour law of 2012 of Hungary). In addition, they can object to the processing of their personal data, and in the event of a violation of their rights, they can go to court.

Length of data management

The medical documentation has to be kept - with the exception of the recordings made with the image diagnostic procedure and the findings made from it - for 30 years; - the final report for 50 years; - the recording made with an image diagnostic procedure for 10 years; - the record of the recording must be kept for 30 years, the mandatory storage period for orders is 5 years.

Retention period for non-medical documentation:

a.) until the goal is achieved

b.) if the date (or its modification) may have any legal effect, or is relevant for the enforcement of a legitimate interest, or is necessary to prove the fulfillment of a legal obligation, Háromszázhatvan Dental Kft. will retain the data for the general limitation period or until the existence of the legitimate interest.

c.) accounting and invoicing documentation is usually 10 years according to the Accounting and Taxation Act in force at all times

d.) the retention of labor and HR documents is mandatory until the end of the company's operations

The individual documents are destroyed according to the set deadline andin accordance with the laws in force at the time of destruction, in a closed system, only within the framework of the institution, using a document shredder in the case of paper-based data carriers, with a full guarantee of destruction.

Data of external parties/data processors used during data management

The prior consent of the data subject (patient) is not required to use these service providers, but to inform is mandatory.
Considering that the contractual partners may change, we do not mention all of them by name in the regulations, but we will provide information on them at any time upon request.
These service providers could be:

- laboratories
- dental laboratories
- external diagnostic service providers
- external healthcare providers

Webhosting provider:

- Rackhost Zrt.
- Tax number: 25333572-2-06
- Company registration number: 06 10 000489
- Headquarter: 6722 Szeged, Tisza Lajos körút 41.

Website manager:

- Cyberkinetic Kft.
- Tax number: 13457990-2-13
- Company registration number: 13 09 102621
- Headquarter: 2600 Vác, Szegfű utca 40.

Online booking platform (Foglaljorvost Online Kft.):

- Foglaljorvost Online Korlátolt Felelősségű Társaság
- Tax number: 25307490-2-12

- Company registration number: 12 09 009222
- Headquarter: 3043 Egyházasdengeleg Petőfi út 2.

Google cookies:

- Google LLC
- Headquarter: 1600 Amphitheatre Parkway, Mountain View, CA 94043, United States
- Mobile number: 650-253-0000
- Website: www.google.com

When engaging all external service providers, the following points are regulated and observed when carrying out the activity. These are in particular:

- in all cases, we request the service provider's own policy
- when transferring data, if it is done electronically, we take care of the security of the data carriers
- if data is transferred on paper, we make sure that it does not fall into the hands of unauthorized persons
- we only transfer data necessary for the given activity
- in all cases, the fact of handover can be tracked, if this would mean a larger quantity, we will take a separate record of it.

Applied regulations for CCTV surveillance cameras

Purpose of data management: asset protection

The camera in the patient waiting room monitors those entering the surgery and provides asset protection. The camera installed in the office specifically protects property and does not see the dental chair under any circumstances, and does not watch our patients during treatment.

The whole area of the clinic is monitored by cameras in accordance with the current laws and regulations on information, data management, personal and property protection, as well as private investigative activities. (see CXXXIII. Law of 2005 Information law, European Data Protection Board and NAIH position, current legislation).

The camera system overwrites its storage space every 48 hours and deletes the events of the previous two days. The data controller undertakes to handle the data in a closed system, not to provide it to third parties and only authorized persons can handle it.

Cookies policy

By using our websites (through any device) you agree that this Cookie Policy applies to that use in addition to any other terms and conditions which may apply. We reserve the right to make changes to our Cookie Policy. Any such changes shall appear here and become effective immediately. Your continued use of our websites is taken as meaning that you agree to our Policy and any such changes.

A cookie, also known as web cookie, or browser cookie, is usually a small piece of data sent from a website and stored in a user's web browser while a user is browsing a website. When the user browses the same website in the future, the data stored in the cookie can be retrieved by the website to notify the website of the user's previous activity.

Cookies pose no risk since they do not contain virus in any form nor do they spy on your PC content to compromise security. They are used to make online surfing faster and easier by make the sites you have visited remember who you are, like remembering your IP address or passwords, along with your own preferences such as items similar to what you looked for in your last visit.

How our cookies help us to improve our business:

- Improve the speed/security of the site
- Make our website work as you would expect
- Continuously improve our website for you
- Make our marketing more efficient

Our company uses cookies on the websites we operate below:
www.360dental.hu
www.fogaszatictbudapest.hu

Our institution uses the following third-party cookies on its website, i.e. cookies that were not created by us, but by an external service provider:
Google Analytics cookies
Google Ads cookies
Instagram cookies

Possibilities of legal remedy

You can file a complaint to the National Data Protection and Freedom of Information Authority, whose details are as follows:

Name:	**NAIH**
Headquarter:	1055 Budapest, Falk Miksa utca 9-11.
E-mail:	ugyfelszolgalat@naih.hu
Phone:	061-391-1400
Fax:	061-391-1410
Website:	http://www.naih.hu
Address:	1374 Budapest, Pf. 603.

How do we handle a data breach incident?

A data protection incident is an injury that may result in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure or unauthorized access to personal data transmitted, stored or otherwise handled.
The Company's manager is responsible for preventing and managing data protection incidents and complying with the relevant legal regulations.
IT systems must log accesses and access attempts.
The employees of the company who are entitled to control should notice a data protection incident during the performance of their duties, and they must immediately notify the head of the company.
The employees of the Company are obliged to report to the head of the Company or to the employer's rights practitioner if they notice a data protection incident or an event indicating such.
A data protection incident can be reported to the Company's central e-mail address and telephone number. When a data protection incident is reported, the data protection officer examines the report, during which the incident must be identified and it must be decided whether it is a real incident or a false alarm. The following shall be examined and established:Az incidens bekövetkezésének időpontját és helyét

A.) The description, circumstances and effects of the incident
B.) The scope and number of data affected during the incident
C.) The range of persons affected in relation to the data
D.) A description of the measures taken to prevent the incident
E.) A description of the measures taken to prevent, eliminate and reduce the damage

In the event of a data protection incident, the affected systems, persons, and data must be demarcated and separated, and evidence supporting the occurrence of the incident must be collected and preserved. After that, you can begin to repair the damage and restore legal operation. A record of data protection incidents must be kept, which includes the range of personal data affected, the range and number of persons affected by the data protection incident, the date of the data protection incident, the circumstances and effects of the data protection incident, the measures taken to remedy the data protection incident, and other data specified in the legislation prescribing data management .