

PRIVACY NOTICE

**FIRSTMED-FMC EGÉSZSÉGÜGYI
SZOLGÁLTATÓ KORLÁTOLT FELELŐSSÉGŰ TÁRSASÁG**

I. Introduction, principles, purpose and scope of this Privacy Notice

Firstmed-FMC Egészségügyi Szolgáltató Korlátolt Felelősségű Társaság, as the Data Controller (hereinafter referred to as: **Data Controller**) acts in accordance with the provisions of Regulation (EU) No 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter referred to as: **Regulation** or **GDPR**) and applicable laws in the course of its data processing activities.

The Data Controller respects the rights of the **Data Subject** to the protection of his or her personal data. This Privacy Notice summarises the data collected by the Data Controller and how such data may be used, the tools used by the Data Controller as well as the Data Subject's options for data protection and remedies available in a clear and straightforward manner.

Detailed rules are laid down in the aforementioned Regulation and related legal acts. Should you require further information, do not hesitate to consult the Regulation or contact the Data Controller at the contact details provided herein.

This Privacy Notice is intended to ensure that the Data Controller complies with the constitutional principles of data protection and the requirements of data security, and to prevent unauthorised access to, alteration, loss or disclosure of data.

The Data Controller shall act in accordance with the following principles in the course of its data processing activities:

The Data Controller shall inform the Data Subject of the data processing rules before the commencement of processing in a timely and required manner.

The Data Controller collects, retains and uses personal data solely for a defined purpose, in accordance with the requirements of purpose limitation.

Personal data collected shall always be suitable, relevant and adequate for the purpose it is collected for, and the Data Controller shall comply with the principle of data minimisation by abiding by this rule.

For the purposes of accuracy of personal data, the Data Controller shall take reasonable measures based on the particular purpose in order to ensure that the personal data of the Data Subject are complete, accurate, up to date and reliable to the extent required for that specific purpose.

The Data Controller shall be entitled to use personal data for marketing purposes solely with the consent of the Data Subject and the Data Subject shall have the opportunity to opt out of such marketing communication.

The Data Controller shall take proportionate and comprehensive measures in order to ensure the protection of the personal data of the Data Subject as detailed herein, including in cases, where personal data is transferred to third parties.

The scope of this Privacy Notice applies to the overall data processing activities of the Data Controller, in particular, but not limited to, the processing of personal data of contact persons of economic and other organisations as well as partner institutions, and other natural persons as Data Subjects, prospective employees (jobseekers/candidates) of the Data Controller, the use of the website(s) and applicable data security principles.

II. Explanatory notes

- **Regulation, GDPR Regulation:** Regulation (EU) No 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data;
- **Privacy Act:** Act CXII of 2011 on Information Self-Determination and Freedom of Information
- **Security Services Act:** Act CXXXIII of 2005 on the rules of Private Security and Private Investigation Activities;
- **Taxation Act:** Act CL of 2017 on the Rules of Taxation;
- **Accounting Act:** Act C of 2000 on Accounting;
- **VAT Act:** Act CXXVII of 2007 on Value Added Tax;
- **Civil Code:** Act V of 2013 on the Civil Code of Hungary;
- **Healthcare Act:** Act CLIV of 1997 on Healthcare
- **Healthcare Data Act:** Act XLVII of 1997 on the Processing and Protection of Healthcare and Related Personal Data
- **Personal data** means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one 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;
- **Special categories of personal data** means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and data concerning health, addictions, criminal record or a natural person's sex life or sexual orientation.
- **Genetic data** means personal data relating to the inherited or acquired genetic characteristics of a natural person that give unique information about the physiology or health of that natural person and is primarily derived from the analysis of a biological sample gathered from such natural person.
- **Biometric data** means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.
- **Data concerning health** means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about the health status of the natural person.
- **Processing of data** means any operation or set of operations, which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- **Data controller** means the natural or legal person, public authority, agency or 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 such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.
- **Processor** means a natural or legal person, public authority, agency or other body, which processes personal data on behalf of the controller.
- **Registration of data processing activities:** pursuant to the obligation laid down in Article 30, paragraph (1) of the GDPR, a register on the processing activities performed by the Data Controller, which register shall contain, in addition to the data concerning the Data Controller, the description of the data processing, the purposes of data processing, the categories of data subjects, the categories of personal data processed, where possible, the recipients to whom the data will be disclosed, the name and

contact details of the data processor(s) and, where possible, the deadline envisaged for the erasure of each category of personal data.

- **Recipient** means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. Public authorities that may access personal data for specific investigations in accordance with EU or Member State law are not considered to be recipients.
- **Third party** means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.
- **Consent of the data subject** means any 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.
- **Profiling** means 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 analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
- **Personal data breach may include:** IT error, personal data breach.
- **IT error** means a disruption or slowdown of an IT system that hinders work, causes abnormal operation and service failure, which does not constitute a data breach but may compromise the confidential nature, integrity or availability of the IT system.
- **Personal data breach** means a breach of security that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transferred, stored or otherwise processed.
- **Data Protection Officer:** The person appointed by the company pursuant to Article 37, paragraph (1), item (a) of Regulation (EU) 2016/679 of the European Parliament and of the Council (GDPR), whose contact details and legal status are contained in this Privacy Notice.
- **Authority:** Hungarian National Authority for Data Protection and Freedom of Information www.naih.hu

III. Data and contact details of the Data Controller (service provider)

Name of the Data Controller: **Firstmed-FMC Egészségügyi Szolgáltató Korlátolt Felelősségű Társaság**

Registered seat: H-1015 Budapest, Hattyú utca 14.

Mailing address: H-1015 Budapest, Hattyú utca 14.

Company registration number: 01-09-958986

Data Protection Officer: Ildikó Diokno

Call center (telephone): +36 1 224 9090

Call center (fax): +36 1 224 9091

Call center e-mail address: info@firstmedcenters.com

Venue of complaints management: H-1015 Budapest, Hattyú u. 14. V. emelet

IV. Purpose of data processing, scope of data processed, duration of data processing, people entitled to access data concerning data subjects who use the services provided by the Data Controller.

1. Purpose of and legal basis for processing of personal data

The personal data referred to in this Chapter are processed by the Data Controller in the course of its operations for legitimate interests, for the conclusion and performance of a contract, for the fulfilment of its obligations under the law and on the basis of the explicit and voluntary consent provided by the Data Subject.

The Data Controller processes personal data for the purposes of conclusion and performance of a contract (to which the Data Subject is a party), for legitimate interests pursued by the Controller and on the basis of an explicit consent provided by the Data Subject (Article 6, paragraph (1), item b), f) and Article 9, paragraph (2), item a) of the GDPR) in the following cases: the intention to conclude a contract, performance of a contract. Provision of healthcare services, conclusion, amendment and termination of relevant contracts, performance of contractual obligations, enforcement of rights and potential claims, defence against claims as well as liaison; identification of the Data Subject; assistance in the performance of effective medical treatment; supervision of the Data Subject's state of health; taking measures necessary in the interests of public health, national health and epidemiology; provision of funding for healthcare services; enforcement of patients' rights, transmission of medical records. Security function: surveillance of the headquarters/premises, answering general inquiries.

In case of occupational health examinations or treatments, the legal basis for the processing may vary, whether the Data Subject is visiting for a fitness for work assessment or, in case of an accident at work, whether the Data Subject has a capacity to act or is not in a position to provide consent:

- fitness for work assessment: compliance with a statutory obligation (pursuant to Section 4 of Decree No 33/1998 of the Ministry of Welfare, the occupational physician performs a preliminary assessment of the fitness for work), the assessment of the employee's fitness for work for occupational health purposes, the establishment of a medical diagnosis, the provision of health or social care or treatment under a contract concluded with a healthcare professional [Article 6, paragraph (1), item c) and Article 9, paragraph (2), item h) of the GDPR];
- accident at work, if the data subject has a capacity to act: compliance with a statutory obligation (pursuant to Section 64, paragraph (4) of Act XCIII of 1993, a physician who provides basic occupational health services shall be informed of an accident at work and the physician shall decide whether to be involved or not, except in severe accidents at work, where his/her involvement is mandatory), assessment of the employee's fitness for work, establishment of a medical diagnosis, provision of health or social care or treatment for occupational health purposes [Article 6, paragraph (1), item (c) and Article 9, paragraph (2), item h) of the GDPR];
- accident at work, if the data subject has no capacity to act: your vital interest in compliance with a statutory obligation (pursuant to Section 64, paragraph (4) of Act XCIII of 1993, a physician who provides basic occupational health services shall be informed of an accident at work and the physician shall decide whether to be involved or not, except in severe accidents at work, where his or her involvement is mandatory) [Article 6, paragraph (1), item (c) and Article 9, paragraph (2), item h) of the GDPR];
- Occupational disease: compliance with a statutory obligation (pursuant to Section 64 of Act XCIII of 1993 as well as Section 5, paragraph (1) and (2) of Decree No. 27/1996 (28 August) of the Ministry of Welfare on the Reporting and Investigation of Occupational Diseases and Cases of Increased or High Exposure, the assessment of the employee's fitness for work for occupational health purposes, the establishment of a medical diagnosis, the provision of health or social care or

treatment under a contract concluded with a healthcare professional [Article 6, paragraph (1), item c) and Article 9, paragraph (2), item h) of the GDPR]. The legal basis for data processing in case of invasive procedures or surgery is the performance of a healthcare contract concluded with you, the provision of healthcare or treatment under a contract with a healthcare professional [Article 6, paragraph (1), item b) and Article 9, paragraph (2), item h) of the GDPR], or in case of life-saving procedures, your vital interest [Article 6, paragraph (1), item d) and Article 9, paragraph (2), item c) of the GDPR].

The Data Controller processes personal data in order to comply with its legal obligations, based on provisions of law in the following cases: compliance with invoicing, accounting, bookkeeping obligations (Accounting Act, VAT Act, Taxation Act), compliance with healthcare records retention obligations - compliance with its obligation pursuant to Section 30 of Act XLVII of 1997 on the Processing and Protection of Healthcare and Related Personal Data, compliance with its obligation to keep healthcare records pursuant to Sections 136 and 137 of Act CLIV of 1997 on Healthcare, Complaint management (Act CLV of 1997 on Consumer Protection), Transfer of data concerning health to the operator of the National eHealth Infrastructure (NHSC) pursuant to Act XLVII of 1997 on the Processing and Protection of Healthcare and Related Personal Data.

The Data Controller processes personal data on the basis of the explicit and voluntary consent of the Data Subject in the following cases: to retain records of previous treatment, to take pictures of the treatment area and use them for scientific or educational purposes, or to send a treatment reminder.

Legal bases for processing special categories of personal data pursuant to Article 9, paragraph (2) of the GDPR:

- the data subject has given explicit consent to the processing of such personal data for one or more specified purposes;
- processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law;
- processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
- processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
- processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law;
- processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services;
- processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices.

2. Scope of data processed, duration of data processing, persons entitled to access personal data

The Data Controller collects and processes personal data referring to the legal basis specified in the table(s) below for the specified retention period:

	Personal data	Retention/Storage period
<p>The conclusion and performance of a contract and personal data processed on the basis of a legitimate interest or the explicit consent of the data subject</p>	<p>name, name at birth, address, place and date of birth, mother's name at birth, gender of the data subject, telephone number, e-mail address, personal data of a minor's guardian (name, telephone number, e-mail address).</p>	<p>5 years after performance of the contract and/or cessation of legitimate interest.</p>
	<p>insurance details, health insurance membership details, bank account details.</p>	
	<p>SSN</p>	
	<p>Data concerning health: Disease details, medical history, recommended/provided treatment, ultrasound and colposcope, X-ray and mammography results, other laboratory test results; diseases which do not directly justify treatment and potential risk factors; overweight status, if applicable; medical data, which has an impact on the performance of the examination; information on previous examinations, previous medical interventions; current symptoms; other data necessary for the performance of treatment, information obtained in the course of the examination.</p>	
	<p>Personal data contained in general inquiries (all personal data provided by the Data Subject to the Data Controller)</p>	

	Personal data	Retention/Storage period
	<p>Data contained in accounting documents</p>	<p>Retention period: as specified in relevant laws (Taxation Act, Accounting Act, VAT Act)</p>
	<p>Healthcare documentation</p>	<p>Retention period: as specified in relevant law - Act XLVII of 1997 on the Processing and Protection of Healthcare and</p>

Data processed under the provisions of law		Related Personal Data (10, 30 and 50 years respectively)
	Transfer of data concerning health to the operator of the National eHealth Infrastructure (NHSC)	pursuant to Act XLVII of 1997 on the Processing and Protection of Healthcare and Related Personal Data
	Compliance with the legal obligation specified in Act CLIV of 1997 on Health Care concerning management of complaints	Pursuant to Act CLIV of 1997 on Healthcare, the period of data processing shall be 5 years upon the closure of the complaint, and data will be erased or destroyed thereafter.

Data processed based on the voluntary consent of the data subject	Personal data	Retention/Storage period
	Name, e-mail address, telephone number Photo/video recording of the treatment area Information on previous treatments	Retention period until consent is withdrawn

Data relating to Data Subjects may be accessed by the Data Controller as follows:

- directly or indirectly from Data Subjects, in line with the provisions of this Privacy Notice
- upon receipt of data from other data controllers;
- from public sources.

The Company shall ensure that data is stored securely in all cases in accordance with the provisions of law, in compliance with the rules and by implementing appropriate technical and organisational measures. The Company shall make the source of data available to the Data Subject.

3. The Data Controller engages the Data Processor(s) listed in Annex 1 attached hereto for the activities specified therein.

Persons entitled to have access to the data: The Data Controller may transfer personal data to its employees and agents engaged in customer service and its other activities, as well as to its employees and data processors as recipients engaged in accounting and taxation tasks. In case of an official inquiry by an investigating authority or other authority in the course of an administrative procedure, the Company shall disclose the requested data in accordance with the provisions of applicable law.

The data subject acknowledges that, pursuant to a health insurance or other contract concluded by and between him or her as a contracting party and an institute (third party, insurance company) which funds healthcare in whole or in part, his or her personal data (personal identification data, data on the service provided: treatment data, diagnosis data, payment data) may be transferred to such third party/insurance company to the extent required and in accordance with the contract concluded by and between the data subject and the insurance company in order to settle the funding of the service used. The services cannot be used without the transfer of such data under an “insurance” scheme. If consent of the Data Subject is required, it is provided by using the service with the funding of an insurance company, by explicitly

requesting the transfer of data or by giving his/her separate consent thereto on the registration form of the Data Controller. The Data Controller shall not be liable for the processing of personal data by the insurance company (third party). The insurance company/third party shall be considered to be an independent data controller in this regard.

Method of storage of personal data: in both electronic and hardcopy formats

V. Purpose of data processing, scope of data processed, duration of data processing, people entitled to access data in case of business partners, agents, and other persons in an employment-like relationship (e.g. sole entrepreneur, etc.), as well as contact persons and employees of business organisations, who come into contact with the Data Controller in the course of its economic (business) activities, as data subjects

1. Purpose of and legal basis for processing of personal data

The Data Controller processes personal data for legitimate interests in the following cases: the intention to conclude a contract, the conclusion and performance of a contract.

The Data Controller processes personal data in order to comply with its legal obligations, based on provisions of law in the following cases: compliance with invoicing, accounting, bookkeeping obligations (Accounting Act, VAT Act, Taxation Act).

Personal data is processed by the Data Controller based on the explicit and voluntary consent of the Data Subject in the following cases: sending out newsletters for promotional and marketing purposes.

2. Scope of data processed, duration of data processing, persons entitled to access personal data

The Data Controller collects and processes personal data referring to the legal basis specified in the table(s) below for the specified retention period based on the classification of Data Subjects:

	Personal data	Retention/Storage period
Data processed on the basis of legitimate interest	<p>Name, e-mail address, telephone number</p> <p>For contact persons of business partners: including the position held in the partner company</p> <p>In addition, in case of Agents and other data subjects who work directly for the Data Controller, but are not employees, depending on their capacity as data subjects: citizenship, place and date of birth, address (registered seat), VAT number, CV, expertise, studies/training, language skills, photo, tax identification number, personal identification number, bank account number, chamber identification number, if applicable, sole entrepreneur registration number.</p>	Retention period shall be 5 years from the date of contractual performance or termination of the contract or cessation of the legitimate interest in accordance with the relevant provision of law (Section 6:22 of the Civil Code)

Data processed under the provisions of law	Personal data	Retention/Storage period
	Data indicated on accounting documents: Name, position held, e-mail address, telephone number.	Minimum 8 years pursuant to Section 169, paragraph (2) of the Accounting Act

Data processed based on the voluntary consent of the data subject	Personal data	Retention/Storage period
	Name, e-mail address, telephone number, in case of contact persons: position held at the business partner's company	Retention period until unsubscription or until consent is withdrawn

The Data Controller engages the Data Processor(s) listed in Annex 1 attached hereto for the activities specified therein.

Persons entitled to have access to the data: The Data Controller may transfer personal data to its employees engaged in customer service and its other activities, as well as to its employees and data processors as recipients engaged in accounting and taxation tasks.

Data relating to Data Subjects may be accessed by the Data Controller as follows:

- directly or indirectly from Data Subjects, in line with the provisions of this Privacy Notice
- upon receipt of data from other data controllers;
- from public sources.

The Company shall ensure that data is stored securely in all cases in accordance with the provisions of law, in compliance with the rules and by implementing appropriate technical and organisational measures. The Company shall make the source of data available to the Data Subject.

Method of storage of personal data: in both electronic and hardcopy formats.

VI. Purpose of data processing, scope of data processed, duration of data processing, people entitled to access data concerning data subjects who contact/submit their application to the Data Controller as jobseekers.

1. Purpose of and legal basis for processing of personal data

Personal data is processed by the Data Controller based on the explicit and voluntary consent of the Data Subject in the following cases: Recruitment, conducting the recruitment/selection process.

2. Scope of data processed, duration of data processing, persons entitled to access personal data

The Data Controller collects and processes personal data referring to the legal basis specified in the table(s) below for the specified retention period:

	Personal data	Retention/Storage period
Data processed based on the voluntary consent of the data subject	name, e-mail address, telephone number, CV, certificates and diplomas.	Until consent is withdrawn or, in the absence of a consent, until the position is filled, but in any case not longer than 1 month.

3. The Data Controller engages the Data Processor(s) listed in Annex 1 attached hereto for the activities specified therein.

Personal data is transferred by the Data Controller to its employees who perform tasks related to security access, customer service, as well as to the employees who manage the competent field of its activity, as well as to data processors as recipients.

Data relating to Data Subjects may be accessed by the Data Controller as follows:

- directly or indirectly from Data Subjects, in line with the provisions of this Privacy Notice

The Company shall ensure that data is stored securely in all cases in accordance with the provisions of law, in compliance with the rules and by implementing appropriate technical and organisational measures. The Company shall make the source of data available to the Data Subject.

Method of storage of personal data: in both electronic and hardcopy formats

VII. Use of www.firstmed.hu and www.firstmedcenters.com

The Data Controller stipulates that the collection and processing of personal data of visitors to the website is performed (in the absence of an online contact) on the website by the use of anonymous User identifiers (cookies) and their acceptance by the Data Subject. The essential features of cookies are summarised below by the Data Controller.

The Data Controller shall be entitled to use alphanumeric information packages, i.e. cookies with variable content via its web server for the purposes of rendering services and using the website. Such cookies are stored on the user's computer for a predetermined period of time and are sent by the web server.

A cookie is a designator that allows identification and storage of profile information and is placed on the Data Subject's computer by service providers. Please note that a designator is not suitable in itself to identify the Data Subject in any manner whatsoever, it is only suitable to identify the computer of the Data Subject. Personalised information and customised services cannot be provided in the world of Internet unless service providers can identify the unique behaviours and needs of their customers. Therefore, service providers use anonymous identification to obtain more information on their customers' information usage patterns in order to improve the quality of their services and to offer customisation options to their customers.

Cookies are used, for example, to store the preferences and settings of Data Subjects; these support log in; may display personalised ads and analyse the operation of the website. Therefore, the Data Controller may use services to collect and track data on the activities of the Data Subject such as relevance, referrals, searches, visits, most important and frequently used features.

Flash cookies are used by website operators to, for example, tell you whether you have ever visited a website before or to help you identify the features/services that may be most interesting to you. Search and Flash cookies enhance the browsing experience by retaining the information preferred by the Data Subject while browsing a particular site. Neither the search engine nor Flash cookies are suitable to personally identify the Data Subject, and the Data Subject may reject browser cookies in the browser settings, however, he or she will not be able to use all the services offered by the website without enabling such cookies.

Anonymous user IDs:

Cookie name	Purpose	Personal data concerned:	Legal basis of data processing	Expiry date
Strictly mandatory cookie	Allowed navigation	During the use of the website: the IP address of the Data Subject's computer; data related to his/her activity in connection with the website.	Consent of the data subject	After leaving the site. No personal data is stored.

Performance cookie	Collection of information about the use of the website (Google Analytics)	Collection of information about the use of the website Personal data of the Data Subject: While using the website: the IP address of the Data Subject's computer; the time spent on the website (start and end times); browser and operating system used depending on the settings of the Data Subject's computer; data concerning the Data Subject's activity on the website.	Consent of the data subject	Personal data is stored until the end of the session depending on the type of the particular cookie: 2 years/24 hours/1 minute/4 hours/ indefinitely
Targeting and advertising cookies	Create and store IDs, display targeted ads. (Google Analytics, Facebook pixels)	IP address of the Data Subject's device	Consent of the data subject	Personal data is stored until the end of the session depending on the type of the particular cookie: 1 day/1 month/6 months/2 years

If the Data Subject prefers not to have such identifiers placed on his/her computer, he or she can configure his or her browser settings to disable the placement of unique identifiers and can withdraw his or her consent at any time, erase the unique identifier, however, in this case the services may not be available to the Data Subject at all or not in the form as if he or she had consented to the placement of identifiers.

Services are used by numerous users in varied software and hardware environments, with different purposes and fields of use. The development of services can be best adapted to the requirements and possibilities of users if the website operator has a comprehensive overview of their usage behaviours and needs. However, due to the large number of users, personal contact and feedback is not sufficient, the operator of the website shall also use effective automated complementary methods in order to collect and analyse user behaviour and operating environment.

Purpose of data processing: to ensure the intended and top-notch operation of the website, to monitor and improve the quality of the services provided by the Data Controller, to identify malicious visitors and hackers to the website and to compile statistics on the number of visitors.

Persons entitled to have access to the data: employees responsible for the monitoring and maintenance of the Data Controller's IT system and any potential data processors.

Method of storage of personal data: electronic, however, in case of a personal data breach, the data concerned by the personal data breach may also be stored in hardcopy format in accordance with the procedures specified in the company's Data Breach Management Policy.

VIII. Social media sites (Facebook, Instagram)

The User can subscribe to the news feed posted on the message board of the Facebook/Instagram account managed by the Data Controller by clicking the link (“like”; “follow”) on the particular page, and unsubscribe by clicking the link (“dislike”) on the same page, or erase unwanted news on the message board by using the settings thereof. The Data Controller has access to the profile of “followers”, but does not record or manage such profiles in its own internal system.

The purposes of data processing: Sharing content related to the services offered by the Data Controller, publication of other news, liaising. Facebook pages allow the Data Subject to gather information on the activities of and services provided by the Data Controller.

The legal basis for data processing is the voluntary consent of the Data Subject, which may be withdrawn at any time by unsubscribing. The withdrawal does not affect the lawful processing performed before the withdrawal. In the case of withdrawal of consent, the Data Subject will not be notified of posts displayed on the Data Controller's news feed, the posts of the Data Controller will not be displayed on the Data Subject's news feed, however, the Data Subject will be able to access the news feed since the website is public.

Data is processed until the Data Subject unsubscribes. No data is transferred and no data processors are engaged.

Facebook and Instagram are data controllers who are separate and independent from the Data Controller. For information about the data processing activities of the website, please consult the privacy policy and privacy notice published on the service providers' website:

1. <https://www.facebook.com/policies/cookies/>
2. <https://www.facebook.com/about/privacy/update>

Information on the data processing activities of Instagram are available at:

1. help.instagram.com

IX. Use of WiFi

Wifi is provided in exchange for the provision of your name and e-mail address at certain stores. In addition, the system also records the IP address of the Data Subject's device.

The purposes of data processing:

The purpose of data processing is to ensure access to the services via Wifi, and to manage complaints and to identify abuse once the Data Subject left.

Legal basis of data processing:

The legal basis for our data processing activities is “performance of a contract”, taking into consideration that providing access to Wifi is one of the services provided by the Data Controller. However, the legal basis of data processing is “the legitimate interest of the Data Controller in managing complaints and identifying abuse” after the Data Subject left. You need to provide your personal data for obtaining access to our services.

Period of data processing:

Your data will be erased in 1 (one) year after the current year.

X. Operation of an electronic surveillance camera system

1. Purpose of and legal basis for processing of personal data

The processing of the Data Subject's personal data on the basis of legitimate interest is performed for the purposes of maintaining the security of the Data Controller's headquarters/premises/other areas operated by the Data Controller, the protection of property, the protection of the life and physical integrity of the Data Controller's employees and visitors, and to investigate the circumstances of any potential extraordinary events.

The Data Controller shall perform its activities in compliance with the provisions of Act CXXXIII of 2005 on the rules of Private Security and Private Investigation Activities (Private Security Act).

The detailed rules for the use of the electronic surveillance camera system operated at the premises of the Data Controller are specified in the prevailing **Electronic Surveillance Camera Policy**, which is available at the Data Controller's registered seat.

The Data Controller processes personal data on the basis of legitimate interest.

The Data Controller operates a surveillance camera system.

2. Scope of data processed, duration of data processing, persons entitled to access personal data

The Data Controller collects and processes personal data referring to the legal basis specified in the table(s) below for the specified retention period:

Data processed on the basis of legitimate interest	Personal data	Retention/Storage period
	Picture of the Data Subject, data that can be obtained through the camera image	For the period of time (3 days) specified in the Data Controller's Electronic Surveillance Camera Policy

Method of storage of personal data: electronic

3. The Data Controller engages the Data Processor(s) listed in Annex 1 attached hereto for the activities specified therein.

The Data Controller will transfer personal data to the following recipients:

The data recorded may solely be accessed by employees of the Data Controller and designated employees of the data processor(s). Previously recorded footage from the electronic surveillance camera system may only be accessible to persons specified in the Electronic Surveillance Camera System Policy, to the extent and in the manner specified in the procedures contained therein.

Data relating to Data Subjects may be accessed by the Data Controller as follows:

- directly or indirectly from Data Subjects, in line with the provisions of this Privacy Policy

The Company shall ensure that data is stored securely in all cases in accordance with the provisions of law, in compliance with the rules and by implementing appropriate technical and organisational measures. The Company shall make the source of data available to the Data Subject.

Method of storage of personal data: electronic

XI. Data security

The Data Controller shall endeavour to ensure the security of the Data Subject's personal data in accordance with its obligations under Act CXII of 2011 on Information Self-Determination and Freedom of Information (hereinafter referred to as: Privacy Act) and the GDPR, and shall take the necessary technical and organisational measures and implement rules of procedure required to enforce the provisions of the Privacy Act, the GDPR and other data protection and confidentiality rules. Data stored in the database of the Data Controller may be accessed solely by the employees of the Data Controller with explicit authorisation to do so.

Data processing services related to the website also include so-called cloud-based applications. Cloud-based applications are usually international or cross-border in nature, and are used for data storage purposes, where data is not stored on the Data Controller's computer/corporate server, but on a server hub located anywhere in the world. The main advantage of cloud-based applications is that they provide highly secure, flexible and scalable IT storage and processing capacity independent of any geographic location.

The Data Controller exercises the utmost care in the selection of its cloud-based service providers, endeavours to contract them under terms and conditions that take into consideration the data security interests of the Data Subjects, ensure that their data processing principles are transparent to the Data Controller and regularly verifies data security.

The Data Controller's website may contain references or links to websites operated by other service providers (including login and share buttons and logos), and the Data Controller has no control over their practices with regard to the processing of personal data. The Data Controller draws the attention of the data subjects to the fact that if they click such links, they might be redirected to websites of other service providers. In such cases, we highly recommend that you read the privacy notice applicable to the use of such websites. This Privacy Notice applies solely to the processing performed by the Data Controller. Should any of your data be amended or erased by the Data Subject on the external website concerned, this will not impact the processing of your personal data by the Data Controller, who shall make such amendments on the website.

XII. Access to, amendment and rectification of personal data, data portability

1. Access

The data subject shall have the right to obtain from the data controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

- 1.1. purposes of data processing;
- 1.2. the categories of relevant personal data;
- 1.3. the recipients or categories of recipients to whom the personal data have been or will be disclosed.

2. Amendment and rectification

The data subject shall have the right to obtain from the data controller without undue delay the rectification of inaccurate personal data concerning him. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

3. Data portability

The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

- 3.1. processing is based on voluntary consent or on a contract to which the Data Subject is a party; and
- 3.2. processing is carried out by automated means.

XIII. Erasure of personal data, restriction of processing, right to object

1. Erasure

(1) The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

- a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- b) the data subject contacts the Call Center to withdraw his or her consent on which the processing was based and there is no other legal basis for the processing;
- c) the data subject objects to the processing on grounds related to his or her particular situation, or due to processing of personal data for the purpose of direct marketing and the Data Controller has no overriding legitimate grounds for the processing;
- d) the personal data has been unlawfully processed;
- e) the personal data has to be erased for compliance with a legal obligation set forth in Union or Member State law the data controller is subject to;
- f) personal data are collected in connection with the provision of information society services directly to children.

(2) Where the controller has made the personal data public and is obliged pursuant to the previous paragraph to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

(3) Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

- a) for exercising the right to freedom of expression and information;
- b) to comply with an obligation under Union or Member State law that requires the data controller to process personal data or to perform a task carried out in the public interest or while exercising public authority;
- c) due to reasons of public interest in the area of occupational health or public health;
- d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in so far as the right referred to in paragraph (1) is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
- e) to bring, enforce or defend legal claims.

2. Restriction

(1) The data subject shall have the right to obtain from the data controller restriction of processing where one of the following applies:

- a) the data subject disputes the accuracy of the personal data; in this case, the restriction concerns the period of time which is required by the data controller to verify the accuracy of the personal data;
- b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of data processing instead;
- c) the data controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims; or
- d) the data subject has objected to processing due to his particular situation, pending the verification whether the legitimate grounds of the controller override those of the data subject.

(2) Where processing has been restricted under paragraph (1), such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

(3) A data subject who has obtained restriction of processing pursuant to paragraph (1) shall be informed by the data controller before the restriction of processing is lifted.

3. **Objection**

The data subject shall have the right to object, on grounds relating to his particular situation, at any time to processing of personal data concerning him, if processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, including profiling based on those provisions. In this case the data controller shall 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 for the establishment, exercise or defence of legal claims.

Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such purposes, which includes profiling to the extent that it is related to such direct marketing.

Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

XIV. Remedies available to the User

If the personality rights of the User are violated as well as in the cases provided for in the Regulation, the User shall have the right to contact

- the Data Controller; or
- the Hungarian National Authority for Data Protection and Freedom of Information for assistance, or lodge a complaint with the Authority at the address below:
- Name: **Hungarian National Authority for Data Protection and Freedom of Information**
 Mailing address: H-1530 Budapest, Pf.: 5.
 Address: H-1125 Budapest, Szilágyi Erzsébet fasor 22/c.
 Telephone: +36 (1) 391 1400
 Fax: +36 (1) 391 1410
 Web: naih.hu
 E-mail: ugyfelszolgalat@naih.hu
- and shall also be entitled to bring a claim at the court of his or her place of residence or stay at his or her sole discretion.

The Data Controller shall support the Data Subject in exercising his or her rights based on the request submitted. The Data Controller shall inform the data subject of the measures taken in response to his or her

request without undue delay and no later than within one month of receipt of the request. If necessary, and taking into consideration the complexity and the number of requests, this deadline may be extended by an additional two months. The Data Controller shall inform the data subject of the extension of the deadline within one month of receipt of the request, stating the reasons for the delay. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in an electronic form.

If the data controller decides not to take action on the request of the data subject, it shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

General information on data processing as well as notification and measures shall be provided to the Data Subject based on his or her rights specified in item XVI without any consideration. Where the data subject's request is manifestly unfounded or excessive, in particular because of its repetitive nature, the Data Controller shall, taking into consideration the administrative costs of providing the information or notification requested or of taking the measure requested:

- a) charge a reasonable fee (taking into consideration the provisions of law on the costs that may be included in case of disclosure of data of public interest), or
- b) refuse to act on the request.

The burden of proof that the request is manifestly unfounded or excessive lies with the Data Controller. Without prejudice to Article 11 of the GDPR, if the Data Controller has reasonable doubts about the identity of the natural person who submitted the request, it may request additional information necessary to confirm the identity of the data subject.

XV. Changes to the Notice, entry into force

The Data Controller reserves the right to amend or update this Privacy Notice at any time without prior notice and to publish the updated version on its websites. Any amendments will only apply to Personal Data collected after the publication of the amended version.

This Privacy Notice shall enter into force on the day of its announcement when the previous Privacy Notice of the Data Controller is simultaneously repealed.

Budapest, 30 June 2020

1. Annex: Data Processors engaged in the processing of personal data

Data Processor	Company registration number / VAT number	Activity performed
Process Solutions Kft.	01-09-679494 / 11847199-2-41	Payroll
SZINVA COMP Szervező és Számítástechnikai Szolgáltató Kft.	05-09-000350 / 10219395-2-05	Invoicing
Grefi-Ász Bt.	01-06-772230 / 22242103-1-42	Accounting
IT Szervíz Kft.	01-09-952734 / 23096479-2-42	Information technology services
IT PRO Health Kft.	01-09-999778 / 26338491-1-41	Healthcare services
Capital Medical Point Korlátolt Felelősségű	01-09- 330023 / 25531141-2-41	Healthcare services
West Health Kft.	01-09-997158 / 24237961-2-41	Healthcare services
Maternity Magánklinika Kft	01-09-918867 / 14766624-2-43	Healthcare services
RADIO DENTAL EXTRA Korlátolt Felelősségű Társaság	01-09-182921 / 24797410-8690-113-01	Healthcare services
T & G Health Kft.	01-09-879970 / 13280484-2-41	Healthcare services
Duna Medical Center Korlátolt Felelősségű Társaság	01-09-191967 / 24963145-2-43	Healthcare services
eRAD-BB Kft.	01-09336036 / 26628950-2-43	Healthcare services
Istenhegyi Családtervezési és Nőgyógyászati Központ Szolgáltató Kft.	01-09-871109 / 13746915-2-43	Healthcare services
Medicover Egészségközpont Zrt.	01-10-042382 / 10895986-2-43	Healthcare services
MEDSERV Egészségügyi Kft.	01-09-560510	Healthcare services
RMC Medical Egészségügyi és Szolgáltató Zrt.	01-10-048721 / 5453072-2-41	Healthcare services
Affidea Magyarország Kft.	01 09 078533 / 10604416-2-42	Healthcare services