DATA PROTECTION INFORMATION - PRIVACY POLICY

Buda Health Center (hereinafter referred to as the "data controller") handles personal data in connection with the provision of its healthcare services.

DATA CONTROLLER DETAILS

Data Controller Details	Data Protection Officer's Details
Buda Health Center LLC (BHC) Represented by: Dr István Csernavölgyi Chief Executive Officer	Dr Ádám Kéri Dr Szonja Kéri, Dr Tamás Sándor Kéri Chief Data Protection Officer: Dr Ádám Kéri
1-3 Királyhágó street Budapest 1126	Mailing address: 1281 Budapest, Post Office Box.12.
Company registration number Cg.01-10-141707. Website: https://bhc.hu/en E-mail adress: dpo@bhc.hu	E-mail adress: adam.keri.office@icloud.com

METHOD OF REGULATION

This document outlines **the key aspects** of data management, with a focus on clarity.
Should you have any questions, please contact our data protection officers on our website at https://online.bhc.en

NAMES OF THE AREAS PRESENTED
1. THE HOSTING PROVIDER OF THE HTTPS://BHC.EN WEBSITE OPERATED BY THE DATA CONTROLLER, AND THE OPERATOR OF ITS MOBILE APPLICATION
2. DATA MANAGEMENT RELATED TO COOKIES USED ON THE HTTPS://BHC.EN WEBSITE, AS WELL AS DATA COLLECTED BY THE MOBILE APPLICATION
3. GENERAL NEWSLETTER DELIVERY
4. SENDING EXCLUSIVE (SPECIAL) NEWSLETTERS AND CAREGIVER (PERSONALIZED) NEWSLETTERS
5. CONTACTING CUSTOMER SERVICE /by phone; or by emailing info@bhc.hu (except: For the Private Inpatient Care Unit); as well as magankorhaz@bhc.hu as well as using the e-mail address in magankorhaz@bhc.hu for Private Inpatient Care/
6. REQUEST FOR PROPOSALS FOR OUR HEALTHCARE SERVICES
7. REGISTRATION FOR THE CUSTOMER SERVICE FEATURE ON THE WEBSITE OR MOBILE APP, AND CREATION OF A PERSONAL CUSTOMER ACCOUNT
8. USE OF THE CUSTOMER SERVICE FUNCTION VIA THE ONLINE PLATFORM OR MOBILE APP, I.E., DATA PROCESSING RELATED TO PERSONAL CUSTOMER ACCOUNTS
9. OPERATION OF THE CORPORATE DATA EXCHANGE PORTAL; AS WELL AS THE SUPPLEMENTARY DATA MANAGEMENT RULES FOR OCCUPATIONAL HEALTH EXAMINATIONS (INCLUDING: SCREENING TESTS)
10. ONLINE APPOINTMENT BOOKING VIA THE WWW.FOGLALJORVOST.HU WEBSITE
11. PATIENT REGISTRATION (DATA VERIFICATION), MEDICAL RECORDS, AND INVOICING
12. HANDLING OF MEDICAL REPORTS SENT TO THE DATA CONTROLLER VIA E-MAIL OR UPLOADED TO PERSONAL ONLINE CUSTOMER ACCOUNTS
13. TELEPHONE CONSULTATION
14. VIDEOCONSULTATION
15. COMPLAINT HANDLING

1. THE HOSTING PROVIDER OF THE HTTPS://BHC.EN WEBSITE OPERATED BY THE DATA CONTROLLER, AND THE OPERATOR OF ITS MOBILE APPLICATION

A web hosting service is an internet-based service in which the resources of a server are shared among multiple users. Each user occupies a dedicated storage space allocated by the system, the public content of which is accessible under a unique domain name. In the present case, the domain name is https://bhc.hu.

For both the https://bhc.hu website and the https://online.bhc.hu subsite, the data controller uses the services of a hosting provider to store the websites, ensure their continuous availability, and provide the necessary technical infrastructure. The hosting provider acts as a data processor. Its details are as follows:

Name of hosting provider:	**MICROSOFT CORPORATION**
Registered office of the hosting provider:	WA 98052, One Microsoft Way Redmond, USA
Email	dpoffice@microsoft.com
Telephone contact:	+353 1 706 3117

The hosting service is provided through AZURE, and the related privacy notice is available here: https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-dsr-azure
MICROSOFT CORPORATION, as a data processor, is not a company registered within the European Union and therefore qualifies as a so-called third-country company. However, since 17 July 2023, it has participated in the data protection frameworks in force between the EU and the USA, the United Kingdom and the USA, and Switzerland and the USA (Data Privacy Framework, https://www.dataprivacyframework.gov/s/participant-search/participant-detail?id=a2zt0000000KzNaAAK&status=Active). Accordingly, its compliance with data protection requirements has been established. The contact details of the company's data protection officer are available at: https://www.dataprivacyframework.gov/s/participant-search/participant-detail?id=a2zt0000000KzNaAAK&status=Active.
For both the https://bhc.hu website and the https://online.bhc.hu subsite, the data controller also uses a data processor for the maintenance (e.g. correcting functions, installing security updates, etc.) and operation of the web framework, as well as for providing support services. The details are as follows:

Name of the mobile app provider:	**SMP Solutions Zrt.**

Registered office of the service provider:	1138 Budapest, Madarász Viktor utca 47-49. 2. ép. 3rd floor
Location of the service provider:	1139 Budapest, Fiastyúk utca 53.
Location of the service provider:	1139 Budapest, Fiastyúk utca 69.
Location of the service provider:	1139 Budapest, Fiastyúk utca 71/b
Location of the service provider:	1138 Budapest, Madarász Viktor utca 47-49. 1. ép. Ground floor
Company registration number:	Cg.01-10-140383.
Contact details of the service provider:	smp@smp.hu https://smpsolutions.hu

The data processor performs the above tasks with the assistance of the following sub-processor:

Sub-processor name:	**Brainsum Ltd.**
Registered office of the sub-processor:	2836 Baj, Bem József utca 27.
Sub-data processor branch:	8652 Siójut, 89/9. hrsz.
Company registration number:	Cg.11-09-024421.
Contact details of the sub-processor:	info@brainsum.com

The data controller **uses the assistance of the following data processor** for the operation of the https://online.bhc.hu sub-page:

Name of hosting provider:	**MOANA SOFTWARE HUNGARY LTD.**
Registered office of the hosting provider:	1025 Budapest, Zöldlomb utca 32-34/b 4th floor, 16.
Branch of the hosting provider:	3100 Salgótarján, Ruhagyári út 32.
Company registration number:	Cg.01-09-699603.
Hosting provider contact details:	info@moanasoftware.com https://www.moanasoftware.com

The data controller **operates a mobile application** called **BHC MyHealth**, which service runs on users' smartphones. For the provision of this mobile application, the Data Controller also uses the assistance of the following data processor:

Name of the data processor:	**SMP Solutions Zrt.**
The registered office of the data processor:	1138 Budapest, Madarász Viktor utca 47-49. 2. ép. 3rd floor
Location of the data processor:	1139 Budapest, Fiastyúk utca 53.
Location of the data processor:	1139 Budapest, Fiastyúk utca 69.
Location of the data processor:	1139 Budapest, Fiastyúk utca 71/b
Location of the data processor:	1138 Budapest, Madarász Viktor utca 47-49. 1. ép. Ground floor
Company registration number:	Cg.01-10-140383.
Contact details of the data processor:	smp@smp.hu https://smpsolutions.hu

When **using the online help desk feature**, users are also identified in Microsoft Azure Active Directory, i.e. using a cloud-based service from **MICROSOFT CORPORATION** (WA 98052, One Microsoft Way Redmond, USA), so MICROSOFT CORPORATION acts as a data processor. Details of the Azure service are available here: https://azure.microsoft.com. The Privacy Policy for the service is available here: https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-dsr-azure
MICROSOFT CORPORATION, as a data processor, is not a company registered in the European Union; thus, it qualifies as a so-called third-country company, but since 17.07.2023 it has been a party to the data protection frameworks (Data Privacy Framework, https://www.dataprivacyframework.gov/s/participant-search/participant-detail?id=a2zt0000000KzNaAAK&status=Active) in force between the EU and the USA, the United Kingdom and Switzerland and the USA .). With this in mind, its data protection compliance has been achieved. Contact details of the company's Data Protection Officer are https://www.dataprivacyframework.gov/s/participant-search/participant-detail?id=a2zt0000000KzNaAAK&status=Active.

2. DATA MANAGEMENT RELATED TO COOKIES USED ON THE HTTPS://BHC.EN WEBSITE, AS WELL AS DATA COLLECTED BY THE MOBILE APPLICATION

Anonymous visitor identifiers (**cookies**) are **files or pieces of information** that are **stored on the user's computer**, internet device, smartphone, or iPad **when visiting the website**. Cookies are used to facilitate the operation of the website, to enable communication with website visitors (e.g., displaying marketing messages), and to collect statistical and other information about website visitors (see, for example: IP address, time of access to the website, navigation on the website, name of the previous website visited).
On the basis of legitimate interest, the data controller uses cookies that are strictly necessary for visiting and operating the website. In addition, based on the legal basis of the data subject's consent, data controller uses cookies for other purposes, such as statistical data collection and marketing. **These cookies can be disabled by the user/data subject or deleted at any time from the user's/data subject's computer (under the "Settings" menu).**

MyHealth mobile application
The BHC MyHealth mobile app collects anonymous data about its use and status. The data cannot be linked to a user; users cannot be identified or tracked based on this data.

The BHC MyHealth mobile app accesses notifications on the user's mobile phone to notify the user of any possible events. Notifications can be disabled in the settings menu of smartphone applications.

The BHC website:
Description of the cookies used by the https://bhc.hu website:

Cookies necessary for the website to operate:
Essential cookies help make the website function properly by enabling basic features such as navigation and access to secure areas of the site. The website will not function properly without these cookies.

Name of the cookie	Function of the cookie	Legal basis	Duration

ARRAffinity	This is to distribute the website's traffic across multiple servers to optimize response times.	Data Controller's legitimate interest.	Until the end of the session.
ARRAffinitySameSite	This is to distribute the website's traffic across multiple servers to optimize response times.	Data Controller's legitimate interest.	Until the end of the session.
bscookie	This cookie is used to identify visitors through the application. This allows visitors to log in to a website through the LinkedIn app, for example.	Data Controller's legitimate interest.	1 year
CookieConsent	Stores the user's consent status regarding cookies for the current domain.	Data Controller's legitimate interest.	1 year
Language	Saves the user's preferred language on the website.	Data Controller's legitimate interest.	30 days
li_gc	Stores the user's consent status regarding cookies for the current domain.	Data Controller's legitimate interest.	180 days

Cookies that track preferences:

Preference cookies allow the website to remember information that changes the way the site functions or appears, such as your chosen language or the region you are in.

Name of the cookie	**Function of the cookie**	**Legal basis**	**Duration**
lidc	It records which server cluster is serving the visitor. This is used in connection with load balancing to optimize the user experience.	The data subject's consent.	1 day

Cookies for statistical purposes:

Statistical cookies help website owners understand how visitors interact with their sites by collecting and reporting anonymous information.

Name of the cookie	Function of the cookie	Legal basis	Duration
_ga	It registers a unique identifier, which is used to generate statistical data on how visitors use the website.	The data subject's consent.	2 years
_gat	This is used by Google Analytics to reduce the number of requests.	The data subject's consent.	1 day
_gid	It registers a unique identifier, which is to generate statistical data on how visitors use the website.	The data subject's consent.	1 day
AnalyticsSyncHistory	Used for synchronizing data with a third-party analytics service.	The data subject's consent.	30 days
ln_or	It collects statistical data on users' behaviour on the website. It is used by the website operator for internal analysis.	The data subject's consent.	1 day

Marketing cookies:

Marketing cookies are used to track visitors on the websites. The aim is to display ads that are relevant and appealing to individual users, and thus more valuable to publishers and third-party advertisers.

Name of the cookie	Function of the cookie	Legal basis	Duration
_fbp	Facebook uses it to deliver a range of advertising products, such as real-time bidding by third-party advertisers.	The data subject's consent.	3 months
ads/ga-audiences	It is to detect whether the user intends to leave the page by moving the cursor. This allows the website to display certain pop-ups to keep the users on the website or convert them into customers.	The data subject's consent.	Until the end of the session.
bcookie	This is used by LinkedIn to track the use of embedded services.	The data subject's consent.	1 year

li_sugr	It collects data on user behaviour and interactions to optimize the website and deliver more relevant ads on the site.	The data subject's consent.	3 months
UserMatchHistory	It ensures visitors' browsing security by preventing cross-site request forgery.	The data subject's consent.	30 days

3. GENERAL NEWSLETTER DELIVERY

The data controller sends a general newsletter to interested parties regarding its services. The condition of sending newsletters is always based on the **prior consent of the data subject**. Please note that **you may withdraw your consent at any time**, **without providing a reason**, either by clicking the unsubscribe link or by contacting us in any form.

You can **subscribe** to the General Newsletter by visiting the data controller's website, where you can request this service by providing your name and the email address - where you wish to receive the newsletter; however, it can also be done if the interested party indicates this request to the customer service, and a customer service representative records this information in the internal administrative system.
The data provided from the internal administrative system is sent to the data processor responsible for sending the newsletter, who always sends a confirmation email to the new subscriber. **To complete your registration, you must return the confirmation within 72 hours.** Following this, actual subscription to the General Newsletter mailing list will take place. If the email address provided is already associated with another newsletter subscriber in the system, the person attempting to subscribe will receive only an **informational e-mail** regarding this fact, but the subscription to the newsletter will not be finalized unless an alternative email address is provided.

You can **unsubscribe** from the General Newsletter service in person at the customer service desk by indicating your request when you visit in person; the customer service staff will then record your request to unsubscribe in the internal administrative system. At the bottom of every newsletter we send out, there is a link labelled "Unsubscribe"; you can also use this link to unsubscribe from the service.
The request to unsubscribe is forwarded from the internal administration system to the data processor responsible for sending the newsletter, who, in this case, sends the patient a **notification email** confirming the unsubscription and immediately deletes the personal data processed for this purpose.

Please note that you cannot subscribe to or unsubscribe from the newsletter in the BHC MyHealth mobile app; as the mobile app does not support the newsletter feature.

Data management is carried out as follows:

The aim of data management	**Information about the data controller's services and current promotions.**
The legal basis for data management:	The data subject's **consent** pursuant to Article 6(1)(a) of the GDPR, **which may be withdrawn at any time without giving a reason.**
Description of the legitimate interest:	The data management is not based on a legitimate interest.

Categories of data subjects:	Natural persons who have subscribed to the General Newsletter.
Categories of personal data processed:	The data subject's name, email address for newsletter delivery, and the type of newsletter requested.
Source of personal data:	The data is provided by the data subject themselves.
The duration of data management:	We process the data until the **data subject withdraws their consent** (or unsubscribes); or, in the case of a subscription request, until the **72-hour confirmation period** specified in the data controller's response email **expires without result** (after which a subscription request not confirmed by the data subject within 72 hours will be deleted).
Recipients (subjects of data transmission):	**MOANA SOFTWARE MAGYARORSZÁG LLC.** (registered office: 1025 Budapest, Zöldlomb Street 32-34/b, 4th floor 16., Cg.01-09-699603., contact details: info@moanasoftware.com, website: https://www.moanasoftware.com) as web hosting provider (and also as a data processor), it processes the data uploaded to the data controller's internal system (in this case, it forwards requests to subscribe to, unsubscribe from, or inquire about the newsletter, but does not store any related data itself). **Brainsum Kft.** (registered office 2836 Baj, 27 Bem József Street, Company registration number: Cg.11-09-024421., website: https://brainsum.com, contact details: info@brainsum.com), As a data processor and hosting provider, it processes the data uploaded to the data controller's website (https://bhc.en) (for example, when users subscribe to the newsletter there); and this data processor carries out the developments requested by the data controller. A **RAAB SOFTWARE Kft.** (9024 Győr, 36 Szigethy Attila Street, 3rd Floor, Apartment 6, Cg.08-09-032732.,contact details: info@raabsoftware.hu, website: https://raabsoftware.hu) acts as a data processor in the process. The data processor is responsible for the editing and structuring newsletters. When using the newsletter subscription feature, the 72-hour confirmation process (confirmation, failure, or rejection of the subscription) is handled within the **Microsoft Azure** system, meaning it is carried out using the cloud-based service provided by **MICROSOFT CORPORATION** (WA 98052, One Microsoft Way, Redmond, USA), and thus MICROSOFT CORPORATION acts as a data processor. Details of the Azure service are available here https://azure.microsoft.com.

	Additionally, **Twilio SendGrid Inc.** (registered office: 101 Spear Street, 1st Floor, San Francisco, CA 94105, USA; acts as a data processor. Court record: California, registration nr: 4518652, contact details: legalnotices@twilio.com), whose duty is – through its cloud-based service – to store subscriber information (name, email address, and newsletter type) and to send newsletters to the stored email addresses. In the course of performing its duties—strictly for the purposes specified—**Bonitás IT Limited Liability Company** may access personal data in its capacity as a data processor. (registered office 6725 Szeged, 18 Szabadkai Street, company registration number: Cg.06-09-012933., TAX id nr: 14445181-4-06, contact details: info@bonitasit.hu), which, in its capacity as a data controller, provides comprehensive application management, application development, infrastructure management, IT consulting and services, as well as IT security services.
Third-country data transfers:	Neither **MICROSOFT CORPORATION**, nor **Twilio SendGride Inc** as a data processors, are not a European Union-registered entities; thus, they qualify as a so-called third-country entities. However, since July 17, 2023, they have been a party to the data protection frameworks in effect between the EU and the US, the UK, and Switzerland and the US (Data Privacy Framework, https://www.dataprivacyframework.gov/s/participant-search/participant-detail?id=a2zt0000000KzNaAAK&status=Active). In light of this, data protection compliance has been achieved. Contact details of **MICROSOFT**'s data protection officer: https://www.dataprivacyframework.gov/s/participant-search/participant-detail?id=a2zt0000000KzNaAAK&status=Active **Twilio SendGrid Inc**.'s data protection and contact information are available here: https://www.twilio.com/en-us/gdpr; and https://www.twilio.com/en-us/legal/privacy.
Automated decision-making, profiling:	No automated decision-making or profiling takes place.
Is the provision of data mandatory:	It is not mandatory, but if the data subject does not provide their information, we will naturally be unable to send the General Newsletter.
What are the consequences if the data subject does not provide their personal data:	The data subject will not receive the General Newsletter.

4. SENDING EXCLUSIVE (SPECIAL) NEWSLETTERS AND CAREGIVER (PERSONALIZED) NEWSLETTERS

Introducing our exclusive (special) newsletter:

Exclusive newsletters are prepared for patients who have previously used the healthcare services provided by the data controller, subject to the patient's consent. Exclusive Newsletters differ from General Newsletters in that they provide specialized, professional information. The data controller provides its patients with ongoing professional information regarding screening tests and draws their attention to seasonal health services (e.g., flu shots, tick-borne encephalitis (TBE) vaccinations, etc.). The purpose of the information provided in the Exclusive Newsletters is to draw patients' attention to healthcare services that can help them maintain their health, prevent the onset of diseases, and detect existing conditions at an early stage. For this purpose, the data controller periodically sends informational, professional updates—specifically, an Exclusive Newsletter—to its patients to the email addresses they have provided.

The legal basis for sending the Exclusive Newsletters is the data subject's **consent**.

Introducing our Care provider (personalised) newsletter:

The data controller—with the explicit consent of the patient concerned—will send the patient a personalized **Caregiver Newsletter** specifically designed to improve their individual health situation; provided that, based on their medical history and demographic data, certain types of healthcare services are indicated for them; for the purposes of health maintenance, prevention, or follow-up care. To achieve this, the data controller also manages the health data of the data subject (i.e., special categories of personal data), including evaluating and analysing such data. Affected patients can only subscribe to the Caregiver Newsletter using the email address associated with their personal online account; they cannot provide any other email address for newsletter delivery.

The group of data subjects (i.e., patients affected by the specific topic of the Caregiver Newsletter who are recipients of the Caregiver Newsletter) is identified **through automated data processing**. The procedure is as follows: the data controller specifies the relevant parameters (e.g., age, gender, place of residence, diagnosis, number of previous treatments, etc.), initiates a corresponding electronic database query, and then compares the search results with the BHC file IDs (i.e., the patients' internal identification numbers) of those subscribed to the Caregiver Newsletter, and finally sends personalized content to those patients who have requested the Caregiver Newsletter.

The legal basis for sending the Caregiver Newsletter is the data subject's **consent**, supplemented by the data subject's **explicit consent** for the processing of health data, in accordance with Article 9(2)(a) of the GDPR.

Common rules for the Exclusive and Caregiver Newsletters:

The process for **subscribing** to and **unsubscribing** from both newsletter services is the same as described for the General Newsletter Service (see details provided in the previous chapter).

Please be advised that you may **withdraw your consent or explicit consent** to receive both the Exclusive Newsletter and the Caregiver Newsletter, **either separately or together, at any time.** If you withdraw your consent, **you will no longer receive the Exclusive Newsletter and/or the Caregiver Newsletter.**

Please also note that the BHC MyHealth mobile app—if downloaded by the patient—may send notifications regarding various informational materials, such as screening tests, as well as the data controller's seasonal health services (e.g., flu shots). Notifications can be disabled in the settings menu of smartphone applications. However, these notifications are not newsletters.

Data processing related to the Exclusive Newsletter and the Caregiver Newsletter mailing services is carried out as follows:

The aim of data management	Information about the data controller's current health services (e.g., screenings) and seasonal health services (e.g., vaccinations) (**Exclusive Newsletter**); and up-to-date information on personalized professional recommendations tailored specifically to the individual, based in part on the analysis and evaluation of their health data; for the purposes of health maintenance, prevention, or follow-up care (**Caregiver Newsletter).**
The legal basis for data management:	**Consent** of the data subject (i.e., given by the patient) pursuant to Article 6(1)(a) of the GDPR; in the case of the Caregiver Newsletters, this is supplemented by the data subject's **explicit consent** for the processing of health data, in accordance with Article 9(2)(a) of the GDPR. **Both consent and explicit consent may be withdrawn at any time without providing a reason.**
Description of the legitimate interest:	The data management is not based on a legitimate interest.
Categories of data subjects:	Patients who are natural persons and have subscribed to the Exclusive Newsletter and/or the Caregiver Newsletter.
Categories of personal data processed:	The data subject's name, email address for newsletter delivery (which, in the case of the Caregiver Newsletter, must be exclusively the email address associated with the online personal client account), and the type of newsletter requested; In the case of the Caregiver Newsletter, additionally the data subject's BHC file ID (i.e., the patient's internal identification number) and medical history data (type, date, and frequency of healthcare services received from the data controller, ICD code), as well as relevant demographic data (e.g., place of residence, gender, age). **Health data** are considered special categories of personal data under Article 9(1) of the GDPR, and their management requires the explicit consent of the data subject.
Source of personal data:	The data is provided by the data subject themselves.
The duration of data management:	We process the data until the **data subject withdraws their consent, or explicit consent** (or unsubscribes); or, in the case of a subscription request, until the **72-hour confirmation period** specified in the data controller's response email **expires without result** (after which a

	subscription request not confirmed by the data subject within 72 hours will be deleted).
Recipients (subjects of data transmission):	**MOANA SOFTWARE MAGYARORSZÁG LLC.** (registered office: 1025 Budapest, Zöldlomb Street 32-34/b, 4th floor 16., Cg.01-09-699603., contact details: info@moanasoftware.com, website: https://www.moanasoftware.com) as web hosting provider (and also as a data processor), it processes the data uploaded to the data controller's internal system (in this case, it forwards requests to subscribe to, unsubscribe from, or inquire about the newsletter, but does not store any related data itself). **Brainsum Kft.** (registered office 2836 Baj, 27 Bem József Street, Company registration number: Cg.11-09-024421., website: https://brainsum.com, contact details: info@brainsum.com), As a data processor and web hosting provider, it processes the data uploaded to the data controller's website (https://bhc.en) (for example, when users subscribe to the newsletter there); and this data processor carries out the developments requested by the data controller. A **RAAB SOFTWARE Kft.** (9024 Győr, 36 Szigethy Attila Street, 3rd Floor, Apartment 6, Cg.08-09-032732., contact details: info@raabsoftware.hu, website: https://raabsoftware.hu) acts as a data processor in the process. The data processor is responsible for the editing and structuring newsletters. When using the newsletter subscription feature, the 72-hour confirmation process (confirmation, failure, or rejection of the subscription) is handled within the **Microsoft Azure** system, meaning it is carried out using the cloud-based service provided by **MICROSOFT CORPORATION** (WA 98052, One Microsoft Way, Redmond, USA), and thus MICROSOFT CORPORATION acts as a data processor. Details of the Azure service are available here https://azure.microsoft.com. Additionally, **Twilio SendGrid Inc.** (registered office: 101 Spear Street, 1st Floor, San Francisco, CA 94105, USA; acts as a data processor. Court record: California, registration nr: 4518652 , contact details: legalnotices@twilio.com), whose task is—through its cloud-based service—to store subscription data (for the Exclusive Newsletter: name, email address, and newsletter type; and for the Caregiver Newsletter: name, email address, newsletter type, and BHC file ID); and to send the newsletter to the email addresses stored in its system.

	In the course of performing its duties—strictly for the purposes specified—**Bonitás IT Limited Liability Company** may access personal data in its capacity as a data processor. (registered office 6725 Szeged, 18 Szabadkai Street, company registration number: Cg.06-09-012933., TAX id nr: 14445181-4-06, contact details: info@bonitasit.hu), which, in its capacity as a data controller, provides comprehensive application management, application development, infrastructure management, IT consulting and services, as well as IT security services.
Third-country data transfers:	Neither **MICROSOFT CORPORATION**, nor **Twilio SendGride Inc** as a data processor, are not a European Union-registered entities; thus, they qualify as a so-called third-country entities. However, since July 17, 2023, they have been a party to the data protection frameworks in effect between the EU and the US, the UK, and Switzerland and the US (Data Privacy Framework, https://www.dataprivacyframework.gov/s/participant-search/participant-detail?id=a2zt0000000KzNaAAK&status=Active). In light of this, data protection compliance has been achieved. Contact details of **MICROSOFT**'s data protection officer: https://www.dataprivacyframework.gov/s/participant-search/participant-detail?id=a2zt0000000KzNaAAK&status=Active **Twilio SendGrid Inc**.'s data protection and contact information are available here: https://www.twilio.com/en-us/gdpr; and https://www.twilio.com/en-us/legal/privacy.
Automated decision-making/profiling:	When determining the recipients of the **Caregiver Newsletter**—that is, its target audience—the data controller uses **automated data processing**, the steps of which are described in detail in the text preceding the table. However, this does not constitute automated decision-making, as it does not have a significant impact on the data subject.
Is the provision of data mandatory:	No, but in this case, we will not be able to send you the Exclusive and/or Caregiver Newsletter.
What are the consequences if the data subject does not provide their personal data:	The data subject will not receive the Exclusive and or the Caregiver Newsletter.

5. CONTACTING CUSTOMER SERVICE

Contacting us by phone; or by email at usinginfo@bhc.hu (except: For the Private Inpatient Care Unit); as well as magankorhaz@bhc.hu as well as using the e-mail address in magankorhaz@bhc.hu for Private Inpatient Care/

If you wish, you can contact us via our website, by phone, or by email. If necessary, our customer service team may call or call you back; we will also respond to any written enquiries you may have.
In the case of a **phone call**, your conversation with customer service—or one facilitated by customer service—will be recorded on the grounds of a legitimate interest to ensure accountability, enable the handling of any complaints, and facilitate the enforcement of legal claims. For similar reasons and on the same legal basis, we record any phone calls made by our customer service team to contact you (e.g., callbacks). This is because the content of telephone calls predominantly involves the recording of highly sensitive personal data, such as appointment bookings, changes to or cancellations of appointments; information regarding requests for medical care; and personal data related to questions asked prior to treatment or the solution of post-treatment problems.
If you contact us **via email**, we will also process the personal data you provide in your email. Given that the person sending the email typically already has a relationship with the data controller (a legal relationship for the purpose of receiving healthcare services) or is sending the email with the intention of establishing such a relationship, we generally process personal data on the legal basis of the performance of a contract.

Please note that **"Telephone Consultation"** is regulated by a separate section in this Privacy Notice (Section 13 of the Privacy Notice) when the telephone conversation takes place with a medical specialist. This section describes only the data processing rules applicable to telephone contact with customer service.
We would also like to inform you that detailed information regarding the substantive procedures for handling complaints and the rules on data management is provided in a separate section—Section 15 of this Privacy Notice, titled "**Complaint Handling**." This chapter deals exclusively with the data processing rules relating to the recording of calls made for the purpose of filing a complaint.

Your personal data will be managed as follows:

The aim of data management	**Responding to inquiries and requests from data subjects; ensuring transparent operations. In addition, another purpose of recording telephone calls is to enable the handling of any complaints and the enforcement of legal claims.**
The legal basis for data management:	The legal basis for the processing of telephone communications—where the call involves a recorded conversation with customer service—is the **legitimate interest of the data controller, the healthcare provider, and the patient**, pursuant to Article 6(1)(f) of the GDPR. The legal basis for processing personal data collected through email contact is the **performance of a contract**, in accordance with Article 6(1)(b) of the GDPR. Regarding special categories of data (e.g., health data), data processing is permitted under Article

	9(2)(a) of the GDPR (**the data subject's explicit consent**) or Article 9(2)(h) (**the provision of health care or other medical services**).
Description of the legitimate interest:	The legal basis for **recording telephone conversations** with customer service is the legitimate interest of the data controller, the healthcare provider, and the patient. The legitimate interest is to ensure greater accountability in connection with the provision of healthcare; to establish and document the possibility of filing complaints or enforcement of legal claims. However, the patient can expect their data to be processed, as they are informed of this both at the start of the consultation and on the data controller's website. Recording of telephone conversations related to healthcare is a particularly important safeguard for which there is no less restrictive alternative. The data subject is also entitled to several rights. These rights are described in detail in this document. It is specifically emphasized that the patient in question may **object** to the recording of their personal data. Under your right of access, you may also request a **copy of the audio recording**, specifying the exact date, time, and phone number of the call. Finally, patients **may request information** regarding the processing of their personal data.
Categories of data subjects:	Individuals who call the data controller's customer service by phone or who are contacted by the data controller's customer service by phone; as well as those who send personal data to the email adressesinfo@bhc.hu ormagankorhaz@bhc.hu .
Categories of personal data processed:	In the case of **telephone contact**, the personal data processed include: the data subject's name, possibly their identification number and contact information, personal data provided by a person calling the data controller's customer service or by a person called back by customer service, as well as special categories of such data (health data); personal data disclosed by customer service, including special categories of personal data (health data).

	In the case of a recorded telephone conversation, the data controller also handles the call's unique identification number (which includes the date and time of the call and the data subject's telephone number), as well as the data subject's voice. **In the case of email**, the personal data processed includes the following: the sender of the email, the sender's email address, the date and time the email was sent, the subject line of the email, and the content of the email and any attachments.
Source of personal data:	The data is provided by the data subject themselves; in the case of a phone call, this is supplemented by personal data provided during the customer service response or callback, while in the case of an email, it is supplemented by personal data included in the written response.
The duration of data management:	In the case of voice recordings, the duration of data processing is **5 years from the date of the recording made on the landline.** An exception to this rule applies if enforcement of legal claims are taken during this period. In this case, data processing will continue throughout the period necessary for the enforcement of legal claims. All personal data related to medical records— including electronic correspondence containing such data— must be retained for at least 30 years pursuant to Section 30(1) of the Health Care Act (Eüak) (depending on the course of medical care). With regard to electronic inquiries in which the personal data contained therein do not constitute a patient's health data (where the statutory obligation to process such data does not apply), and where no coordination process aimed at providing health services takes place following the inquiry, the data controller will **retain the personal data** contained in the email **for 60 days**.
Recipients (subjects of data transmission):	Personal data may be disclosed to third parties for the purpose of providing healthcare services. Third parties are defined as professional staff **involved** in the provision of healthcare services who are not employed by the facility, as well as cooperating independent business entities (doctors, patient transport providers,

	laboratories, diagnostic companies, home visit service providers, etc.). Patients are also informed separately about the transfer of data. The **VCC Life Hungary Kft.** (registered office: 1117 Budapest, 8–10 Október huszonharmadika Street Allee Corner Office Building, Bercsényi Tower, 4th Floor; company registration number: Cg.01-09-735941., TAX id nr: 13452696-2-43, contact details:info@virtual-call-center.hu) As a data processor, it provides the technical infrastructure for storing audio recordings of recorded telephone conversations conducted with customer service, and, if necessary, provides the technical infrastructure for customer service to access the audio recordings; it then deletes the audio recordings after the data retention period has expired. E-prescriptions issued as part of healthcare services, as well as medical records, are transmitted to the Electronic Healthcare Services Platform (EESZT) operated by the Ministry of the Interior (1051 Budapest, József Attila u. 2-4, Health Line; Email: info@egeszsegvonal.gov.hu). 2-4. Healthline: 1812, E-mail: info@egeszsegvonal.gov.hu) the Electronic Healthcare Services Platform (**EESZT**) operated by the **Ministry of Interior** (1051 Budapest, 2-4 József Attila street). This is based on the fulfilment of a legal obligation (Section 2(1a) of EMMI Decree No. 39/2016 (XII.21)). https://e-egeszsegugy.gov.hu/hu/mi-az-eeszt- In the course of performing its duties—strictly for the purposes specified—**Bonitás IT Limited Liability Company** may access personal data in its capacity as a data processor. (registered office 6725 Szeged, 18 Szabadkai Street, company registration number: Cg.06-09-012933., TAX id nr: 14445181-4-06, contact details: info@bonitasit.hu), which, in its capacity as a data controller, provides comprehensive application management, application development, infrastructure management, IT consulting and services, as well as IT security services.
Third-country data transfers:	Data transfer does not take place.
Automated decision-making, profiling:	Automated decision-making, profiling does not take place.

Is the provision of data mandatory:	The data subject is not required to provide this information.
What are the consequences if the data subject does not provide their personal data:	In the absence of data provided by the data subject, achieving the purpose of contacting them may be hindered (e.g., it may not be possible to reach the data subject with the response; or it may not be possible to provide an accurate response due to a lack of data, etc.). Data reporting is the foundation of quality healthcare.

6. REQUEST FOR PROPOSALS FOR OUR HEALTHCARE SERVICES

Become a patient of our healthcare provider and request a personalized quote for our healthcare services. **Please include the most essential personal information only in your request for a quote.** If you choose to request a quote from us, we will process the personal data you provide as follows:

The aim of data management	**Submitting a bid for healthcare services in response to a request for proposals.**
The legal basis for data management:	If an individual requests the offer for their own use, the legal basis for data processing is the performance of a contract pursuant to Article 6(1)(b) of the GDPR. If the request is made by a legal entity or organization—for example, if an employer's contact person or legal representative requests it on behalf of their employees as part of an occupational health examination; then the legal basis for processing the data of the contact persons and legal representatives is legitimate interest pursuant to Article 6(1)(f) of the GDPR (which is the legitimate interest of both the data controller, BHC, and the employer). If you also provide us with special categories of personal data (e.g., health data), data processing is permitted under Article 9(2)(a) and (h) of the GDPR (**based on the data subject's explicit consent, or for the purpose of providing health services or medical care**).
Description of the legitimate interest:	Data processing is based on legitimate interests only in the case of the processing of data pertaining to contacts and legal representatives. In such cases, the contact person or legal representative of the legal entity/organization contacts the data controller with a request for a quote; therefore, the processing of the contact person's or legal

	representative's data is unavoidable for the purposes of communication and responding to the request and is also in the significant interest of both parties. In addition, the details of legal representatives are recorded in an official registry and are accessible and verifiable by anyone.
Categories of data subjects:	Natural persons requesting a quote; contact persons or legal representatives of legal entities requesting a quote (e.g., in the case of an intention to use occupational health services).
Categories of personal data processed:	The name and address of the natural person making the request; where applicable, the name of the legal representative or contact person and the name and registered office of the legal entity/organization on whose behalf they are acting; optional contact details (email address and/or phone number)a description of the healthcare service and the associated prices (unit price, quantity, net price / VAT / gross price, total amounts); any discounts offered and their legal basis; the date of the quotation request and the date of issuance and delivery of the quotation, the validity period of the quotation. If the quote is sent to the potential customer via email, the data controller will also process the contact email address of that person. (The quote is attached as a password-protected, encrypted PDF file.)
Source of personal data:	The data subject (or their legal representative or contact person) provides the data themselves.
The duration of data management:	The data controller typically **retains the personal data** provided in the request for proposal **for 60 days**. If services are provided, data processing will continue for the duration of the contractual relationship related to the service. **All personal data contained in medical records must be retained for at least 30 years in accordance with Section 30(1) of the Health Care Act (depending on the course of medical treatment).**
Recipients (subjects of data transmission):	The company operating the data controller's internal management system is **MOANA SOFTWARE MAGYARORSZÁG Kft.**, data is thereby transferred to that company, acting as a data processor 1025 Budapest, Zöldlomb Street 32-34/b, 4th floor 16 apt. contact details:

	info@moanasoftware.com, Cg.01-09-699603., TAX id nr: 12709407-2-41., e-mail: info@moanasoftware.com, website: https://www.moanasoftware.com). Personal data—if the request for proposal process results in an agreement for the provision of healthcare services—will be disclosed to the parties specified in Section 11 for the purpose of providing such healthcare services (see: Section 11, RECIPIENTS). While performing its duties—strictly for the purposes specified—**Bonitás IT Limited Liability Company** may access personal data in its capacity as a data processor. (registered office 6725 Szeged, 18 Szabadkai Street, company registration number: Cg.06-09-012933., TAX id nr: 14445181-4-06, contact details: info@bonitasit.hu), which, in its capacity as a data controller, provides comprehensive application management, application development, infrastructure management, IT consulting and services, as well as IT security services.
Third-country data transfers:	Data transfer does not take place.
Automated decision-making, profiling:	Automated decision-making, profiling does not take place.
Is the provision of data mandatory:	No, in this is the case, we are unable to provide a quote for medical services in response to your request.
What are the consequences if the data subject does not provide their personal data:	The data subject in question does not receive an offer, so the healthcare service cannot be provided.

7. REGISTRATION FOR THE CUSTOMER SERVICE FEATURE ON THE WEBSITE OR MOBILE APP, AND CREATION OF A PERSONAL CUSTOMER ACCOUNT

The online registration features available on the data controller's website (https://online.bhc.hu) allows users to access online customer service functions. With the same registration, users can also use the BHC MyHealth app. Registration is therefore valid for both platforms, that is, for both versions of the personal customer account. By registering, patients can manage their affairs online without having to come in person. Examples of such options include accessing medical findings online or through the mobile app, or scheduling appointments online or through the mobile app.

The registration process for a personal customer account:

During registration, you will provide us with your personal information, which we will process. We will send you a **confirmation email** and an **activation code** via SMS, which can be used to activate your personal online account. The registration becomes successful by this former activation procedure, and we will continue to process your registration data. If no confirmation is received, your registration data will be deleted after 24 hours. It is important to note that registration is performed by your consent, and you can delete your personal account at any time. If you use the data controller's healthcare services, please note that, contrary to what is described above, the data controller is legally obligated to continue processing your medical records even after your personal customer account has been deleted.

The details of data management are described below:

The aim of data management	**Creating a personal customer account for the purpose of dealing with administrative matters online or by using the mobile app.**
The legal basis for data management:	The data subject's **consent** pursuant to Article 6(1)(a) of the GDPR, which may be withdrawn at any time without giving a reason. In this case, your registration (i.e., your personal account) will be deleted. Regarding special categories of data (e.g., health data), data processing is permitted under Article 9(2)(a) and (h) of the GDPR (**based on the data subject's explicit consent, or for the purpose of providing health services or medical care).**
Description of the legitimate interest:	The data management is not based on a legitimate interest.
Categories of data subjects:	Patients registering to create a personal account.
Categories of personal data processed:	The registrant's username, password, email address, name, mother's maiden name, gender, address, date of birth, phone number, preferred method of communication with the data controller (submit documentation), and social security number.
Source of personal data:	The data is provided by the data subject themselves.
The duration of data management:	Registration is based on the patient's consent, which may be **withdrawn at any time without providing a reason.** In this case, your personal account will be deleted. However, please note that if you use our healthcare services, the data controller remains obligated to process your health data in accordance with Data Protection Act.
Recipients (subjects of data transmission):	When using the online customer service feature, users are authenticated via the Microsoft Azure Active Directory system, i.e., through a cloud-based service provided by **MICROSOFT AZURE MICROSOFT CORPORATION** (WA 98052, One Microsoft Way, Redmond, USA); thus, MICROSOFT acts as a data processor. Contact details of MICROSOFT's data protection officer: https://www.dataprivacyframework.gov/s/participant-search/participant-detail?id=a2zt0000000KzNaAAK&status=Active

	The data controller also transfers data to **MOANA SOFTWARE MAGYARORSZÁG Kft.**, to the data processor that operates the data controller's online internal management system, 1025 Budapest, Zöldlomb Street 32-34/b, 4th floor 16 apt. contact details: info@moanasoftware.com, Cg.01-09-699603., TAX id nr: 12709407-2-41., e-mail: info@moanasoftware.com, website: https://www.moanasoftware.com). To operate the mobile app, the data controller uses a data processor, which is the following company: **SMP Solutions Zrt.** (Registered office: 1138 Budapest, 47–49 Madarász Viktor Street, Building 2 3rd floor. company registration number: Cg. 01-10-140383, TAX id nr: 26777810-2-44., e-mail: smp@smp.hu, website: https://smpsolutions.hu) While performing its duties—strictly for the purposes specified—**Bonitás IT Limited Liability Company** may access personal data in its capacity as a data processor. (Registered office 6725 Szeged, 18 Szabadkai Street, company registration number: Cg.06-09-012933., TAX id nr: 14445181-4-06, contact details: info@bonitasit.hu), which, in its capacity as a data controller, provides comprehensive application management, application development, infrastructure management, IT consulting and services, as well as IT security services.
Third-country data transfers:	Data is transferred to a data processor, **MICROSOFT CORPORATION**, located in the United States, which is not a European Union-registered company; and is therefore considered a third-country entity; however, since July 17, 2023, it has been a participant of the data protection frameworks in effect between the EU and the US, the UK, and Switzerland and the US (Data Privacy Framework, https://www.dataprivacyframework.gov/s/participant-search/participant-detail?id=a2zt0000000KzNaAAK&status=Active). Considering this, data protection compliance has been achieved.
Automated decision-making, profiling:	Automated decision-making, profiling does not take place.
Is the provision of data mandatory:	No, but in this case, we cannot create a personal customer account.
What are the consequences if the data subject does not provide their personal data:	A significant portion of administrative tasks cannot be handled online or via the mobile app (see the description in the following section).

8. USE OF THE CUSTOMER SERVICE FUNCTION VIA THE ONLINE PLATFORM OR MOBILE APP, I.E., DATA PROCESSING RELATED TO PERSONAL CUSTOMER ACCOUNTS

Once our clients have successfully registered on our website at https://online.bhc.en, they can deal with administrative matters online without having to visit in person (patients are enabled to book or cancel appointments without making a phone call, to download their medical records and invoices, and to use our online or mobile app customer service). Our online customer service and the mobile application service—which allows you to use both the online customer service features and the mobile app—are available 24 hours a day, every day.

The details of data management related to the operation of the personal customer account are described below:

The aim of data management	**The purpose of the personal customer account is to enable users to manage their administrative matters via the online portal and mobile app; to book appointments for healthcare services, modify appointments, and view appointment history; and to access medical records and invoices issued in connection with healthcare services received from the data controller.**
The legal basis for data management:	In the personal customer account, the data controller processes personal data not covered by the categories listed in the following paragraphs (e.g., username, password, etc.) based on the **data subject's consent**, in accordance with Article 6(1)(a) of the GDPR; this continues until the data subject withdraws such consent and deletes their personal customer account. The data subject may do so at any time. If the data subject has received healthcare services from the data controller, the data controller is required to retain the medical records pursuant to Section 136 of Act CLIV of 1997 (Health Care Act). The documentation also includes the date and time of the examination registered online. The legal basis for the processing of this personal data complies with Article 6(1)(c) of the GDPR **complying with a legal obligation** (documentation of medical records). Similarly, the legal basis for processing invoices is the fulfilment of a legal obligation. Regarding invoices issued for the provision of healthcare services, the basis for the **documentation requirement** (invoicing) is Section 159 and 169 of Act CXXVII of 2007 on Value-Added Tax, and Sections 166–169 of Act C of 2000 on Accounting. Regarding special categories of data (e.g., health data), data processing is permitted under Article 9(h) of the GDPR (**data processing for the purpose of providing health care)**.
Description of the legitimate interest:	The data management is not based on a legitimate interest.
Categories of data subjects:	Natural persons who register for a personal customer account.
Categories of personal data processed:	**Registration data:** The registrant's username, password, email address, name, mother's maiden name, gender, address, date of birth, phone

	number, preferred method of communication with the data controller (submitting documentation), and social security number. **Other data:** invoices, medical history, medical records, appointments for healthcare services, and the cancellation or rescheduling of appointments.
Source of personal data:	The data subject provides some of the data themselves, while other data is provided (or determined) by healthcare professionals involved in the provision of care.
The duration of data management:	Data **constituting part of the health records** must generally be retained for **30 years** pursuant to Section 30(1) of the Health Care Act, (depending on the course of health care). The basis for the **documentation requirement** (invoicing) is Section 159 and Section 169 of Act CXXVII of 2007 on Value Added Tax, as well as Sections 166–169 of Act C of 2000 on Accounting; the data retention period is until the last day of the **8.th** year following the issuance of the invoice. The data controller will process **other data** until the data subject terminates their personal account.
Recipients (subjects of data transmission):	Personal data may be disclosed to third parties for the purpose of providing healthcare services. Third parties are defined as professional staff **involved** in the provision of healthcare services who are not employed by the facility, as well as cooperating independent business entities (doctors, patient transport providers, laboratories, diagnostic companies, home visit service providers, etc.). Patients are also informed separately about the transfer of data. E-prescriptions issued as part of healthcare services, as well as medical records, are transmitted to the Electronic Healthcare Services Platform (EESZT) operated by the Ministry of the Interior (1051 Budapest, József Attila u. 2-4, Health Line; Email: info@egeszsegvonal.gov.hu). medical records, Healthline: 1812, E-mail:info@egeszsegvonal.gov.hu) the Electronic Healthcare Services Platform (**EESZT**) operated by the **Ministry of Interior** (1051 Budapest, 2-4 József Attila street). This is based on the fulfilment of a legal obligation (Section 2(1a) No. 39/2016 (XII.21) EMMI DECREE. The data controller also transfers data to **MOANA SOFTWARE MAGYARORSZÁG Kft.**, to the data processor operating the online system 1025 Budapest, 32–34/b Zöldlomb Street 16 4th floor, info@moanasoftware..com,

	website: https://www.moanasoftware.com: company registration number Cg.01-09-699603). To operate the mobile app, the data controller also uses a data processor, which is the following company: **SMP Solutions Zrt.** (Registered office: 1138 Budapest, 47–49 Madarász Viktor Street, Building 2 3rd floor. company registration number: Cg. 01-10-140383, TAX id nr: 26777810-2-44., e-mail: smp@smp.hu, website: https://smpsolutions.hu). Online registration via personal customer accounts and the identification of users by the data controller take place within the Microsoft Azure Active Directory system, that is, through the cloud-based service provided by **MICROSOFT AZURE (MICROSOFT CORPORATION**, WA 98052, One Microsoft Way, Redmond, USA), meaning that MICROSOFT acts as a data processor. Contact details of MICROSOFT's data protection officer: https://www.dataprivacyframework.gov/s/participant-search/participant-detail?id=a2zt0000000KzNaAAK&status=Active While performing its duties—strictly for the purposes specified—**Bonitás IT Limited Liability Company** may access personal data in its capacity as a data processor. (registered office 6725 Szeged, 18 Szabadkai Street, company registration number: Cg.06-09-012933., TAX id nr: 14445181-4-06 , contact details: info@bonitasit.hu), which, in its capacity as a data controller, provides comprehensive application management, application development, infrastructure management, IT consulting and services, as well as IT security services.
Third-country data transfers:	Data is transferred to a data processor, **MICROSOFT CORPORATION**, located in the United States, which is not a European Union-registered company; and is therefore considered a third-country entity; however, since July 17, 2023, it has been a participant of the data protection frameworks in effect between the EU and the US, the UK, and Switzerland and the US (Data Privacy Framework, https://www.dataprivacyframework.gov/s/participant-search/participant-detail?id=a2zt0000000KzNaAAK&status=Active). Considering this, data protection compliance has been achieved.
Automated decision-making, profiling:	Automated decision-making, profiling does not take place.
Is the provision of data mandatory:	No, in this case, the data subject cannot manage their affairs through their personal account.

What are the consequences if the data subject does not provide their personal data:	A significant part of administrative tasks cannot be handled online or via a mobile app.

9. OPERATION AND REGISTRATION PROCESS OF THE CORPORATE DATA EXCHANGE PORTAL; AS WELL AS THE SUPPLEMENTARY DATA MANAGEMENT RULES FOR OCCUPATIONAL HEALTH EXAMINATIONS (INCLUDING: SCREENING TESTS)

The Data Controller enters into agreements with numerous companies (i.e., legal entities, hereinafter referred to as "companies") to provide healthcare services to their employees. To provide healthcare services, the company transfers various data to the data controller in advance so that the identification and medical examination of its employees—that is, the fulfilment of the ordered service package—can proceed smoothly. The data controller also provides the company with documents that, for example, the company must complete prior to the examination, or that record the data requested by the company following the examination.

The data controller established the corporate data exchange portal with the aim of ensuring that the data exchange takes place in the simplest possible manner while guaranteeing the highest level of data security. The portal is protected from an IT security perspective, so there is no need to encrypt data or documents before uploading them.

The corporate data exchange portal (or "corporate customer service portal") is available here: https://vallalatiportal.bhc.hu/

The Data Controller generates an online user account for its corporate partners who wish to use the corporate data exchange portal, based on the company's corporate data and the contact person(s) designated by the company or other (non-personally identifiable) email addresses provided by the company. The data controller will then send the corporate user account details to this email address, with the understanding that the company (or its designated contact person) must create the password associated with the username to finalize the setup of the corporate online user account.

After that, the company—through its designated contact person authorized to use the portal—can log in using the username and password to upload documents and data, as well as download documents uploaded by the data controller. **We emphasize that it is the company's responsibility to ensure that the password it assigns at its discretion is known only to those individuals within the company who have authorization to access the portal.** The data controller will have no influence or control over this matter. We recommend that if you suspect your password has fallen into unauthorised hands, it should be changed immediately; furthermore, it is advisable to change your password at regular intervals.

The portal displays the following information about the documents: the name of the uploaded document, the upload date, the document size, the client's name, the document type, the uploader's name (if the document is uploaded by a data controller, the specific person's name is displayed; if uploaded by a company, only the account username is shown), the name of the first person to download the document (if the data controller uploads the document, the specific person's name is displayed; in the case of a company, only the account username), date of first download, whether processing has taken place, comments.

Documents can be downloaded by clicking the "Download" button; they can be uploaded by clicking the "Upload New Document" button. All documents uploaded to the portal remain available for 30 days for delivery purposes; after that, they are permanently deleted from the platform.

During registration, the contact person provides their name and (if applicable) email address as personal data to the data controller; meanwhile, when using the corporate user account, the company transmits various personal data of its employees—including health-related data—to the company's data controller, which the data controller will subsequently process. It is important to note that registration and use of the portal are subject to the company's consent, so the company may delete its corporate user account at any time. The corporate user account will be deleted upon termination of the contractual relationship. However, if your company uses the data controller's healthcare services, please note that the data controller is legally obligated to continue processing your employees' medical records even after the company's user account has been deleted; these records will not be deleted. For information on the management of company employees' personal data while providing healthcare services—which is carried out in the same manner as the processing of all patients' personal data—please review Section 11 of the Privacy Notice.

The details of data management are described below:

The aim of data management	The creation and operation of a corporate user account for the purpose of secure data transfer and the delivery of medical records between the contracting parties (the company and the data controller). In the broader sense, the purpose of data processing is to ensure the rapid and seamless delivery of healthcare services.
The legal basis for data management:	The registration and operation of the corporate customer account are carried out with the consent of the company, which the company may revoke at any time. In this case, your personal account will be deleted. However, this data processing falls outside the scope of the GDPR. With regard to the personal data of the company contact person (name and, where applicable, email address) and the data controller's employees (their names) displayed on the portal, the legal basis for data processing is the legitimate interest of the data controller pursuant to Article 6(1)(f) of the GDPR (which is also consistent with the **legitimate interest** of the company). If an employee of the company receives healthcare services from the data controller, the data controller is required, pursuant to Section 136 of Act CLIV of 1997 (Health Care Act), to document the care provided and retain the medical records. The documentation may also include documents uploaded to the portal. The legal basis for the processing of this personal data complies with Article 6(1)(c) of the GDPR **complying with a legal obligation** (documentation of medical records).

	Regarding special categories of data (e.g., health data), data processing is permitted under Article 9(2)(a) of the GDPR (based on the data subject's explicit consent) or Article 9(2)(h) (**the provision of health care or other medical services**). Similarly, the legal basis for the management and retention of invoice data is following a legal obligation. Regarding invoices issued for the provision of healthcare services, the basis for the **documentation requirement** (invoicing) is Section 159 and 169 of Act CXXVII of 2007 on Value-Added Tax, and Sections 166–169 of Act C of 2000 on Accounting.
Description of the legitimate interest:	In connection with the use of the portal, the legitimate interest regarding the personal data of the contact persons (name and, where applicable, email address) and the employees of the data controller (name) are linked to the legitimate interest in the obligation to cooperate with the contracting partner and the fulfilment of contractual rights and obligations; however, the employees of the parties may have a right to self-determination regarding the protection of their names and workplace contact information, however, providing this information—to their employer—is also a legal obligation arising from their employment contract; contractual performance and smooth communication are in the fundamental labour law interests of these contacts and employees, so no actual infringement of rights affects these data subjects. The data controller processes the personal data of these data subjects solely in relation to the legal entity they represent and not in their capacity as natural persons.
Categories of data subjects:	Company contacts authorized to create and manage corporate user accounts, employees involved in the data controller's data upload process (whose names appear on the portal interface); and employees receiving healthcare services from the company, in their capacity as patients.
Categories of personal data processed:	Regarding the contact person who activates and manages the corporate user account: name, corporate username, password, email address, and company name. Regarding data controller employees who upload documents and data to the data exchange portal: name. All personal data of company employees affected by the documentation uploaded to the portal that appears in such documentation. Typical documents and the personal data they contain: "List of eligible individuals": full name, birth name, gender, personal identification number, mother's name, exact address, Social Security number, occupational health classification code (A, B, C, or

	D), job title, company-specific data, Hungarian Standard Classification of Occupation (FEOR nr), date of birth, date of occupational health examination, fitness for duty, examination validity, fitness to work from ophthalmology standpoint testing visual acuity, visual examination validity, email address, phone number, health insurance fund code, tax identification number. "Referral Form" (for an occupational health examination): employee's name, date of birth, address, job title, Social Security number, reason for the examination, the main health risks associated with the job, and the duration of such risks during working hours. "Occupational Health Statistics Form": company name; names of employees subject to the examination; for each employee: date of birth, social security number, job title, occupational health category, date of occupational health examination, description of the occupational health examination, occupational health fitness status, validity of occupational health fitness examination, date of ophthalmic examination, eye fitness status, validity of eye fitness, validity of fitness for work justified by chest X-ray, contract description, company email address, employee ID nr**,** any company-specific data. "Screening TESTS Statistics Sheet": the date of the screening test, the names of the employees affected, and the following details: type of screening, type of contract. Fitness for work assessments: Date of examination, name, date of birth, job title, employer, opinion (simply stating whether the individual is suitable for the position, possibly with restrictions, or whether they are unsuitable). Other information that can be uploaded to the portal includes appointments for healthcare services, cancellations of appointments, and changes to appointments, etc. Regarding healthcare services, Section 11 of this Privacy Notice provides detailed guidance on other personal data recorded about the employee as a patient—which the data controller processes uniformly for all patients in accordance with legal requirements.
Source of personal data:	Some of the data processed is provided by the company, as the employer, through its contact person. The employee appearing for the examination, as the data subject, provides the personal data documented there in part on his or her own when appearing for the examination; other data is determined by the professional staff of the data controller involved in the provision of healthcare services.
The duration of data management:	Documents uploaded to the corporate data exchange portal and the personal data they contain remain **accessible for 30**

	days from the date of upload (provided the user account is active); after that, they are automatically deleted (since the purpose of the portal is not data storage, but rather data exchange and data transmission). Please note, however, that when you use our healthcare services, the data controller remains obligated under the law to process your health and related data; therefore, deleting your user account does not automatically result in the deletion of documents uploaded or downloaded to it from the data controller's administrative system. Data **constituting part of the health records** pursuant to Section 30(1) of the Health Care Act, must generally be retained for **30 years** (depending on the course of health care). The basis for the **documentation requirement** (invoicing) is Section 159 and Section 169 of Act CXXVII of 2007 on Value Added Tax, as well as Sections 166–169 of Act C of 2000 on Accounting; the data retention period is until the last day of the **8.th** year following the issuance of the invoice.
Recipients (subjects of data transmission):	Corporate user account registration and customer identification take place within the Microsoft Azure Active Directory system, that is, through the cloud-based service provided by **MICROSOFT AZURE (MICROSOFT CORPORATION**, WA 98052, One Microsoft Way, Redmond, USA), thus MICROSOFT acts as a data processor. Contact details of MICROSOFT's data protection officer: https://www.dataprivacyframework.gov/s/participant-search/participant-detail?id=a2zt0000000KzNaAAK&status=Active The data controller also transfers data to **MOANA SOFTWARE MAGYARORSZÁG Kft.**, to the data processor that operates the data controller's online internal management system, (1025 Budapest, Zöldlomb Street 32-34/b, 4th floor 16 apt. contact details: info@moanasoftware.com, Cg.01-09-699603., TAX id nr: 12709407-2-41., e-mail: info@moanasoftware.com, website: https://www.moanasoftware.com). Personal data may be disclosed to third parties for the purpose of providing healthcare services. Third parties are defined as professional staff **involved** in the provision of healthcare services who are not employed by the facility, as well as cooperating independent business entities (doctors,

	patient transport providers, laboratories, diagnostic companies, home visit service providers, etc.). Patients are also informed separately about the transfer of data. E-prescriptions issued as part of healthcare services, as well as medical records, are transmitted to the Electronic Healthcare Services Platform (EESZT) operated by the Ministry of the Interior (1051 Budapest, József Attila u. 2-4, Health Line; Email: info@egeszsegvonal.gov.hu). medical records, Healthline: 1812, E-mail: info@egeszsegvonal.gov.hu) the Electronic Healthcare Services Platform (**EESZT**) operated by the **Ministry of Interior** (1051 Budapest, 2-4 József Attila street). This is based on the fulfilment of a legal obligation (Section 2(1a) of 39/2016 (XII.21 EMMI Decree). For the purposes of electronic invoicing, invoice data—in connection with the "szamlazz.hu" invoicing software—will be transmitted to the following subcontractor: **KBOSS.hu Kereskedelmi és Szolgáltató Korlátolt Felelősségű Társaság** (registered office: 1031 Budapest 7. Záhony str company registration number: Cg.01-09-303201., TAX id nr: 13421739-2-41., e-mail: info@szamlazz.hu, website: https://www.szamlazz.hu/szamla/main). While performing its duties—strictly for the purposes specified—**Bonitás IT Limited Liability Company** may access personal data in its capacity as a data processor. (registered office 6725 Szeged, 18 Szabadkai Street, company registration number: Cg.06-09-012933., TAX id nr: 14445181-4-06, contact details: info@bonitasit.hu), which, in its capacity as a data controller, provides comprehensive application management, application development, infrastructure management, IT consulting and services, as well as IT security services.
Third-country data transfers:	Data is transferred to a data processor, **MICROSOFT CORPORATION**, located in the United States, which is not a European Union-registered company; and is therefore considered a third-country entity; however, since July 17, 2023, it has been a participant of the data protection frameworks in effect between the EU and the US, the UK, and Switzerland and the US (Data Privacy Framework, https://www.dataprivacyframework.gov/s/participant-search/participant-detail?id=a2zt0000000KzNaAAK&status=Active). Considering this, data protection compliance has been achieved.
Automated decision-making, profiling:	Automated decision-making, profiling does not take place.
Is the provision of data mandatory:	No, in this case we are unable to create and maintain a corporate user account; furthermore, a refusal to provide

	data, or the provision of inaccurate or delayed data, may also hinder the delivery of healthcare services.
What are the consequences if the data subject does not provide their personal data:	This makes it impossible to conduct secure and simple data exchange and administrative procedures on the portal, and, in a broader sense, even to provide healthcare services.

10. ONLINE APPOINTMENT BOOKING VIA THE HTTPS://FOGLALJORVOST.HUWEBSITE

Buda Health Center LLC. has contracted Foglaljorvost Online Kft. as a service provider to provide a new appointment scheduling system. In accordance with the agreement Foglaljorvost Online Kft., as the website operator, displays on the **https://www.foglaljorvost.hu website**, the personal data of those physicians (name, photo, educational background, and professional profile) with whom website visitors can schedule appointments. In addition, the website operator allows patients who have used the healthcare services to post reviews, opinions (including criticism) about the doctor on the website.

If you have requested, modified, or cancelled an appointment at the data controller's (Buda Health Center) facility via the online appointment booking system available on the **https://www.foglaljorvost.hu** website, we will process your personal data—which was processed and transmitted to us by Foglaljorvost Online Kft., as an independent data controller—and transmitted to us, for an independent data controller—will be processed in accordance with the following rules:

The aim of data management	**The provision of healthcare; the coordination of interactions between doctors/healthcare professionals and patients (care coordination); the implementation of treatment and preventive and curative healthcare activities.**
The legal basis for data management:	**Until** the meeting between the **doctor (healthcare professional) and the data subject takes place at our clinic** at the relevant time, the legal basis for our data processing is "performance of a contract for the provision of healthcare services," as specified in Article 6(1)(b) of the GDPR. The legal basis for subsequent data management: However, after the medical service (doctor-patient consultation) has taken place, the healthcare provider (including our facility) is required to retain the medical records in accordance with Section 136 of the Health Care Act. The date of the examination is also part of the documentation. The legal basis for data processing in this regard is therefore **compliance with a legal obligation** under Article 6(1)(c) of the GDPR (medical records). The legal basis for the processing of invoices is similarly the **fulfilment of a legal obligation**; the statutory basis for this is Sections 159 and 169 of Act CXXVII of 2007 on Value Added Tax, as well as Sections 166–169 of Act C of 2000 on Accounting.

	Regarding **special categories of data** (e.g., health data), data processing is permitted under Article 9(h) of the GDPR (data processing for the purpose of providing health care).
Description of the legitimate interest:	The data management is not based on a legitimate interest.
Categories of data subjects:	Natural persons who book appointments at the data controller's facility via the online appointment scheduling system on the https://foglaljorvost.hu website.
Categories of personal data processed:	**Personal data provided to Foglaljorvost Online Kft. during the appointment booking process and forwarded by them to our institution (i.e., the data controller, Budai Health Center):** Name of the data subject; if the data subject is a legal representative, the fact that he/she is acting as such; in the case of a registered representative, the name of the patient being represented; Social Security number, phone number, and/or email address (contact information), the name and address of the healthcare facility to be visited, the name of the chosen doctor/healthcare professional, the exact date booked online (year, month, day), the booked hour and minute; information regarding any cancellation of the appointment; details of any appointment changes (same data fields as those for the original appointment booking).
Source of personal data:	The data subject provides the personal data directly to https://foglaljorvost Foglaljorvost Online Kft., which acts as the data controller and forwards—exclusively the above-mentioned data—to our facility (as an independent data controller).
The duration of data management:	Until the appointment between the doctor (healthcare professional) and the patient takes place, **the patient may cancel the appointment**, which also means that our clinic will terminate the data management, i.e., the data controller will delete the data received from Foglaljorvost Online Kft., as well as the booked appointment, upon the patient's request. The data controller follows a similar procedure when a **date of appointment is changed:** it deletes the record of the previous appointment along with the booked service, while continuing to process the new appointment and any related data. Following a consultation between the doctor (healthcare professional) and the patient, the duration of data management is as follows: Data **constituting part of health records** which includes the date of the healthcare service must generally be retained for **30 years** pursuant to Section 30(1) of the Health Care Act, (depending on the course of health care). The basis for the **documentation requirement** (invoicing) is Section 159 and Section 169 of Act CXXVII of 2007 on Value Added Tax, as well as Sections 166–169 of Act C of 2000 on

	Accounting; the data retention period is until the last day of the **8.th** year following the issuance of the invoice.
Recipients (subjects of data transmission):	The data processing procedures related to the online appointment booking process on the https://foglaljorvost.hu website are described by **Foglaljorvost Online Kft**., as an **independent data controller**, in its own privacy policy, which is available here: https://foglaljorvost.hu/adatkezelesi-tajekoztato. As an independent data controller, our facility receives the personal data listed above from Foglaljorvost Online Kft. via data transfer. Personal data may be disclosed to third parties for the purpose of providing healthcare services. Third parties are defined as professional staff **involved** in the provision of healthcare services who are not employed by the facility, as well as cooperating independent business entities (doctors, patient transport providers, laboratories, diagnostic companies, home visit service providers, etc.). Patients are also informed separately about the transfer of data. E-prescriptions issued as part of healthcare services, as well as medical records, are transmitted to the Electronic Healthcare Services Platform (EESZT) operated by the Ministry of the Interior (1051 Budapest, József Attila u. 2-4, Health Line; Email: info@egeszsegvonal.gov.hu). medical records, Healthline: 1812, E-mail: info@egeszsegvonal.gov.hu) the Electronic Healthcare Services Platform (**EESZT**) operated by the **Ministry of Interior** (1051 Budapest, 2-4 József Attila street). This is based on the fulfilment of a legal obligation (Section 2(1a) of EMMI Decree No. 39/2016 (XII.21)). To store data, the data controller uses the cloud-based service provided by MICROSOFT AZURE (MICROSOFT CORPORATION), and thus **MICROSOFT CORPORATION** (One Microsoft Way, Redmond, WA 98052, USA) acts as a data processor. Contact details of MICROSOFT's data protection officer: https://www.dataprivacyframework.gov/s/participant-search/participant-detail?id=a2zt0000000KzNaAAK&status=Active. While performing its duties—strictly for the purposes specified—**Bonitás IT Limited Liability Company** may access personal data in its capacity as a data processor. (registered office 6725 Szeged, 18 Szabadkai Street, company registration number: Cg.06-09-012933., TAX id nr: 14445181-4-06 , contact details: info@bonitasit.hu), which, in its capacity as a data controller, provides comprehensive application management, application development, infrastructure

	management, IT consulting and services, as well as IT security services.
Third-country data transfers:	Data is transferred to a data processor, **MICROSOFT CORPORATION**, located in the United States, which is not a European Union-registered company; and is therefore considered a third-country entity; however, since July 17, 2023, it has been a participant of the data protection frameworks in effect between the EU and the US, the UK, and Switzerland and the US (Data Privacy Framework, https://www.dataprivacyframework.gov/s/participant-search/participant-detail?id=a2zt0000000KzNaAAK&status=Active). Considering this, data protection compliance has been achieved.
Automated decision-making/profiling:	Automated decision-making, profiling does not take place.
Is the provision of data mandatory:	No, in this case, the data subject cannot use the services of our clinic—that is, the data controller—by booking an appointment online at https://foglaljorvost.hu
What are the consequences if the data subject does not provide their personal data:	Online appointment bookings not enabled onhttps://foglaljorvost.hu website.

Budai Health Center LTD., as the data controller, uses only the online appointment scheduling service among the services provided by Foglaljorvost Online Kft. Please note that Foglaljorvost Online Kft. provides its services as an independent data controller; information regarding its data processing activities can be requested from the company.

11. PATIENT REGISTRATION (DATA VERIFICATION), MEDICAL RECORDS, AND INVOICING

The data controller processes patients' personal data in connection with the provision of its healthcare services. During patient registration, the source of the personal data is the patient themself, who provides the personal data as part of the data verification process. In the case of occupational health examinations, the personal data generated during the ordering process (or part thereof) is provided by the employer. The data controller is also required to process personal data generated in connection with the healthcare services provided.

During both patient admission and the subsequent provision of healthcare services, we process data that is required by applicable legislation as part of healthcare records. Section 136 of Act CLIV of 1997 on Health Care (**Eütv**) (hereinafter "the Health Care Act") prescribes the following categories of data:

The following must be included in the medical documentation:
(a) the patient's personally identifiable information as defined in the act on the processing and protection of health and related personal data,
b) in the case of a patient with legal capacity, the name, address, and contact information of the person to be notified, as well as—if the patient so requests—the name, address, and contact information of the support person as defined by the act on supported decision-making; and in the case of a minor or a patient under

guardianship that partially or completely restricts legal capacity, the name, address, and contact information,
c) the patient's medical history,
(d) the results of the first examination,
e) the test results on which the diagnosis and treatment plan are based, the dates on which the tests were performed,
f) the name of the illness justifying the care, the underlying condition, any concomitant illnesses, and complications,
(g) other illnesses not directly justifying the provision of care, or a description of the risk factors,
(h) the date of the interventions performed and their results,
(i) medication and other therapies, and their results,
(j) information regarding the patient's hypersensitivity to medications,
(k) the name of the healthcare professional making the record and the date of the record,
(l) the recording of the content of information provided to the patient or to another person entitled to receive such information,
(m) the fact of consent [Section 15(3)] or refusal (Sections 20–23), as well as the date thereof,
(n) any other information or facts that may affect the patient's recovery.

The legal basis for processing these data is to comply with a legal obligation. The law also specifies the duration of data management. This legislation is the Act XLVII of 1997 on the Processing and Protection of Health and Related Personal Data (hereinafter referred to as the "**Eüak, Health Data Act**").

PREVIEW, PROVIDING INFORMATION

The patient is entitled to inspect their medical records in person and request a free copy of them.

During treatment, the patient may **authorize another person** in writing to access their health records or request copies thereof; after treatment, such authorization may be granted in a private document having full probative force.

The patient's **spouse, partner**, **sibling**, or **direct relative** may be authorized in writing to access the patient's medical records or request copies thereof.

Clients' health data is considered sensitive information, so special care must be taken when handling it. Considering this, we are unable to provide information over the phone.

INVOICING

The Data Controller issues electronic invoices for services requiring payment provided to patients, which are sent to the patient's contact email address and uploaded to the patient's personal account, provided the patient has registered for this service.

The aim of data management	**The provision of healthcare services, the documentation and verification of medical, therapeutic, and preventive activities, as well as the fees paid by the patient.**
The legal basis for data management:	Pursuant to Section 136 of the Health Care Act, a health care provider (and thus a data controller) is required to issue and retain medical **documentation**. The legal basis for data processing in this regard is therefore **compliance with a legal obligation** under Article 6(1)(c) of the GDPR.

	The legal basis for issuing and storing invoices, as well as for the related data reporting, is likewise the **fulfilment of a legal obligation;** the legal basis for which is Sections 159 and 169 of Act CXXVII of 2007 on Value Added Tax, as well as Sections 166–169 of Act C of 2000 on Accounting. Regarding **special categories of data** (e.g., health data), data processing is permitted under Article 9(h) of the GDPR (data processing for the purpose of providing healthcare).
Description of the legitimate interest:	The processing of data is not based on legitimate interests.
Categories of data subjects:	Individuals receiving healthcare services from the data controller.
Categories of personal data processed:	The patient's name, mother's maiden name, address, social security number, place and date of birth, contact information (email address and/or phone number); passport number or other form of identification for foreign nationals; the name, address, and contact information of the authorized representative; the name, address, and contact information of the supporting person or the legal representative of a minor, personal data recorded in the health records; the name of the document issued (invoice, advance invoice, cancellation invoice, correction invoice), the fee for the service provided, and the invoice details related to payment; the details of the individual listed as the "customer" on the invoice, if that person is not the same as the data subject.
Source of personal data:	During data collection, the data subject provides personal data; during the provision of care, the data controller, as a healthcare provider, provides personal data. In the case of occupational health services, the employer itself provides personal data regarding its employees for the purpose of patient registration.
The duration of data management:	Data **constituting part of the health records** must generally be retained for **30 years** pursuant to Section 30(1) of the Health Care Act, (depending on the course of health care). The basis for the **documentation requirement** (invoicing) is Section 159 and Section 169 of Act CXXVII of 2007 on Value Added Tax, as well as Sections 166–169 of Act C of 2000 on Accounting; the data retention period is until the last day of the **8.th** year following the issuance of the invoice.
Recipients (subjects of data transmission):	Personal data may be disclosed to third parties for the purpose of providing healthcare services. Third parties are defined as professional staff **involved** in the provision of healthcare services who are not employed by the facility, as well as cooperating independent business entities (doctors, patient transport providers, laboratories, diagnostic companies, home visit service providers, etc.).

	Patients are also informed separately about the transfer of data. We will inform the **employer** on the results (and only the results) of the occupational health examination. E-prescriptions issued as part of healthcare services, as well as medical records, are transmitted to the Electronic Healthcare Services Platform (EESZT) operated by the Ministry of the Interior (1051 Budapest, József Attila u. 2-4, Health Line; Email: info@egeszsegvonal.gov.hu). medical records, Healthline: 1812, E-mail:info@egeszsegvonal.gov.hu) the Electronic Healthcare Services Platform (**EESZT**) operated by the **Ministry of Interior** (1051 Budapest, 2-4 József Attila street). This is based on the fulfilment of a legal obligation (Section 2(1a) of EMMI Decree No. 39/2016 (XII.21)). To store data, the data controller uses the cloud-based service provided by MICROSOFT AZURE (MICROSOFT CORPORATION), and thus **MICROSOFT CORPORATION** (One Microsoft Way, Redmond, WA 98052, USA) acts as a data processor. Contact information for MICROSOFT'S data protection officer: https://www.dataprivacyframework.gov/s/participant-search/participant-detail?id=a2zt0000000KzNaAAK&status=Active For the purposes of electronic invoicing, invoice data—in connection with the "szamlazz.hu" invoicing software—will be transmitted to the following subcontractor: **KBOSS.hu Kereskedelmi és Szolgáltató Korlátolt Felelősségű Társaság** (registered office: 1031 Budapest 7 Záhony street, company registration number: Cg.01-09-303201., TAX id nr: 13421739-2-41., contact details: info@szamlazz.hu, website: https://www.szamlazz.hu). The company operating the data controller's internal management system is **MOANA SOFTWARE MAGYARORSZÁG Kft.**, data is thereby transferred to that company, acting as a data processor (1025 Budapest, Zöldlomb Street 32-34/b, 4th floor 16 apt. contact details: info@moanasoftware.com, Cg.01-09-699603., TAX id nr: 12709407-2-41., e-mail: info@moanasoftware.com, website: https://www.moanasoftware.com). While performing its duties—strictly for the purposes specified—**Bonitás IT Limited Liability Company** may access personal data in its capacity as a data processor. (registered office 6725 Szeged, 18 Szabadkai Street, company registration number: Cg.06-09-012933., TAX id nr: 14445181-4-06 , contact details: info@bonitasit.hu), which, in its capacity as a data controller, provides comprehensive application management, application development, infrastructure

	management, IT consulting and services, as well as IT security services.
Third-country data transfers:	Data is transferred to a data processor, **MICROSOFT CORPORATION**, located in the United States, which is not a European Union-registered company; and is therefore considered a third-country entity; however, since July 17, 2023, it has been a participant of the data protection frameworks in effect between the EU and the US, the UK, and Switzerland and the US (Data Privacy Framework, https://www.dataprivacyframework.gov/s/participant-search/participant-detail?id=a2zt0000000KzNaAAK&status=Active). Considering this, data protection compliance has been achieved.
Automated decision-making/profiling:	Automated decision-making, profiling does not take place.
Is the provision of data mandatory:	Under the law, the provision of personal data is voluntary; however, without such data, healthcare services cannot be accessed, unless the law provides for an exception (e.g., the need for emergency treatment).
What are the consequences if the data subject does not provide their personal data:	According to the law, the collection of medical records is a mandatory part of medical treatment. Without the relevant data reported by the data subject, medical services cannot be provided; unless the law specifies an exception (e.g., the need for urgent medical intervention).

12. HANDLING OF MEDICAL REPORTS SENT TO THE DATA CONTROLLER VIA E-MAIL OR UPLOADED TO PERSONAL ONLINE CUSTOMER ACCOUNTS

The data controller lays high priority on the careful handling of health data. Please submit your medical records and examination results (hereinafter referred to as "medical records") to us exclusively through the methods specified here. Medical records are accepted as follows:

1.) By uploading data to your personal online account:
You have the option to upload your medical records to your patient account so that your attending physician can access them directly online. This is particularly advisable in cases where the necessary documentation is not available in the EESZT registry. **We primarily recommend this method of data reporting to our clients.**

2.) By sending the medical records to the orvosilelet@bhc.hu e-mail address:
You also have the option of sending your medical records to the email address orvosilelet@bhc.hu instead of uploading them to your personal online account. In this case, the data controller will upload your medical records to your personal online account, allowing your attending physician to access them directly. If necessary, this information will also be forwarded to the attending physician via email. At the same time, we strive to ensure that personal data is managed through the online customer account and that it is not unnecessarily transmitted via email.

We will process the documentation you have submitted with your consent. You may withdraw your consent at any time without giving a reason. **However, if you use our healthcare services in connection with the documentation you have submitted, we are legally obligated to continue processing the medical**

documentation related to the services provided. In this case, therefore, we are unable to delete such personal data.

We would like to remind our clients that any medical records sent to the email addresses info@bhc.hu or magankorház@bhc.hu will be deleted in all cases. For the sake of protecting personal data, the data controller, Buda Health Center accepts these data exclusively in the ways described above.

Your personal data registered in the medical records will be processed as follows:

The aim of data management	**Managing patients medical records in a single location (personal online account) was designed to improve accessibility, ensure quick and secure access exclusively for authorized users, and to support healthcare services. The data controller processes the documentation uploaded or received via email for the purpose of providing future healthcare services and accessing the patient's past medical history.**
The legal basis for data management:	The legal basis for data processing **prior to the provision of healthcare services** is the **consent** provided by the patient pursuant to Article 6(1)(a) of the GDPR. **After this date**, data management will be based on the **legal obligation** specified in Article 6(1)(c) of the GDPR. The legal basis for this obligation is established by Section 136 of the Health Care Act, which stipulates that the data controller is required to retain medical records (including test results). Regarding special categories of data (e.g., health data), data management is allowed under Article 9(2)(a) of the GDPR (**the data subject's explicit consent**) and Article 9(2)(h) (**the provision of medical care or health services**).
Description of the legitimate interest:	The data management is not based on a legitimate interest.
Categories of data subjects:	Natural persons who send their medical records to the email address orvosilelet@bhc.hu or who upload these documents to their personal online customer account.
Categories of personal data processed:	Personal data contained in the document, or—in the case of data transmission via email—the sender's name, email address, the date and subject of the email, as well as the email's content and attachments.
Source of personal data:	The data is provided by the data subject themselves.

The duration of data management:	**Up until the point of receiving healthcare services**, the data subject may withdraw their consent to the processing of their data at any time. In this case, the personal data (uploaded medical records) will be deleted. **If you have received medical services:** Data constituting part of the healthcare records—including previous medical records uploaded by the patient— must generally be retained for **30 years** pursuant to Section 30(1) of the Health Care Act, (depending on the course of health care).
Recipients (subjects of data transmission):	Personal data may be disclosed to third parties for the purpose of providing healthcare services. Third parties are defined as professional staff **involved** in the provision of healthcare services who are not employed by the facility, as well as cooperating independent business entities (doctors, patient transport providers, laboratories, diagnostic companies, home visit service providers, etc.). Patients are also informed separately about the transfer of data. Medical documents/ are forwarded to Healthline: 1812, E-mail: info@egeszsegvonal.gov.hu) the Electronic Healthcare Services Platform (**EESZT**) operated by the **Ministry of Interior** (1051 Budapest, 2-4 József Attila street). This is based on the fulfilment of a legal obligation (Section 2(1a) of EMMI Decree No. 39/2016 (XII.21)). https://e-egeszsegugy.gov.hu/hu/mi-az-eeszt-. While performing its duties—strictly for the purposes specified—**Bonitás IT Limited Liability Company** may access personal data in its capacity as a data processor. (registered office 6725 Szeged, 18 Szabadkai Street, company registration number: Cg.06-09-012933., TAX id nr: 14445181-4-06, contact details:info@bonitasit.hu), which, in its capacity as a data controller, provides comprehensive application management, application development, infrastructure management, IT consulting and services, as well as IT security services.
Third-country data transfers:	Data transfer does not take place.
Automated decision-making, profiling:	Automated decision-making, profiling does not take place.

Is the provision of data mandatory:	The patient initiates contact; in his or her own interest and to ensure the success of the medical care, he or she provides his or her medical history in this manner.
What are the consequences if the data subject does not provide their personal data:	If the documentation has not been sent to the healthcare provider—and is not available in the EESZT—the patient must present it in physical form during the appointment or personal consultation.

13. TELEPHONE CONSULTATION:

The data controller's clients (patients) may call the phone number listed in the discharge summary in case of an emergency (e.g., patients who have undergone surgery may call this number if they encounter a problem and expect an immediate response); or operates a non-emergency telephone health advice service (in this case, patients request a future appointment at which they can consult with a healthcare professional). As part of the telephone consultation service, patients can consult with a specialist over the phone, receive medical advice, and, as part of this service, have e-prescriptions issued. A brief written summary of the phone consultation will be prepared; this will form part of the patient's medical records and will also be available in the patient's personal account, provided the patient has created an account after registering.
During non-emergency telephone consultation services, the call is not handled through customer service and is not recorded.
In the case of an urgent telephone consultation request, the patient calls the customer service number provided on the discharge summary, and customer service then connects the patient to the attending physician; the telephone conversation is recorded as specified in section 5. An exception to this rule applies when the attending physician or the on-call physician is unavailable (unable to answer the call), in which case the patient will be placed on a priority list and the physician will call them back later. Since the callback process is no longer handled through customer service, this conversation will not be recorded.

Data processing related to the provision of the service is carried out as follows:

The aim of data management	**Provision of emergency and non-emergency medical advice, as well as specialist consultations, without the need for an in-person visit; The purpose of the written summary is to fulfil the legal requirement to maintain health records, ensure the provider's accountability, and enable the handling of any complaints and the enforcement of legal claims (which is also the reason for recording telephone conversations conducted through customer service).**
The legal basis for data management:	**Performance of a contract for the provision of healthcare services** pursuant to Article 6(1)(b) of the GDPR. In the case of emergency medical advice, the legal basis is also the **vital interest of the data subject** under Article 6(1)(d) of the GDPR, which is the provision of appropriate medical advice and care.

	Data processing related to the health advisory service is necessary and permissible for the purposes of preventive healthcare and the provision of healthcare services (GDPR Article 9(2)(h)). Regarding medical records, **compliance with the legal obligation** specified in Article 6(1)(c) of the GDPR. The legal basis for this obligation is established by Section 136 of the Health Care Act, which stipulates that the data controller is required to prepare and retain medical records. Regarding the recording of telephone calls made through customer service, the legal basis for data processing is the legitimate interest of the data controller (the healthcare provider) and the patient, pursuant to Article 6(1)(f) of the GDPR. Regarding special categories of data (e.g., health data), data processing is permitted under Article 9(h) of the GDPR (**provision of medical care and health services**).
Description of the legitimate interest:	The legal basis for **recording telephone conversations** conducted through customer service is the legitimate interest of the data controller (the healthcare provider) and the patient. The legitimate interest is to ensure greater accountability in connection with the provision of healthcare; to establish and document the possibility of filing complaints or enforcement of legal claims. However, the patient can expect their data to be processed, as they are informed of this both at the start of the consultation and on the data controller's website. Audio recording is a particularly important safeguard in emergency consultations, for which there is no less restrictive alternative. The data subject is also entitled to several rights. These rights are described in detail in this document. It is specifically emphasized that the patient in question may **object** to the recording of their personal data. Under your right of access, you may also request a **copy of the audio recording.** Finally, patients may

	request **information** regarding the processing of their personal data.
Categories of data subjects:	Patients calling the data controller's designated phone number to ask for urgent or non-urgent specialist medical advice.
Categories of personal data processed:	Name of the person concerned, and, if applicable, the name of their employer, Social Security number, the data subject's phone number, the data subject's address/place of residence if an on-site consultation or transport to a facility is required, personal data provided by the patient necessary for specialist medical consultation, as well as special categories of such data (health data), the personal data and special categories of personal data (health data) contained in the specialist's response, as well as the personal data recorded in the written summary. In the case of a recorded telephone conversation, the data controller also handles the call's unique identification number (which includes the date and time of the call and the data subject's telephone number), as well as the data subject's voice.
Source of personal data:	In most cases, the patient in question provides the data themselves (upon request for a specialist's response); this is supplemented by personal data provided verbally or recorded in writing during the specialist's response.
The duration of data management:	Regarding medical records, in accordance with Section 30(1) of the Health Care Act (depending on the course of medical treatment), the retention period for data management is typically **30 years**. In the case of voice recordings, the duration of data processing is **5 years from the date of the recording made on the landline.** An exception to this rule applies if enforcement of legal claims is taken during this period. In this case, data processing will continue throughout the period necessary for the enforcement of legal claims.
Recipients (subjects of data transmission):	Personal data may be disclosed to third parties for the purpose of providing healthcare services. Third parties are defined as professional staff **involved** in the provision of healthcare services who are not employed by the facility, as well as cooperating independent business entities (doctors, patient transport providers,

	laboratories, diagnostic companies, home visit service providers, etc.). Patients are also informed separately about the transfer of data. The **VCC Life Hungary Kft.** (registered office: 1117 Budapest, 8–10 Október huszonharmadika Street Allee Corner Office Building, Bercsényi Tower, 4th Floor; company registration number: Cg.01-09-735941., TAX id nr: 13452696-2-43, contact details:info@virtual-call-center.hu) As a data processor, it provides the technical infrastructure for storing audio recordings of recorded telephone conversations conducted with customer service, and, if necessary, provides the technical infrastructure for customer service to access the audio recordings; it then deletes the audio recordings after the data retention period has expired. E-prescriptions issued as part of healthcare services, as well as medical records, are transmitted to the Electronic Healthcare Services Platform (EESZT) operated by the Ministry of the Interior (1051 Budapest, József Attila u. 2-4, Health Line; Email: info@egeszsegvonal.gov.hu). are forwarded to Healthline: 1812, E-mail: info@egeszsegvonal.gov.hu) the Electronic Healthcare Services Platform (**EESZT**) operated by the **Ministry of Interior** (1051 Budapest, 2-4 József Attila street). This is based on the fulfilment of a legal obligation (Section 2(1a) of EMMI Decree 39/2016 (XII.21)). https://e-egeszsegugy.gov.hu/hu/mi-az-eeszt-. While performing its duties—strictly for the purposes specified—**Bonitás IT Limited Liability Company** may access personal data in its capacity as a data processor. (registered office 6725 Szeged, 18 Szabadkai Street, company registration number: Cg.06-09-012933., TAX id nr: 14445181-4-06, contact details: info@bonitasit.hu), which, in its capacity as a data controller, provides comprehensive application management, application development, infrastructure management, IT consulting and services, as well as IT security services.
Third-country data transfers:	Data transfer does not take place.
Automated decision-making, profiling:	Automated decision-making, profiling does not take place.

Is the provision of data mandatory:	The data subject is not required to provide this information.
What are the consequences if the data subject does not provide their personal data:	Data reporting is the foundation of quality healthcare. It becomes impossible or inaccurate to provide a medical specialist opinion without adequate data reporting.

14. VIDEOCONSULTATION

In addition to telephone consultations, the data controller also offers video consultation services to its patients. In the cases specified in Sections 106/A–C of the Health Care Act, the use of the service is subject to photo identification via the EESZT system. The advantage of this service is that it facilitates a more comprehensive doctor-patient relationship than a telephone consultation, allowing for a more accurate assessment of the patient's condition. As part of the video consultation service, patients can consult with a specialist, receive advice, and, if necessary, have an e-prescription issued. A brief written summary of the video consultation will be prepared; this will form part of the patient's medical records and will also be available in the patient's personal account, provided the patient has created an account after registering. The audio and video content of the video consultation will not be recorded.

Your personal data is processed as follows:

The aim of data management	**Providing specialist consultations and enabling more accurate diagnosis of the patient's health conditions via video conference; the purpose of the brief written summary is also to document the patient's health-related complaints (symptoms) and the specialist's advice, thereby ensuring the healthcare provider's accountability.**
The legal basis for data management:	**Performance of a contract for the provision of healthcare services** pursuant to Article 6(1)(b) of the GDPR. Data processing related to the health advisory service is necessary and permissible for the purposes of preventive healthcare and the provision of healthcare services (GDPR Article 9(2)(h)). The processing of special categories of personal data for the **purposes of preventive healthcare or the provision of healthcare services** (Article 9(2)(h) of the GDPR) is necessary and permissible. Regarding medical records, **compliance with the legal obligation** specified in Article 6(1)(c) of the GDPR. The legal basis for this obligation is established by Section 136 of the Health Care

	Act, which stipulates that the data controller is required to prepare and retain medical records. No video or audio recordings are made, so no further data processing takes place there.
Description of the legitimate interest:	The data management is not based on a legitimate interest.
Categories of data subjects:	Patients using the video consultation service.
Categories of personal data processed:	Name of the person concerned, and, if applicable, the name of their employer, Social Security number, address/place of residence of the data subject in case of an on-site consultation or the need for transport to a medical facility, data necessary for patient identification, personal data provided by the patient(s) necessary for specialist medical consultation, as well as special categories of such data (health data); the personal data and special categories of personal data (health data) contained in the specialist's response, as well as the personal data recorded in the written summary.
Source of personal data:	In most cases, the patient in question provides the data themselves (upon request for a specialist's response); this is supplemented by personal data provided verbally or recorded in writing during the specialist's response.
The duration of data management:	Since the video consultation is not recorded, the data controller does not store the data subject's voice, the video footage showing the data subject, or the verbatim transcript of the conversation. Regarding the other data, the duration of data processing is as follows: **Pursuant to Section 30 of the Health Care Act, the written summary must generally be retained for 30 years.**
Recipients (subjects of data transmission):	Personal data may be disclosed to third parties for the purpose of providing healthcare services. Third parties are defined as professional staff **involved** in the provision of healthcare services who are not employed by the facility, as well as cooperating independent business entities (doctors, patient transport providers, laboratories, diagnostic companies, home visit service providers, etc.). Patients are also informed separately about the transfer of data.

	E-prescriptions issued as part of healthcare services, as well as medical records, are forwarded to the Electronic Healthcare Services Platform (EESZT) operated by the **Ministry of Interior** (1051 Budapest, József Attila u. are forwarded to Healthline: 1812, E-mail: info@egeszsegvonal.gov.hu) the Electronic Healthcare Services Platform (**EESZT**) operated by the **Ministry of Interior** (1051 Budapest, 2-4 József Attila street). This is based on the fulfilment of a legal obligation: Section 2, Paragraph 1a of EMMI Decree No. 39/2016 (December 21) https://e-egeszsegugy.gov.hu/hu/mi-az-eeszt-. While performing its duties—strictly for the purposes specified—**Bonitás IT Limited Liability Company** may access personal data in its capacity as a data processor. (registered office 6725 Szeged, 18 Szabadkai Street, company registration number: Cg.06-09-012933., TAX id nr: 14445181-4-06, contact details:info@bonitasit.hu), which, in its capacity as a data controller, provides comprehensive application management, application development, infrastructure management, IT consulting and services, as well as IT security services.
Third-country data transfers:	Third-country data transfer do not take place.
Automated decision-making, profiling:	Automated decision-making, profiling does not take place.
Is the provision of data mandatory:	Data provision is not mandatory.
What are the consequences if the data subject does not provide their personal data:	The provision of data is the basis of appropriate healthcare services; therefore, a lack of data reporting can constitute an obstacle to it.

15. COMPLAINT HANDLING

The patient—as a patient of the data controller—is entitled, pursuant to Section 29 of Act CLIV of 1997 (i.e., the Health Care Act), to file a complaint with the health care provider (which is the data controller, Buda Health Center LLC) regarding health care services; at the same time, the right to file a complaint is generally granted under Section 17/A of Act CLV of 1997 on Consumer Protection.

The healthcare provider or the maintaining authority is required to investigate the complaint and notify the complainant in written form of the results as soon as possible, but no later than thirty business days. Complaints must be recorded, and all documents related to the complaint, including the investigation, must be retained for 5 years.

The exercising the right to file a complaint does not affect the patient's right to contact the authorities responsible for patient rights, care recipient rights, and children's rights, as well as other relevant authorities,

in accordance with the provisions of specific legislation, for the purpose of investigating the complaint. The data controller is required to bring this circumstance to the patient's attention.
The data controller sets out the detailed rules for investigating complaints in its own internal policies (the **Complaint Handling Policy**—which is publicly available on the data controller's website—and detailed **Internal rules regarding the complaint handling process**).
Please note that if you file a complaint by phone, the data controller will record the phone call in accordance with the provisions of Chapter 5 of this Privacy Policy.

In connection with the handling of complaints, personal data is processed as follows:

The aim of data management	Investigating the complaint filed, taking appropriate action; and determining whether the same complainant has filed a repeat complaint regarding the same matter.
The legal basis for data management:	Compliance with a legal obligation under Article 6(1)(c) of the GDPR (the legal basis is Section 29(4) of the Health Care Act regarding health care, and Section 17/A(2) of the Consumer Protection Act regarding general complaints). About special categories of data (e.g., health data), data management is permitted under Article 9(h) and (i) of the GDPR.
Description of the legitimate interest:	The data management is not based on a legitimate interest.
Categories of data subjects:	Natural persons who have filed a complaint not related to healthcare; or the contact persons or legal representatives of legal entities filing such complaints; Patients filing complaints regarding healthcare services (pursuant to Section 3(a) of the Health Care Act, "patient" means a person who uses or receives healthcare services); and a representative authorized by the person filing the complaint, or the legal representative of the natural person filing the complaint; the person(s) affected by the complaint based on its content.
Categories of personal data processed:	The name and contact information of the person concerned (for the purpose of contacting them), the place and date of the complaint, the content of the complaint; the content of any attached documents; handwritten signature of the complainant; the name(s) of the person(s) concerned by the complaint—based on its content—and all data concerning them;

	the date and place of possible withdrawal of the complaint; the reason for the withdrawal, if provided by the data subject; the signature of the data subject or the data subject's representative who is withdrawing the complaint; the name of the authorized representative, contact person, or legal representative; the contact information provided by them (to facilitate communication); the date (place and time) and content of the power of attorney; and the names, addresses, and signatures of the witnesses to the document; where applicable, the name, registered office, and chamber identification number of the legal representative; and, in the case of a power of attorney recorded in a public document, the personal data requested to establish the complainant's identity and included in the public document, as well as any personal data of the notary public appearing in the public document. In the case of complaints submitted by telephone, the data controller also handles the complaint's unique identification number (which consists of the date and time of the call and the caller's phone number).
Source of personal data:	The data is provided by the data subject themselves.
The duration of data management:	The data controller shall **retain** the information contained in the complaint, as well as data related to the investigation conducted on that basis and the measures taken, for a period of **five years** from the completion of the last investigative action or measure (in accordance with Section 29(4) of the Health Care Act) However, if a legal claim is filed within five years and the legal proceedings are still ongoing after five years, data processing will continue until the legal claim is resolved.
Recipients (subjects of data transmission):	Personal data may be disclosed to third parties only in cases **specified by law** (e.g., bad faith) or with the complainant's **consent**, in connection with the investigation of the complaint. Third parties are defined as professional staff **involved in the provision of healthcare services** who are not employed by the facility, as well as cooperating independent business entities (doctors, patient transport providers,

	laboratories, diagnostic companies, home visit service providers, etc.). We hereby draw the attention of the data subject to the fact that if they do not consent to the transfer of data, their complaint may not be investigated, as the investigation will face limitations or obstacles in the absence of the ability to transfer data. The **VCC Life Hungary Kft.** (registered office: 1117 Budapest, 8–10 Október huszonharmadika Street Allee Corner Office Building, Bercsényi Tower, 4th Floor; company registration number: Cg.01-09-735941., TAX id nr: 13452696-2-43.; e-mail address: info@virtual-call-center.hu), as a data processor, in the case of complaints made by phone, it provides the technical infrastructure for storing the audio recordings of calls with customer service, and, if necessary, provides the technical infrastructure for customer service to access the audio recordings; it then deletes the audio recordings after the data retention period has expired. If the complaint is forwarded to an **authority, court, prosecutor's office**, or **other** third party, such recipients will act as independent data controllers. While performing its duties—strictly for the purposes specified—**Bonitás IT Limited Liability Company** may access personal data in its capacity as a data processor. (registered office 6725 Szeged, 18 Szabadkai Street, company registration number: Cg.06-09-012933., TAX id nr: 14445181-4-06, contact details: info@bonitasit.hu), which, in its capacity as a data controller, provides comprehensive application management, application development, infrastructure management, IT consulting and services, as well as IT security services.
Third-country data transfers:	Data transfer does not take place.
Automated decision-making, profiling:	Automated decision-making, profiling does not take place.
Is the provision of data mandatory:	No, in such case, the ability to investigate the complaint or provide information regarding, is limited or impeded.

What are the consequences if the data subject does not provide their personal data:	In such case, the ability to investigate the complaint or provide information regarding, is limited or impeded.

16. CUSTOMER SATISFACTION SURVEY

To improve its services, the data controller encourages its patients to share their opinions regarding the provision of healthcare services and has introduced a questionnaire for this purpose. The questionnaire is also available at **https://bhc.hu/urlapok-kerdoivek/vevo-elegedettseg-egyeni-jaro**, and all patients of the data controller will receive it via email after receiving medical care (if they have provided the data controller with their email address). Respondents can choose to complete the questionnaire anonymously or by providing their personal information. This is based on the patient's freedom of choice. Providing personal information helps us to investigate reports, to identify specific errors or shortcomings, as well as to contact the patient. The patient may also choose not to receive future questionnaires; in this case, the data controller will not send the patient a satisfaction survey in connection with any future healthcare services.

The management of personal data in connection with the satisfaction survey is as follows:

The aim of data management	**Evaluating the data controller's services, ensuring that the services meet the required standards, and correcting and eliminating errors and deficiencies.**
The legal basis for data management:	The legal basis for sending out satisfaction surveys is the **legitimate interest** of the data controller under Article 6(1)(f) of the GDPR. When questionnaires are returned with personal data provided, the legal basis for further data processing is the **data subject's consent** pursuant to Article 6(1)(a) of the GDPR, **which may be withdrawn at any time without giving a reason.** If a complaint procedure is initiated based on the processing of additional personal data provided when returning the questionnaire, the legal basis for data processing is following **a legal obligation pursuant to Article 6(1)(c) of the GDPR (the legal basis is Section 29(4) of the Health Act**).
Description of the legitimate interest:	The data controller's legitimate interest is to identify errors and shortcomings and to continuously improve the quality of the service. However, this legitimate interest of the data controller also aligns with the legitimate interest of the data subject/patient.
Categories of data subjects:	Regarding the distribution of questionnaires, the data subjects are patients who have used the data controller's healthcare services and have not opted out of receiving satisfaction surveys.

Categories of personal data processed:	The data subject's name and email address (for the purpose of sending out the questionnaires); if the data subject submits a response containing additional personal data, the personal data processed also includes: the date the satisfaction survey was submitted, the date of the healthcare service used and mentioned, the healthcare professionals involved, and the data content of the evaluation.
Source of personal data:	The data is provided by the data subject themselves.
The duration of data management:	The data controller will process the data subject's personal data for this purpose until the data subject **objects** to receiving the questionnaires; after that, the data subject will no longer receive the questionnaires. If a patient returns the questionnaire without remaining anonymous and provides only positive feedback, the data controller will **send a thank-you email** and then delete any personal data contained in the response. If the patient returns the questionnaire without remaining anonymous and raises a problem or expresses criticism, the data controller will **treat this as a complaint submission** and proceed in accordance with Section 15 ("Complaint Handling"). The provisions of paragraph 15 apply.
Recipients (subjects of data transmission):	While performing its duties—strictly for the purposes specified—**Bonitás IT Limited Liability Company** may access personal data in its capacity as a data processor. (registered office 6725 Szeged, 18 Szabadkai Street, company registration number: Cg.06-09-012933., TAX id nr: 14445181-4-06, contact details:info@bonitasit.hu), which, in its capacity as a data controller, provides comprehensive application management, application development, infrastructure management, IT consulting and services, as well as IT security services.
Third-country data transfers:	Third country data transfer do not take place.
Automated decision-making, profiling:	Automated decision-making, profiling does not take place.
Is the provision of data mandatory:	No, in this case, the survey is evaluated anonymously.

What are the consequences if the data subject does not provide their personal data:	The survey is evaluated anonymously, which may limit the identification and effective solutions of specific problems.

17. REPORTING FOUND ITEMS

The data controller accepts written reports regarding found items at the email address **talalttargyak@bhc.hu.** The related data processing procedures are as follows:

The aim of data management	**Reviewing reports; locating and identifying the rightful owners of found items; communicating with the person who reported the item.**
The legal basis for data management:	The data controller's **legitimate interest** pursuant to Article 6(1)(f) of the GDPR.
Description of the legitimate interest:	The legitimate interest is to return lost items to their owners and to demonstrate the data controller's accountability in this regard.
Categories of data subjects:	Natural persons who send a report to the email address above.
Categories of personal data processed:	The data subject's name, email address, the date the email was sent, the subject line, and the content.
Source of personal data:	The data is provided by the data subject themselves.
The duration of data management:	One year period from the date of submission.
Recipients (subjects of data transmission):	While performing its duties—strictly for the purposes specified—**Bonitás IT Limited Liability Company** may access personal data in its capacity as a data processor. (registered office 6725 Szeged, 18 Szabadkai Street, company registration number: Cg.06-09-012933., TAX id nr: 14445181-4-06, contact details: info@bonitasit.hu), which, in its capacity as a data controller, provides comprehensive application management, application development, infrastructure management, IT consulting and services, as well as IT security services.
Third-country data transfers:	Third country data transfer do not take place.
Automated decision-making, profiling:	Automated decision-making, profiling does not take place.
Is the provision of data mandatory:	No, in this case, the purpose and effectiveness of data processing could be compromised.
What are the consequences if the data subject does not provide their personal data:	In this case, the purpose and effectiveness of data processing could be compromised, and it could hinder efforts to locate the owner.

18. BEK ACADEMY

Data processing on the BEK Academy website at "https://akademia.bhc.hu"

As part of the **BEK Academy Program**, the data controller organizes **professional training courses** for doctors and healthcare professionals, some of which are credit based and others are not. Doctors typically register for credit-based courses via the OFTEX website, while doctors and healthcare professionals must register for non-credit-based courses via the BEK ACADEMY website. The website can be found at: https://bek-akademia.hu. This website also offers the option for third parties to **rent** the Academy's premises for a specified period under a contract, for the purpose of holding **events** or **gatherings** not organized by the data controller.
The data controller also publishes the **BEK Academy Newsletter**, which covers the operations of BEK Academy, current developments in healthcare, and its training and continuing education programs; readers can choose to subscribe.

The following data management processes take place on the BEK Academy website:

17.1 Contact information for the data controller of the BEK Academy website
17.2 The web hosting provider for the BEK Academy website
17.3 Data processing related to cookies used on the BEK Academy website
17.4 Management of personal data regarding textual content, names, job titles, and contact information appearing on the website
17.5 Data processing related to the photos appearing on the website
17.6 Rules of data processing related to registration on the BEK Academy website (opening a customer account)
17.7 Rules for the processing of personal data related to applications for training and education events via the BEK Academy website
17.8 Rules Governing Data Management in Connection with the Distribution of the BEK Academy Newsletter (Newsletter)
17.9 Rules governing data processing related to the reservation of the BEK Academy venue for other purposes

18.1 CONTACT INFORMATION FOR THE DATA CONTROLLER OF THE BEK ACADEMY WEBSITE

Data Controller Details	Data Protection Officer's Details
Buda Health Center LLC (BHC) Represented by: Dr István Csernavölgyi Chief Executive Officer	Dr. Ádám Kéri, Dr Szonja Kéri, Dr Tamás Sándor Kéri Chief Data Protection Officer: Dr Ádám Kéri
1126 Budapest, 1-3. Királyhágó street	1281 Budapest, Post Office Box.12.
Cg.01-10-141707., https://www.bhc.en, dpo@bhc.hu	adam.keri.office@icloud.com

18.2 THE WEB HOSTING PROVIDER FOR THE BEK ACADEMY WEBSITE

Web hosting service is an online service in which the resources of a server are shared among multiple users. Each user occupies a dedicated storage space provided by the system, and the public content stored there is accessible via a unique domain name. In this case, the domain name is https://bek-akademia.hu. The data controller, BHC uses the services of the web hosting provider to operate this website.
101 Avenue of the Americas 10th Floor New York, NY 10013 United States.

The data controller uses the virtual server services provided by **DigitalOcean LLC** (headquartered at: 101 Avenue of the Americas 10th Floor New York, NY 10013 United States. website: https://www.digitalocean.com; e-mail address: privacy@digitalocean.com). The service provider is a third-country service provider that uses the European Commission's standard contractual clauses. The website provider's privacy policy is available there: https://www.digitalocean.com/legal/gdpr-faq

18.3. DATA PROCESSING RELATED TO COOKIES USED ON THE BEK ACADEMY WEBSITE

Anonymous visitor identifiers (**cookies**) are **files or pieces of information** that are **stored on the user's computer**, internet device, smartphone, or iPad **when visiting the website**. Cookies are used to facilitate the operation of the website, to enable communication with website visitors (e.g., displaying marketing messages), and to collect statistical and other information about website visitors (see, for example: IP address, time of access to the website, navigation on the website, name of the previous website visited).
Based on legitimate interest the data controller uses cookies that are strictly necessary for visiting and operating the website. In addition, based on the legal basis of the data subject's consent, data controller uses cookies for other purposes, such as statistical data collection and marketing. **These cookies can be disabled by the user/data subject or deleted at any time from the user's/data subject's computer (under the "Settings" menu).**

The data controller provides information on the cookies used, as well as their functions and duration, on its website (https://akademia.bhc.hu).

18.4. PROCESSING OF PERSONAL DATA RELATED TO TEXTUAL CONTENT, NAMES, JOB TITLES, AND CONTACT INFORMATION APPEARING ON THE WEBSITE

Under the "**About Us**" menu item on the website, in the "OUR TEAM" section, the data controller lists the names, job titles, email addresses, and mobile phone numbers of the employees responsible for training and venue reservations.

In addition, the data controller publishes articles and news under the "**News/Blog**" menu item, with the aim of providing information about events and training courses related to the data controller's activities, as well as presenting the current state of healthcare, important developments, and so on. In rare cases, articles and news may record names, medical specialties associated with those names, or significant events, awards, honours, etc., related to those names.

The processing of personal data related to the website's text content is carried out as follows:

The aim of data management	**Information about the data controller's authorized employees; and facilitating contact with them (see: "About Us"); as well as information about the data controller's healthcare activities, educational and other events it organizes, and current topics in healthcare (see: „News/blog").**
The legal basis for data management:	The legal basis for data management is the data controller's **legitimate interest** pursuant to Article 6(1)(f) of the GDPR.
Description of the legitimate interest:	On the one hand the data controller's **significant legitimate interest** is, **the publication of contact**

	information to support its training and educational activities and the participants in such training, as well as the description of the responsibilities of the staff organizing the training ("About Us"); and, on the other hand, to **publish news, information, and current events related to the healthcare sector** ("News/Blog"). The publication of contact and job-related information about employees is necessary for the purpose of data management. In all cases, the description of their duties and contact information is provided to facilitate their work; furthermore, only work-related contact information is disclosed. Personal data may also be displayed in text content (news articles, blog posts) in a targeted manner. Such data includes the data subject's name, place of employment, job title, and position, as well as the fact that the data subject is involved in the event or incident described by the data controller. The textual content not only highlights the data controller's achievements and future plans but also sheds a positive light on the third party mentioned in the text (recognition, awards, etc.),and thus is unlikely to infringe upon the aforementioned right, or may not infringe upon it at all. **We would like to specifically draw the attention of those concerned to their right to object.** We would also like to highlight that this table solely regulates the text-based display form; different rules apply to images and photos appearing on the website (see the table on data management in the following section).
Categories of data subjects:	Individuals who contribute as employees to the implementation and organization of the data controller's educational and training activities conducted via the website ("About Us"); as well as individuals mentioned in the texts published on the website ("News/Blog").
Categories of personal data processed:	The name of the employee concerned; their job title, email address, and mobile phone number ("**About Us**"); or the name, job title, or professional qualifications of the person concerned; or, possibly, any achievements they have made, supported, or

	presented, or other information of positive news value ("**News/Blog**").
Source of personal data:	Most of the data is collected by the data controller itself, with no involvement of the data subject (through the publication of articles and news, and the introduction of employees involved in the organization). The personal data regarding the data subject is appearing in articles and news reports is, for the most part, publicly available information that can be obtained from freely accessible sources—in many cases, sources that have already been published in the press. Employee data refers to workplace contact information available to the data controller.
Categories of recipients:	The website is **freely accessible** without prior registration or identification, meaning that any personal data uploaded to it is freely available to anyone until the data controller removes it from the website. **DigitalOcean LLC**, a virtual server provider, may access the data for specific purposes in its capacity as a data processor.
Third-country data transfers:	Data is transferred to **DigitalOcean LLC, a virtual server provider** operating as a data processor (as described in Section 2).
Automated decision-making, profiling:	Automated decision-making, profiling does not take place.
Scheduled deadline for data cancellation:	The written content appearing on the website is public and accessible to anyone; it remains available for review as long as it is current and newsworthy, that is, until the data controller removes it from the website. **We would like to remind those concerned once again of their right to object to the processing of personal data based on legitimate interests.**
Is the provision of data mandatory:	The data is collected partly by the data controller itself ("News/Blog") and partly is already available ("About Us"), so the involvement of the data subjects is not necessary. Most of the personal data mentioned in articles and news reports is publicly available information that can be obtained from websites and other news sources. In addition to the employee's name, employee data includes information necessary for communication, the provision of which is a prerequisite for the employee to perform their duties and for contacting applicants for training.

What are the consequences if the data subject does not provide their personal data:	The data controller does not collect the personal data listed here directly from the data subject.

18.5. DATA PROCESSING RELATED TO THE PHOTOS APPEARING ON THE WEBSITE

The photos displayed on the website under the "About us" menu item in the "OUR TEAM" section, as well as in the "GALLERY" section under the "Event venue" menu item, are managed as follows:

The aim of data management:	**Information about the data controller's employees, to help identify them ("OUR TEAM"); and, in the "Gallery" section, a presentation of the atmosphere, quality, and characteristics of past events.**
The legal basis for data management:	The **data subject's prior consent** pursuant to Article 6(1)(a) of the GDPR. If the data subject does not wish to give consent to the processing of images (photos) taken of him/her, he/she has the right to inform the data controller thereof. The data subject's consent regarding the use of images is **voluntary**; that is, they are **free to deny consent**. In such cases, the images taken of him/her will not be processed. If the data subject has given consent to the processing of images taken of them, they **may withdraw that consent at any time thereafter without providing a reason.** In such cases, the data controller will immediately remove the image uploaded to the website. Please note that the data controller does not upload any photos or videos of children under the age of 16.
Description of the legitimate interest:	The processing of data is not based on legitimate interests.
Categories of data subjects:	The individuals appearing in the photos uploaded to the website (under the headings "OUR TEAM" and "Gallery").
Categories of personal data processed:	A photo of the data subject (image) and his/her company shown in the photo, surroundings visible in the photo; the location of the photo and other information appearing in the photo.
Source of personal data:	The data subject provides this information voluntarily; however, the provision of personal data is not mandatory, and the data subject's consent to the processing of personal data already provided may be freely withdrawn at any time.
Categories of recipients:	These areas of the website (the "About Us" menu item and the "Gallery" menu item under "Event Venue") are **freely accessible** without prior registration or identification, meaning that any

	personal data uploaded there can be viewed by anyone; this remains the case until the data controller removes such data from the website. Data is transferred to **DigitalOcean LLC**, a virtual server provider operating as a data processor.
Third-country data transfers:	Data is transferred to **DigitalOcean LLC**, a virtual server provider operating as a data processor (as described in Section 2).
Automated decision-making, profiling:	Automated decision-making, profiling does not take place.
Scheduled deadline for data cancellation:	The photos appearing on the website are public and accessible to anyone; they remain available for review until the data controller removes them from the website or the data subject withdraws their consent.
Is the provision of data mandatory:	No. The data subject's consent regarding the use of images is **voluntary**; that is, they are **free to deny consent**. In addition, the data subject may **withdraw their consent at any time in the future without providing a reason.**
What are the consequences if the data subject do not provide their personal data:	The data subject is free to choose not to provide their personal data; in that case, the photo taken of them will not be uploaded to the website. If the data subject subsequently withdraws their consent, the photo of them will be removed from the website.

18.6. RULES OF DATA PROCESSING RELATED TO REGISTRATION ON THE BEK ACADEMY WEBSITE (OPENING A CUSTOMER ACCOUNT)

If the website visitor wishes to browse the website not only with limited content but in its entire scope, and at the same time wishes to use its key functions, registration is required.

Key functions of the website: submitting applications for training and education events; providing the personal data required to enter into an adult education contract related to further training; certifying participation in (further) training; subscribing to the BEK Academy Newsletter; reserving or booking the BEK Academy venue for other purposes; and, if necessary, providing the personal data required for invoice payment.

Registration involves first opening a personal customer account and then filling out your profile information. All you need to open a customer account is to provide your email address and a password. The system then sends a confirmation email to the user, who must confirm their intention to register by clicking on the link provided in the email. After that, the entire content of the website will be available for viewing and browsing.

However, to use the website's key functions listed above, you must complete your profile information, either in part or in full.

The aim of data management	**-Getting to know the full extent of the website;** **-Selecting events for (further) training purposes;**

	-Applying for training/education event; **-Providing the additional information required to enter an adult education contract;** **-Proof of attendance at the training course;** **- Reservation of the BEK Academy venue for another event;** **-Providing the information required to issue an invoice (if a payment obligation arises);** **- Providing the option to subscribe to BEK Academy Newsletters regarding the data controller's events and training sessions organized by it.**
The legal basis for data management:	The data subject's **consent** pursuant to Article 6(1)(a) of the GDPR, which may be withdrawn at any time. In this case, your registration (i.e., your personal account) will be deleted.
Description of the legitimate interest:	The data management is not based on a legitimate interest.
Categories of data subjects:	Patients registering to create a personal customer account.
Categories of personal data processed:	To complete the first step of registering on the website—**creating a personal account**—you must provide an email address and password and agree to this Privacy Policy. We would like to note in advance that before registering for specific adult education events—the data processing for which is described in the following section—you must provide your **Profile Data** in full (pursuant to Act LXXVIII of 2013 on Adult Education /hereinafter: Please note that before registering for specific adult education events—the data processing for which is described in the following section—you must provide your Profile Data in full (since these are training programs falling under the scope of Act LXXVIII of 2013 on Adult Education /hereinafter: Fktv./), which are as follows: name, email address, phone number, identification of the category required for professional registration (doctor, healthcare professional, or other), birth name, mother's name, place and date of birth, professional qualifications, highest level of education, medical license number, operating license number, healthcare professional registration number, whether the data subject is a BEK employee or BEK contributor, billing information (individual or legal entity/ company /name exact residential address or registered office, mailing address); whether the data subject subscribes to the BEK Academic Newsletter. In your Profile Information, you will later find details about the events you have already registered for or attended.
Source of personal data:	The data is provided by the data subject themselves.
The duration of data management:	Registration is based on the patient's consent, which **may be withdrawn at any time without providing a reason.** In this case, your personal account will be deleted. Please note, however, that if you have registered for a training or continuing education event; or have reserved a venue at the BEK Academy; or if any other legal relationship has been established between you and the data controller; the data controller will continue

	to process your personal data within the data processing period prescribed for these legal relationships (see: data processing described in the following sections); only the deletion of your personal customer account will be carried out in accordance with your request.
Recipients (subjects of data transmission):	Data is transferred to **DigitalOcean LLC**, a virtual server provider operating as a data processor (as described in Section 2).
Third-country data transfers:	Data is transferred to **DigitalOcean LLC**, a virtual server provider operating as a data processor (as described in Section 2).
Automated decision-making, profiling:	Automated decision-making, profiling does not take place.
Is the provision of data mandatory:	No, but in this case, we cannot create a personal customer account.
What are the consequences if the data subject does not provide their personal data:	You will not be able to browse the entire website or use its key features.

18.7. RULES FOR THE PROCESSING OF PERSONAL DATA RELATED TO APPLICATIONS FOR TRAINING AND EDUCATION EVENTS VIA THE BHC ACADEMY WEBSITE

Registering for (continuing) education events is a key feature of the website, which requires not only the creation of a personal account but also the completion of all profile information.
Personal data provided in the registration form submitted via the website for the training event is processed as follows:

The aim of data management	**- Indication of intent to participate in training/further education events;** **-Providing the additional information required to enter an adult education contract;** **-Providing the personal information required to verify attendance at the training;** **-Providing the information required to issue an invoice (if a payment obligation arises);**
The legal basis for data management:	In the context of adult education, the legal basis for data processing is partly the performance of a **contract for adult education pursuant to Article 6(1)(b) of the GDPR**; and partly the fulfilment of a legal obligation under the Adult Education Act (Article 6 (1)(c) **Fktv**), with the obligation prescribed by Section 21(1) of the Adult Education Act (see: Data that is mandatory to be processed in the context of adult education). Regarding the transfer of data to OFTEX, as listed among the recipients (data recipients), the legal basis for data processing is the **fulfilment of the legal obligation** under Article 6 (1)(c) of the GDPR, the legal basis for which is 64/2011. (XI. 29.) NEFMI Decree on the continuous professional education of physicians, dentists, pharmacists, and holders of higher education degrees in healthcare. (XI.29.) NEFMI Decree No. 64 of November 29, 2011. Regarding adult education, the legal basis for the mandatory data transfer to the **Pest County Government Office** (**Adult Education Data Reporting System**) is the fulfilment of a legal obligation under Section 15 of the Adult Education Act /Article 6(1)(c) of the GDPR/.

	The legal basis for the processing of personal data necessary to comply with the documentation requirement is the **fulfilment of a legal obligation** pursuant to Article 6(1)(c) of the GDPR. This legal obligation is based on Sections 159 and 169 of Act CXXVII of 2007 on Value-Added Tax, and Sections 166–169 of Act C of 2000 on Accounting. In the event of a legal dispute between the data controller and the data subject regarding the legal relationship relating to adult education, the legal basis for data processing is the **legitimate interest** referred to in Article 6(1)(f) of the GDPR.
Description of the legitimate interest:	Personal data is processed solely based on legitimate interest in the event of a legal dispute. In such cases, the data controller's legitimate interest lies in fully clarifying the facts of the matter and facilitating the imposition of lawful sanctions, as well as in providing the available data as evidence to the competent authority, the public prosecutor's office, and the court. Since the legitimate interest described above is consistent with the interests of the data subject, no actual infringement of rights occurs.
Categories of data subjects:	Doctors, pharmacists, and healthcare professionals applying for training.
Categories of personal data processed:	Since the training event falls under the **scope of the Fktv**., it is mandatory to provide all profile information, which includes the following: name, email address, phone number, identification of the category required for professional registration (physician, healthcare professional, or other), birth name, mother's name, place and date of birth, professional qualifications, highest level of education, medical license number, operating license number, healthcare professional registration number, whether the data subject is a BEK employee or BEK contributor, billing information (individual or legal entity, company name, exact residential address or registered office, mailing address, tax ID number of the legal entity). We would like to point out now that, under the "Profile Data" menu item, the personal customer account will record details of all training events for which the individual has registered or in which they have already participated (training history). In connection with the **conclusion of an adult education contract,** the data controller is required, pursuant to Section 21(1) of the Data Protection Act, to process the following data for the purpose of conducting the adult education program: a) the person participating in the training (aa) their personal identification data and—in connection with the issuance of an education identification number—their education identification number, ab) their email address and (ac) information regarding their highest level of education. (b) data related to the training, concerning the person participating in the training (ba) their highest level of education, vocational qualifications, professional skills, and knowledge of foreign languages, (bb) upon entering the program and completing it, or, if the program is not completed, upon withdrawing from it, (bc) assessment and grading during the course, (bd) relate to payment obligations associated with the training and to the training loan taken out

	Personal data processed for the purpose of **verifying attendance:** name, signature, training location, topic, and date of the training. Personal data processed in connection with **invoices issued** for fee-based training events: company/name, address or registered office, tax ID number.
Source of personal data:	The data is provided by the data subject themselves.
The duration of data management:	The data controller will **process the profile data provided by the data subject** on the website until the data subject requests the termination of their personal customer account. Pursuant to Section 21(5) of the Fktv. the data controller must **retain adult education data for a period of 8 years from the date of conclusion of the adult education contract; the date of completion of attendance records; or the date of completion of the initial assessment of prior knowledge and competencies,** regardless of whether the personal account is subsequently terminated. Similarly, an **8-year** retention requirement applies to the retention of **account data** and **supporting documents** under Act CXXVII of 2007 on Value Added Tax and Act C of 2000 on Accounting. If **legal proceeding**s (e.g., a dispute before an administrative authority, a prosecutor's office, or a court) have been initiated within the aforementioned data retention period, the processing of the data will continue for the entire duration of the legal proceedings.
Recipients (subjects of data transmission):	For credit-based training, physicians are required to register through the **OFTEX** data management system. Oftex data management system is operated by **ENEF Kft** (2151 Fót, 14/a Mária Street Cg.13-09-066514., e-mail address: nfkft@nf.hu) which is an independent data controller. Their data protection notice is available here: https://oftex.hu/project_o/actual_prg/system/launch.php?pg=./oftex/ADATVEDELEM.html The data controller is required to report data on adult education events to the FAR system (**Adult Education Data Reporting System**) (Section 15 of the Adult Education Act) Data Controller provides data regarding: (a) the name, nature, location, number of hours, first day of the training, and—except for trainings conducted via closed-system distance learning—the scheduled completion date of the education or training, b) the personal identification data, email addresses, and highest level of education of the individuals participating in the training, c) the tuition fee and who is responsible for paying it the data is submitted to the state administrative body responsible for adult education (currently: **Pest County Government Office, National Vocational and Adult Education Office.** , 1089 Budapest, 7 Kálvária square felnottképzés@pest.gov.hu, phone: +36 1 210 9722) via the adult education data reporting system. This body acts as an independent data controller. The reporting obligation must be fulfilled no later than the start date of the training; in the event of a change in the data, no later than the third business day following the

	change; and, in the case of in-house training, by the last day of the quarter in which the training concludes. The data provided in this manner may be used for statistical purposes and may be transferred for such purposes in a form that does not allow for the identification of individuals; furthermore, it may be transferred to and used by the **Hungarian Central Statistical Office** for statistical purposes in a form that allows for individual identification, free of charge. Hungarian Central Statistical Office is also an independent data controller. In the event of a payment obligation, payment is processed using the Simple Pay application provided by **OTP Mobile Service Provider** 1138 Budapest, 135–139 Váci street, Building B, 5th floor; contact: idea@otpmobil.com), which is considered an independent data controller. Their data protection notice is available here: https://simplepay.hu/adatkezelesi-tajekoztatok/ As the data controller, BHC processes only the date, amount, and payment reference of online payments. The invoice data is forwarded to the **National Tax and Customs Administration of Hungary (NAV)** For the purpose of troubleshooting the accounting, payroll, and labour records software (ORGWARE), **OrgwareCommercial and Service Limited Liability Company** (headquartered at: 1149 Budapest, 32 Angol Street, company registration number: Cg.01-09-062418., TAX id nr: 10244830-2-42, e-mail address: support@orgware.hu or management@orgware.hu, website: http://www.orgware.humay access personal data as an independent data controller . Data is transferred to **DigitalOcean LLC**, a virtual server provider operating as a data processor (as described in Section 2). Data is transferred to the **training provider** to the minimum extent necessary (names of training applicants, number of applicants, and any personal data requested in advance by the provider—e.g., in the event of a knowledge level assessment, contact information). In the event of an **official inspection**, personal data will be disclosed to the relevant authority (e.g., the Government Office); in the event of **legal proceedings**, personal data will be disclosed to the competent authority, the public prosecutor's office, the court, or the legal representative. All these recipients are independent data controllers. While performing its duties—strictly for the purposes specified—**Bonitás IT Limited Liability Company** may access personal data in its capacity as a data processor. (registered office 6725 Szeged, 18 Szabadkai Street, company registration number: Cg.06-09-012933., TAX id nr: 14445181-4-06, contact details: info@bonitasit.hu), which, in its capacity as a data controller, provides comprehensive application management, application development, infrastructure management, IT consulting and services, as well as IT security services.
Third-country data transfers:	Data is transferred to **DigitalOcean LLC**, a virtual server provider acting as a data processor (as described in section 2).

Automated decision-making, profiling:	Automated decision-making, profiling does not take place.
Is the provision of data mandatory:	Providing personal information is a prerequisite for participating in the training program.
What are the consequences if the data subject does not provide their personal data:	He or she cannot participate in the training because, in the absence of the required data, an adult education contract cannot be entered into with him or her; his or her attendance and the earning of credit hours cannot be verified; and the data controller's legal obligation to report adult education data cannot be fulfilled.

18.8. RULES ON DATA PROCESSING RELATED TO THE SENDING OF THE BEK ACADEMY NEWSLETTER (NEWSLETTER)

Data subjects who have a personal customer account may subscribe to the BEK Academy Newsletter by checking the box in the section that appears after the "Newsletter Subscription" question following the Profile Data section. In this case, the data controller will send the BEK Academic Newsletters to the email address provided by the data subject until the data subject unsubscribes from this newsletter service. The service may be cancelled at any time, without restriction and without the need to provide a reason.

The aim of data management	Presenting information about the Data Controller's events and training sessions and sharing general health-related news.
The legal basis for data management:	The data subject's consent pursuant to Article 6(1)(a) of the GDPR, which may be withdrawn at any time without giving a reason.
Description of the legitimate interest:	The data management is not based on a legitimate interest.
Categories of data subjects:	Natural persons who have subscribed to the BEK Academy's General Newsletter.
Categories of personal data processed:	The name and email address provided by the data subject.
Source of personal data:	The data is provided by the data subject themselves.
The duration of data management:	Until the data subject withdraws their consent (unsubscribes).
Recipients (subjects of data transmission):	Data is transferred to **DigitalOcean LLC**, a virtual server provider acting as a data processor (as described in section 2). While performing its duties—strictly for the purposes specified—**Bonitás IT Limited Liability Company** may access personal data in its capacity as a data processor. (registered office 6725 Szeged, 18 Szabadkai Street, company registration number: Cg.06-09-012933., TAX id nr: 14445181-4-06, contact details: info@bonitasit.hu), which,

	in its capacity as a data controller, provides comprehensive application management, application development, infrastructure management, IT consulting and services, as well as IT security services.
Third-country data transfers:	Data is transferred to **DigitalOcean LLC**, a virtual server provider acting as a data processor (as described in section 2).
Automated decision-making, profiling:	Automated decision-making, profiling does not take place.
Is the provision of data mandatory:	No, in this case, the BEK Academy Newsletter cannot be sent by the data controller.
What are the consequences if the data subject does not provide their personal data:	The data subject will not receive the BEK Academy's General Newsletter.

18.9. RULES ON DATA PROCESSING RELATED TO THE RESERVATION OF THE BHC ACADEMY VENUE FOR OTHER PURPOSES

Data subjects with a personal customer account are entitled to reserve the BEK Academy venue for other purposes by initiating the request-for-quote process on the website.

To make a reservation—that is, to express your intention to enter a contract or request a quote for a specific date and duration—it is not necessary to complete all sections of the Profile Information; you need only provide the personal data required to prepare for and enter the contract. After the request is submitted on the website, the data controller will contact the data subject.

Personal data provided for the purpose of making a reservation on the website is processed as follows:

The aim of data management	Reservation of the BEK Academy venue for other events—i.e., events not organized or advertised by the data controller—or an indication of intent to rent the premises.
The legal basis for data management:	The legal basis for data processing is the **performance of a contract** between the data subject (or the person represented by the data subject) and the data controller, in accordance with Article 6(1)(b) of the GDPR. Regarding the personal data necessary to fulfil the documentation obligations associated with the contract, the legal basis for data processing is **compliance with a legal obligation** under Article 6(1)(c) of the GDPR. This legal obligation is based on Sections 159 and 169 of Act CXXVII of 2007 on Value-Added Tax, and Sections 166–169 of Act C of 2000 on Accounting. In the event of a legal dispute between the data controller and the data subject regarding the lease agreement, the legal basis for data processing is the **legitimate interest** referred to in Article 6(1)(f) of the GDPR.
Description of the legitimate interest:	Personal data is processed solely based on legitimate interest in the event of a legal dispute. In such cases, the data controller's legitimate interest lies in fully clarifying the facts of the matter and facilitating

	the imposition of lawful sanctions, as well as in providing the available data as evidence to the competent authority, the public prosecutor's office, and the court. Since the legitimate interest described above is consistent with the interests of the data subject, no actual infringement of rights occurs.
Categories of data subjects:	Individuals who have reserved the BEK Academy venue for another event and are requesting a contract proposal.
Categories of personal data processed:	**Personal data processed when booking the BEK Academy venue for other events—i.e., data requested on the website**—includes: the requester's name, email address, phone number, company name, the event date, start and end date, the estimated number of attendees, and details of any additional requirements (projector, projection screen; technical assistance; cloakroom; wireless presenter; microphone; parking; streaming; microport; cleaning; laptop; sound system; catering; flipchart; stage setup; hostess), any additional comments from the requester, and the date and time the request for quotation was sent. Following the successful booking of the venue and acceptance of the data controller's offer, the following additional personal data are processed in the venue rental agreement: specific details of the venue, the nature of the event, the rental fee, payment details, the names and contact information of the contact persons and representatives, the date of the agreement, and their handwritten signatures. Personal data processed in connection with the **invoice** issued: company name, address or registered office, tax identification number.
Source of personal data:	The data is provided by the data subject themselves.
The duration of data management:	The data controller will continue to process personal data processed in connection with the performance of the contract for the duration of the civil law **statute of limitations (5 years from the date the claim arises)**, to ensure the possibility of processing such data should it be necessary to assert any legal claims. In contrast, an **8-year** retention requirement applies to the management of **invoice data and supporting documents** under Act CXXVII of 2007 on Value Added Tax and Act C of 2000 on Accounting.
Recipients (subjects of data transmission):	The invoice data is forwarded to the **National Tax and Customs Administration of Hungary (NAV)** For the purpose of troubleshooting the (ORGWARE), **OrgwareCommercial and Service Limited Liability Company** (registered office: 1149 Budapest, 32 Angol Street, company registration number: Cg.01-09-062418., TAX id nr: 10244830-2-42, e-mail address: support@orgware.hu or management@orgware.hu, website: http://www.orgware.humay access personal data as an independent data controller .

	The data controller may disclose the personal data it processes to the **authority** conducting an inspection (e.g., the National Tax and Customs Administration) in the event of an **official inspection**; furthermore, in the event of a **legal dispute**, the personal data will be disclosed to the relevant authority, the public prosecutor's office, the court, or a legal representative. All these recipients above are independent data controllers. Once the data controller receives a request for a quote via the website, the data is transferred to **DigitalOcean LLC**, a virtual server provider acting as a data processor (as described in section 2). While performing its duties—strictly for the purposes specified—**Bonitás IT Limited Liability Company** may access personal data in its capacity as a data processor. (registered office 6725 Szeged, 18 Szabadkai Street, company registration number: Cg.06-09-012933., TAX id nr: 14445181-4-06 , contact details:info@bonitasit.hu), which, in its capacity as a data controller, provides comprehensive application management, application development, infrastructure management, IT consulting and services, as well as IT security services.
Third-country data transfers:	Data is transferred to **DigitalOcean LLC**, a virtual server provider acting as a data processor (as described in section 2).
Automated decision-making, profiling:	Automated decision-making, profiling does not take place.
Is the provision of data mandatory:	To reserve a venue at the BEK Academy via the website or request a quote online, you must provide your personal information.
What are the consequences if the data subject does not provide their personal data:	In the absence of this information, online reservations for the BEK Academy venue cannot be processed, as it is impossible to verify whether the time slot is available or to record who is making the reservation and to whom the offer should be sent.

19. ACCEPTING JOB APPLICATIONS

The data controller also welcomes job applications via the email address **hr@bhc.hu** when a position is advertised. It is also possible that a data controller may be contacted regarding a job application even if no position has been advertised. Considering this, we outline the related data management procedures below:

The aim of data management	**Filling vacant positions; identifying and selecting suitable candidates; assessing competencies; handling unsolicited job applications.**
The legal basis for data management:	The legal basis for data management is the performance of a contract pursuant to Article 6(1)(b) of the GDPR. This is because, under the GDPR, submitting a job application constitutes an offer to enter a contract. If an advertised position is filled, the legal basis for data processing regarding unsuccessful applications after the

	position has been filled—during the period for asserting claims under labour law or equal opportunity law—is the legitimate interest of the data controller pursuant to Article 6(1)(f) of the GDPR.
Description of the legitimate interest:	The reason behind data processing based on legitimate interests is that the applicant may assert a legal claim against the employer (or the parties may assert claims against each other) (e.g., why the applicant was not hired). The legitimate interest of the employer, as the data controller—which also coincides with the interests of the data subject—is to properly clarify the facts of the case, uncover evidence (i.e., establish provability), identify any potential violations of the law, and ensure that appropriate legal consequences can be applied. Applicants can expect their data to be processed (the parties should be aware of the possibility of asserting civil claims, and the privacy notice available on the website provides details on this); furthermore, the availability of application documents will assist applicants in asserting their legal claims. Both the data controller and the data subject therefore have a significant interest in clarifying the facts of the case. During the period in which legal claims are being pursued, the data controller will not process personal data in any other way and will store the applications separately from other personal data.
Categories of data subjects:	Natural persons who submit job applications to the data controller via the email address hr@bhc.hu are considered data subjects; that is, the data controller processes their personal data in the manner described herein.
Categories of personal data processed:	The data subject's name, contact information, education, qualifications, professional experience, and any other relevant personal data necessary for the fulfilment of the position. **Please DO NOT SUBMIT photocopies of documents or photographs as part of your application.** If the data controller receives such personal data, it shall be deleted in electronic form, and any documents held in paper form will be disposed. If this is not possible, the application will be returned and deemed invalid.
Source of personal data:	The data subject provides the personal data themselves and is therefore considered the source of the personal data.
The duration of data management:	If the data controller has published a job posting, the data controller will retain personal data in the event of an unsuccessful job application until the last day of the 3rd year following notification of the outcome of the application process. This is the last day of the **statute of limitations for labour and equal opportunity law**. It then permanently deletes

	the data stored electronically and destroys the paper-based materials. If the data controller has not posted a job advertisement, but an interested party wishes to work for the data controller and therefore submits an application to the email address hr@bhc.hu, the data controller will retain the job application for **6 months**. If no vacancy arises during this period, the application materials will be deleted or destroyed. The application materials of successful applicants will become part of their employment records; they will receive a separate privacy notice regarding this data processing. **If the applicants submits their application to the email address hr@bhc.hu, which is not dedicated for this purpose, but to another email address of the data controller (which was not created for this purpose), we hereby inform you that the applications sent to the incorrect address will be deleted.**
Recipients (subjects of data transmission):	While performing its duties—strictly for the purposes specified—**Bonitás IT Limited Liability Company** may access personal data in its capacity as a data processor. (registered office 6725 Szeged, 18 Szabadkai Street, company registration number: Cg.06-09-012933., TAX id nr: 14445181-4-06, contact details: info@bonitasit.hu), which, in its capacity as a data controller, provides comprehensive application management, application development, infrastructure management, IT consulting and services, as well as IT security services.
Third-country data transfers:	Third-country data transfer do not take place.
Automated decision-making, profiling:	Automated decision-making or profiling does not take place.
Is the provision of data mandatory:	Data provision is not mandatory.
What are the consequences if the data subject does not provide their personal data:	The job application cannot be evaluated without the required information.

20. THE DATA CONTROLLER'S APPEARANCE ON SOCIAL MEDIA SITES

The data controller is present on **Facebook** and **LinkedIn**. The pages can be followed by any user, who can write recommendations, like individual posts, and comment on them. In some cases, registration on the social media site is required to use certain features. You can also send general messages through the pages. **Please do**

not send us job applications or medical records via social media sites; furthermore, it is also not possible to schedule an appointment for an examination through these channels.

If you use social media platforms, you should be aware that these platforms are themselves data controllers and apply their own data management rules.

Should you have any questions regarding these data processing activities, please feel free to contact us.

21. RELEVANT IMPORTANT LEGISLATION:

List of the most important laws and regulations referred to in this privacy notice:
-General Data Protection Regulation: Regulation (EU) 2016/679(**GDPR)**
CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information (Hereinafter referred to as the **Infotv.**)
-Act CLIV of 1997 on Health Care (hereinafter referred to as the "Health Care Act" or **Eütv.**)
Act XLVII of 1997 on the Processing and Protection of Health and Related Personal Data Hereinafter referred to as the Health Data Act, **Eüak**).

The following resources may help you better understand the rules:
-The resolutions of the Data Protection Working Party and the European Data Protection Board
-Resolutions, opinions, and case-by case decisions of the National Authority for Data Protection and Freedom of Information (NAIH, supervisory body)
-Decisions of the Court of Justice of the European Union

You can access current legislation free of charge in the National Legislation Database (www.njt.hu), and via the European Commission's website https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32016R0679&from=HU)

22. OVERVIEW OF DATA SUBJECT RIGHTS

Data subjects have several rights in connection with data processing. We present these rights below:

The data subject's rights regarding data processed on the legal basis of compliance with a legal obligation are as follows:

The data subject's rights include the right to be informed ,|273ΠΤΙΘΜΜΜΜΘΙΤΠ274|of the existence of data processing; the right to access the above information regarding data processing, |273ΠΤΙΘΜΜΜΜΘΙΤΠ274|the right to receive a copy of the personal data being processed;, |273ΠΤΙΘΜΜΜΜΘΙΤΠ274|the right to request the rectification of personal data concerning the data subject or the restriction of processing;,|273ΠΤΙΘΜΜΜΜΘΙΤΠ274|the right to lodge a complaint with the supervisory authority; and the right to appeal to the court.

The data subject's rights with respect to data processed on the basis of legitimate interests are as follows:

The data subject's rights include the right to be informed ,|281ΠΤΙΘΜΜΜΜΘΙΤΠ282|about the ongoing data processing; the right to access the above information regarding data processing|281ΠΤΙΘΜΜΜΜΘΙΤΠ282|; the right to receive a copy of the personal data being processed; |281ΠΤΙΘΜΜΜΜΘΙΤΠ282| the right to request the rectification, erasure, or restriction of processing of personal data concerning them|281ΠΤΙΘΜΜΜΜΘΙΤΠ282| the right to object to the processing of personal data|281ΠΤΙΘΜΜΜΜΘΙΤΠ282| the right to lodge a complaint with the supervisory authority; and the right to appeal to the court.

The data subject's rights regarding data processed on the legal basis of contract performance are as follows:

The data subject's rights include the right to be informed of the ongoing data processing|281ΠΤΙΘΜΜΜΜΘΙΤΠ282|; the right of access to the aforementioned information regarding data processing;|281ΠΤΙΘΜΜΜΜΘΙΤΠ282| the right to receive a copy of the personal data being processed;|281ΠΤΙΘΜΜΜΜΘΙΤΠ282| the right to data portability (in the case of data processed in a non-paper format); the right to request the rectification of personal data concerning the data subject and the restriction of processing;|281ΠΤΙΘΜΜΜΜΘΙΤΠ282|the right to lodge a complaint with the supervisory authority; the right to appeal to the court.

The data subject's rights regarding data processed on the legal basis of consent are as follows:

The data subject's rights include the right to be informed of the ongoing data processing|281ΠΤΙΘΜΜΜΜΘΙΤΠ282|; the right of access to the aforementioned information regarding data processing;|281ΠΤΙΘΜΜΜΜΘΙΤΠ282| the right to receive a copy of the personal data being processed;|281ΠΤΙΘΜΜΜΜΘΙΤΠ282| the right to data portability (in the case of data processed in a non-paper format); the right to request the rectification, erasure, or restriction of processing of personal data concerning the data subject; ;|281ΠΤΙΘΜΜΜΜΘΙΤΠ282|the right to lodge a complaint with the supervisory authority; and the right to appeal to court.
You may withdraw your consent at any time.

Explanation of the data subject's rights listed above:

Right to information:
You may request information from the data controller regarding the processing of your personal data.

The data controller is required to provide you with all information regarding the processing of your personal data in a concise, transparent, comprehensible and easily accessible form, using clear and plain language.

The data controller shall provide the information in writing without delay, but no later than one month after receiving the request. At the request of the data subject, information may also be provided verbally, provided that the data subject has previously verified his or her identity in a credible manner.

If the application is complex and involves a large number of items, the one-month deadline may be extended by additional two months. The data controller shall inform the data subject of the extension of the deadline within one month of receiving the request, specifying the reasons for the delay. If the data subject submitted the request electronically, the information shall be provided electronically where possible, unless the data subject requests otherwise.

If the data controller does not take action in response to the data subject's request, it shall inform the data subject without delay, and in any event within one month of receiving the request, of the reasons for not taking action, as well as of the data subject's right to lodge a complaint with a supervisory authority and to appeal to the court.

The right of access to personal data and information regarding data processing:
The data subject has the right to obtain confirmation from the data controller as to whether their personal data is being processed, and if such processing is taking place, they have the right to access their personal data and the following information:

a) the aim of data management
b) categories of personal data processed:
c) the recipients, or categories of those recipients to whom the personal data have been or will be disclosed;
d) the planned duration of the storage of personal data, or the criteria used to determine that duration;
e) informing the data subject that he or she may request the data controller to rectify, erase, or restrict the processing of personal data concerning him or her, and may object to the processing of such personal data;
f) the right to lodge a complaint with the supervisory authority (which is the NAIH);
g) if the data were not collected from the data subject, any available information regarding their source;
h) whether automated decision-making (including profiling) takes place at the data controller, and if so, in which areas, what logic is applied, what significance such data processing has, and what consequences it is likely to have for the data subject.

Right to receive a copy:
The data controller shall provide the data subject with a copy of the personal data being processed upon the data subject's request. **For any additional copies requested by the data subject, the data controller may charge a reasonable fee based on administrative costs.** If the data subject submitted the request electronically, the information must be provided in a commonly used electronic form, unless the data subject requests otherwise.

However, the right to request a copy is subject to the limitation that it must not adversely affect the rights and freedoms of others.

The right to data portability:
The data subject has the right to receive the personal data concerning him or her, which he or she has provided to the controller, in a structured, commonly used, and machine-readable format, and has the right to transmit those data to another controller without hindrance from the controller; provided that the legal basis for the processing is the data subject's consent, or explicit consent, or the performance of a contract; and provided that the processing is carried out by automated means.

If the above conditions are met, the data subject has the right—where technically feasible—to request the direct transfer of their personal data between data controllers.

However, the right to data portability is subject to the limitation that it must not adversely affect the rights and freedoms of others.

Right to rectification:
The data subject has the right to request that the data controller rectify inaccurate personal data concerning him or her without undue delay, or to have incomplete personal data completed—including, for example, by means of a supplementary statement.

Right to erasure:
The data subject has the right to request that the data controller erase personal data concerning him or her without undue delay, and the data controller is obliged to erase personal data concerning the data subject without undue delay if any of the following reasons apply:
a) the personal data is no longer necessary for the purposes for which it was collected or otherwise processed;
b) the data subject withdraws the consent (or explicit consent) on which the data processing is based, and there is no other legal basis for the data processing;

c) the data subject objects to the processing of their data on grounds of public interest or legitimate interest, and there is no overriding legitimate ground for the processing, or the data subject objects to the processing of their data for direct marketing purposes;
d) the data controller processed the personal data unlawfully;
e) Personal data must be erased to comply with a legal obligation under Union or Member State law to which the data controller is subjected.

If the data controller has made the personal data public and is required to erase it, the data controller shall take all reasonable steps, taking into account available technology and the cost of implementation — including technical measures — to inform other data controllers processing the data that the data subject has requested the deletion of links to the personal data in question or of copies or duplicates of such personal data.
The erasure of data cannot be requested if the data processing is necessary:
a) for the exercise of the right to freedom of expression and the right to information;
b) for compliance with a legal obligation under EU or member state law to which the controller is subjected, or for the implementation of a task carried out in the public interest or in the exercise of official authority assigned to the data controller;
c) based on public interest in the field of public health;
d) for public archiving purposes, scientific or historical research purposes, or statistical purposes, if the right to data erasure would likely make this data processing impossible or would seriously impede it, or
e) to assert, enforce, and defend legal claims.

The right to restrict data management:
The data subject has the right to request that the data controller restrict the processing of their data if any of the following conditions are met:
a) the data subject disputes the accuracy of the personal data; in such cases, the restriction applies for a period enabling the controller to verify the accuracy of the personal data;
b) the data processing is unlawful, but the data subject objects to the erasure of the data and instead, requests that its use be restricted;
c) the data controller no longer needs the personal data for the purposes of data processing, but the data subject requires them for the establishment, exercise, or defense of legal claims; or
d) the data subject has objected to the processing; in this case, the restriction applies for as long as it has not been determined whether the objection is lawful, valid.

If the processing of personal data is restricted - with the exception of storage - such personal data may be processed only with the data subject's consent, or for the purpose of establishing, exercising, or defending legal claims, or for the protection of the rights of another natural or legal person, or for reasons of substantial public interest of the Union or of a Member State.

The data controller is required to notify the data subject in advance if it lifts the restriction on data processing.

The right to object to data processing:
The data subject has the right to object at any time, on grounds relating to their particular situation, to the processing of their personal data based on legitimate interests.

In that case, the data controller may no longer process the personal data unless it demonstrates compelling legitimate grounds for the processing which override the interests, rights, and freedoms of the data subject, or which are related to the establishment, exercise, or defense of asserting legal claims.

Right to file a complaint:
The data subject has the right to lodge a complaint with the supervisory authority if any of the above rights are infringed.

The supervisory authority is the **National Authority for Data Protection and Freedom of Information** (mailing address: 1055 Budapest,9-11 Falk Miksa street 9-11., 1363 Budapest, Post office box: 9., telephone: +36 (30) 683-5969, +36 (30) 549 6838, email: ugyfelszolgalat@naih.hu, website: www.naih.hu), where you can file a complaint or initiate an investigation by reporting that your rights have been infringed or are at immediate risk of infringement in connection with the processing of your personal data, or in the event of a violation of your rights.

Please be advised that if your personal data has been processed in a manner that infringes upon your rights, or if there is an imminent risk of such an infringement, you may also bring a claim directly before a court.

You may also submit your comments, questions, or complaints to the **Data Protection Officer.**

23. HOW WE PROTECT YOUR PERSONAL DATA

The data controller shall take into account the state of science and technology, the costs of implementation, as well as the nature, scope, context, and purposes of the data processing, taking into account risks of varying likelihood and severity, implements appropriate technical and organizational measures to ensure a level of data security appropriate to the risk, including, among other things, where applicable:

a) the pseudonymization and encryption of personal data;
b) ensuring the ongoing confidentiality, integrity, availability, and resilience of the systems and services used to process personal data;
c) in the event of a physical or technical incident, the ability to restore access to personal data and ensure the availability of such data in a timely manner;
d) a procedure for regularly testing, assessing, and evaluating the effectiveness of the technical and organizational measures taken to ensure the security of data processing.

The data controller has information security policy in force.

We always ensure that your personal data is accessible only to those individuals who need access to it to provide healthcare services.

24. DEFINITIONS

The purpose of these definitions is to clarify who is subject to the regulations and exactly what the regulatory framework means by each term. **The following section introduces the most important concepts:**

"**Personal data**": any information relating to an identified or identifiable natural person ("data subject"); "identifiable" means a natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. **All data we record in connection with our patients is considered personal data.**

"**Health data**": personal data relating to the physical or mental health of a natural person, including data relating to the provision of health services to that natural person that contains information about the natural person's health.

"**Genetic data**": any personal data relating to the inherited or acquired genetic characteristics of a natural person that provides unique information about the physiology or health of that person and that is derived primarily from the analysis of a biological sample taken from that natural person.

"**Biometric data**": any personal data relating to the physical, physiological, or behavioural characteristics of a natural person, obtained through specific technical procedures, which enables or confirms the unique identification of that natural person, such as a facial image or dactyloscopic data;

"**Data processing**": **any operation or set of operations** performed on personal data or on sets of personal data, whether or not by automated means, including collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, preview, use, disclosure by transmission, distribution or making accessible by other means, alignment or combination, restriction, erasure, or destruction.

"**Restriction of data processing**": marking stored personal data to restrict their future processing.

"**Controller**": a natural or legal person, public authority, agency, or any other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by EU or member state law, EU or member state law may also specify the data controller or specific criteria for designating the data controller **The data controller in this case is Buda Health Center. In the case of data transfers, the recipient may be classified as a data controller or a data processor.**

"**Data processor**": a natural or legal person, public authority, agency, or any other body that processes personal data on behalf of the data controller.

"**Recipient**": a natural or legal person, public authority, agency, or any other body to whom or which personal data is disclosed, whether or not that body is a third party.

"**Third party**": a natural or legal person, public authority, agency, or any other body that is not the data subject, the data controller, the data processor, or any person authorized to process personal data under the direct authority of the data controller or data processor.

"**Profiling**": any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to assess workplace performance, economic situation, health, personal preferences, interests, reliability, behaviour, location, or movement.

"**Pseudonymization**": the processing of personal data in such a manner that the personal data can no longer be attributed to a specific natural person without the use of additional information, provided that such additional information is kept separately and technical and organizational measures are implemented to ensure that the personal data cannot be linked to identified or identifiable natural persons.

"**Filing system**": a collection of personal data organized in any way—whether centralized, decentralized, or structured according to functional or geographical criteria—that is accessible based on specific criteria.

"**Consent of the data subject**": a freely given, specific, informed, and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

"**Data breach**": a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or unauthorized access to, personal data transmitted, stored, or otherwise processed.

"**Enterprise**": a natural or legal person engaged in economic activity, regardless of its legal form, including partnerships and associations engaged in regular economic activity.

"**Supervisory authority**": an independent public authority established by a Member State in accordance with Article 51. In this case, the supervisory authority is the National Authority for Data Protection and Freedom of Information (1363 Budapest, Post Office Box 9, ugyfelszolgalat@naih.hu).

25. PRINCIPALS OF PRIVACY POLICY

The processing of personal data must be carried out in accordance with the following principles, and the data controller processes data in this manner:

(a) Data processing must be carried out lawfully, fairly, and in a transparent manner in relation to the data subject ("**lawfulness, fairness, and transparency**");

(b) data shall be collected only for specified, explicit, and legitimate purposes and shall not be processed in a manner incompatible with those purposes ("**purpose limitation**");

c) data must be appropriate and relevant to the purposes of the data processing and must be limited to what is necessary ("**data minimization**");

(d) They must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes of the processing, are erased or rectified without delay ("**accuracy**");

(e) storage must be implemented in a form that allows for the identification of data subjects only for as long as is necessary to achieve the purposes of the processing. Personal data may be stored for a longer period only if the processing of such data is carried out for the purpose of public archiving pursuant to Article 89(1), for scientific or historical research purposes or for statistical purposes, subject to the implementation of appropriate technical and organizational measures required by this Regulation to safeguard the rights and freedoms of data subjects ("**limited storage**")

(f) Processing must be carried out in such a manner that appropriate technical or organizational measures ensure the security of personal data, including protection against unauthorized or unlawful processing, accidental loss, destruction, or damage ("**integrity and confidentiality**").

The data controller is responsible for ensuring compliance with the above provisions and must be able to prove such compliance ("**accountability**").