Privacy Policy

The purpose of this Privacy Policy (hereinafter referred to as: **the Policy**) is to ensure that the personal data of Data Subjects (herinafter referred to as: **Data Subjects**) using the health services (namely various musculoskeletal therapies and APPI Rehabilitaion Pilates Instructor Training Courses) of Fiziopont Kft.

(1122 Budapest,Almatca 10/A.) Building A; hereinafter referred to as: the **Service Provider** or **Data Controller**) be performed in a legally compliant, trustworthy and transparent manner, as well as in accordance with the provisions of Act No. CXII of 2011 on the right to informational self-determination and freedom (hereinafter referred to as: the **Information Act**) and with the EU General Data Protection Regulation (GDPR). Thus, this Policy covers the purpose and legal basis of data management in the "Budapestfizio" clinic (1026 Budapest, Szilágyi Erzsébet fasor 17-21.; hereinafter referred to as: the **Clinic**), as well as the http://www.budapestfizio.hu website (hereinafter referred to as: the **Website**) operated by the Service Provider, the duration of data storage and the Data Subjects' personal data related rights and remedies.

The provisions of the following legal regulations must also be adhered to upon certain data processing steps: Act CLIV of 1997 on health care (hereinafter referred to as: the **Health Care Act**), Act No. XLVII of 1997 on the protection of health and related personal data (hereinafter referred to as: the **Health Care Data Protection Act**), Act No. CLV of 1997 on Consumer Protection (hereinafter referred to as: the **Consumer Protection Act**) and Act No. C of 2000 on Accounting (hereinafter referred to as: the **Accounting Act**).

The Service Provider hereby draws the Data Subject's attention to the fact that giving consent to any data processing included in this Policy means that the Subject has given consent to all such data processing, however the Data Subject is entitled to revoke such consent at any time as described in the Policy.

1. PERSONAL DATA PROCSSING DURING WEBSITE USE

1.1. Website logging

1.1.1. Web server logging

Upon visiting the Website the web server automatically logs the Data Subject's activities in order to ensure the smooth operation of services. The following data will be processed during this procedure: IP address, device and browser data, which in themselves are not suitable for identifying the Data Subject, however allow certain deductions regarding the Data Subject when linked to other data (i.e. data disclosed on the online booking form). The Service Provider shall not link the data encountered upon analyzing the log files with any other information and does not endeavor to identify the Data Subject.

Data processing pursued via the logging of website visiting data by the web server are common data processing techniques on the Internet, thus the Data Subject will accept them by using the Internet and visiting websites.

1.1.2. Logging related data processing by third party service providers

The external service providers' servers communicate directly with the Data Subject's computer and so the external service providers can collect data (such as IP address, browser and operating system data, mouse movements, websites visited and visit duration) due to their direct communication with the Data Subject's browser.

Website hits and other web analytics data are independently measured and audited by Google Analytics. The data processors can provide the Data Subject detailed information on the management of measurement data at http://www.google.com/analytics/.

In order to enable access to Facebook and Google+ services the Website is directly connected to the vendor servers accessible at facebook.com and plus.google.com

The data processors' data processing policies are available at their respective websites at https://www.facebook.com/privacy/explanation; http://www.google.com/intl/hu/policies.

The Service Provider has no influence on the data processing policies of other websites in case of links directing visitors to other websites. In the event that the Data Subject leaves the Website via such links, the so visited website operator's privacy policy shall prevail.

1.2. Cookies

A cookie is small file created on the Data Subject's computer upon visiting a website. Cookies may have numerous functions including that of collecting information, storing the Data Subject's personal settings and they generally support the Data Subject in using a website more comfortably.

The Service Provider uses cookies to identify Data Subjects, their current browsing session, to store the data disclosed during that session and thereby prevent any loss of data.

1.2.1. Necessary (session) cookies

These cookies are required for the Data Subjects to be able to browse our Website, use its various functions, such as storing the Data Subject's activities during a visit. These cookies expire at the end of the Data Subject's visit to the website and are deleted from the Data Subject's device at the end of the given browsing session. We cannot guarantee the browsing of our Website without the use of such cookies.

1.2.2. Functional Cookies

These cookies enable the Service Provider to store the Data Subject's choices on the Website or the information disclosed by him/her. This allows the Service Provider to customize the Website to the Data Subject's needs. These are (permanent) cookies with exact expiration times that are stored on the device until deletion or their expiration time.

1.2.3. Third party cookies on the Website:

The following third parties operate cookies on our Website:

Third party	Detailed information on cookies available at
google.com/analytics	https://developers.google.com/analytics/devguides/collection/analyticsjs/cookie-usage
Facebook	https://hu-hu.facebook.com/policies/cookies/

1.2.4. Embedded content from other websites

Website postings may include embedded content (i.e. videos, images, articles etc.) from external sources. Embedded content from external sources operate as if we had visited another website. Such websites may collect data about their visitors, use cookies or third party tracking codes, monitor embedded content-related user activities if the Data Subject has a user account and is logged in on the site.

1.2.5. Enabling or blocking cookies

Cookies can legally be used on the basis of the Data Subject's consent. Consent is given by the Data Subject clicking on the *"Accept"* button on the Website.

All modern browsers enable the changing of cookie settings. Most browsers automatically enable cookies as a default setting, but these can usually be changed to prevent automatic consent and have the browser offer the option upon each site visit to check whether you would like to enable cookies or not. If the Data Subject does not accept the use of cookies, he/she will automatically be redirected from our Website.

We warn the Data Subject that since the purpose of our cookies is to enable the smooth and effective use of our Website, blocking the use of cookies or erasing them may result in the Data Subject not having full access to all functions of our Website or the Website may not operate as originally designed in his/her browser.

You may consult the following websites for the cookie settings and restriction of cookies in major browsers:Google ChromeFirefoxMicrosoft Internet Explorer 11Microsoft Internet Explorer 10Microsoft Internet Explorer 9Microsoft Internet Explorer 8Safari

If you need assistance in managing your cookie settings or deleting cookies, please contact us via our contact channels indicated in section 7 of this policy.

2. DATA PROCESSED UPON CONTACTING US

2.1. Data pocessing content

If the Data Subject has any questions, wishes to leave a message, would like a consultation or request an appointment, he/she may initiate contact with the Service Provider by clicking on the *"Contact"* and *"Book Online"* menu of our Website. Personal data are requested when filling out the online booking form.

Appointments for the Service Provider's health services may be made by phone or email or via the contact points listed in this Policy or found on the Website. In such cases the name, email address and phone number are requested for communication purposes.

Purpose of data pocessing	Legal basis for data processing	Scope of processed data	Duration of data pocessing
Providing the Data Subject information regarding his/her questions, comments made upon contacting us; traceability of information exchanged during contact; booking appointments	Data Subject's consent	name, email address, phone number, date and time of appointment, type of care requested and other personal data given in the message	until the Data Subject revokes his/her consent, but maximum 5 years from the time of disclosing the data

The Service Provider records the Data Subject's relevant data - meaning his/her name, phone number, time of appointment - in the *"online booking calendar"* (Google Calendar).

The Data Subject may revoke his/her consent to processing his/her personal data given upon initial contact at any time via the points of contact listed in section 7.

2.2. Joint data processing

Data given while filling out the *„Online booking form"* are automatically forwarded to the info@budapestfizio.hu email address (hereinafter referred to as: the **Email Address**). The Service Provider may also be contacted directly through the Email Address. The Email Address is jointly managed by the following organizations (hereinafter referred to as: the **Joint Data Processors**):

Name	Contact Info
Fiziopont Kft.	1122 Budapest, Alma utca 10. Building A
Dr Daniele Mei	1026 Budapest Gábor Áron utca 23.
	69365515-1-51

The online booking calendar is also jointly managed by the Joint Data Processors.

Each of the Joint Data Processors are authorized to process contact related data, thus to process incoming emails to the Email Address and record the personal data and the appointments in the online booking calendar. Therefore, each of the Joint Data Processors are authorized to access the personal data found in the online booking calendar.

If the email message is specifically addressed to one of the Joint Data Processors or if the appointment logged in the booking calendar is specifically related to one of the Joint Data Processors, then that data processor shall be considered the exclusive processor of that specific personal data while rendering the requested health service.

2.3. External data processors

Name	Contact info	Data processing role
Total Studio Kft.	1043 Budapest Kassai utca 11. 4th floor, door 24	providing Website and email memory space, operating the online booking form (appointment booking system)

3. PERSONAL DATA PROCESSING IN THE COURSE OF USING HEALTH SERVICES

3.1. Data processing content

The Service Provider can only perform its health services at the Clinic upon receiving the Data Subject's personal data which will be processed as per the following terms and conditions:

Purpose of data processing	Legal basis for data processing	Scope of data processed	Duration of data processing
communication	voluntary consent	name, email address, phone	5 years

		number	
performing the service (treatment), romoting the maintenance or improvement of health, monitoring the subject's state of health	Health Care Data Protection Act § 4	medical history, Data Subject's medical complaint, services rendered, treatments given and related comments, Social Security Number	30 years [Health Care Data Protection Act §30]
invoicing and compliance with accounting requirements	Accounting Act	name, address, name of services rendered, fee, invoice number, date of issuing invoice, payment deadline	8 years [Accounting Act (2) §169]

Please note that failure to provide the above data required for performing our services and invoicing will result in the Service Provider's inability to the render the Data Subject any services.

3.2. Data Transfer

In case of bank card payments the card payment transaction data will be processed by Budapest Bank (official seat: 1138 Budapest, Váci út 193.).

Data transfer recipient	Transferred data	Legal grounds for data transfer
Budapest Bank (official seat: 1138 Budapest, Váci út 193.)	Data Subject's identification number, transaction value, date, time	Data Subject's consent

3.3. External data processors

Name	Contact info	Data processing role
Naturasoft Magyarország Kft.	1113 Budapest Bocskai út 77-79.	invoicing services
BéCsi 2000 Bt.	1131 Budapest Nővér utca 37.	accounting services

3.4. Service provider substitution

Based on the Data Subject's explicit and voluntary consent the Service Provider is authorized to transfer the Data Subject's personal data to a substitute in the event that the Service Provider is unable to render the service.

Authorized substitutes:
Dr Daniele Mei self-employed entrepreneur 1036 Budapest Gábor Áron utca 23.

In case of substitution the substitute's own privacy policy shall prevail.

4. PERSONAL DATA PROCESSING DURING PARTICIPATION IN THE APPI Rehabilitation Pilates Trainer COURSE

4.1. Data processing content

The Service Provider is the exclusive organizer of Pilates trainer courses in cooperation with the London-based Australian Pilates and Physical Therapy Institute where the relevant personal data are processed with the following conditions:

Purpose of data processing	Legal basis for data processing	Scope of data processed	Duration of data processing
rendering its services, certification, registration of credit points, communication	Data Subject’s consent	name, place and date of birth, mother’s maiden name, address, phone number, email address, name, qualifications, professional degree serial number, operating license/basic registration number	5 years subsequent to course completion
invoicing and compliance with accounting requirements	Accounting Act	name, address, name of services rendered, fee, invoice number, date of issuing invoice, payment deadline	8 years [Section (2) of § 169]

Please note that failure to provide the above data required for performing our services and invoicing will result in the Service Provider’s inability to render the Data Subject any services.

4.2. External data processors

Name	Contact info	Data processing role
APPI Education Ltd.	The Chapel Wellington Road, London NW10 5LJ, United Kingdom	to provide the training

5. OTHER DATA PROCESSING

5.1. Complaints management

If the Data Subject has any complaints regarding the Service Provider’s services, related data shall be processed according to the following:

Purpose of data processing	Legal basis for data processing	Scope of data processed	Duration of data processing
To manage complaints regarding the quality of services rendered by the Service Provider	Consumer Protection Act Section (7) of § 17/A	name, address, name of service purchased, its fee, date and time of using the service and filing the complaint, description of complaint	a copy of the complaint records and their written responses 5 years

Please note that failure to provide the above data will result in the Service Provider’s inability to remedy the complaint.

5.2. Job applications

The Service Provider shall store the applications received.

Purpose of data processing	Legal basis for data processing	Scope of data processed	Duration of data processing
application to a job vacancy, participation in the selection process	Data Subject's consent	cover letters, CVs, applications and the personal data therein	6 months from the date of submitting application

Please note that failure to provide the above data will exclude the Data Subject from applying to the published job vacancies via electronic channels.

5.3. Other

Information regarding data processing not included in this document shall be disclosed upon collecting such data.

A court of justice, prosecutor, investigating authority, authority dealing with administrative offences, administrative authorities, the National Authority for Data Protection and Freedom of Information (hereinafter referred to as: **NAIH**) and other organizations may request the Service Provider to provide information, disclose or transfer of data or provide access to physical records. If the authorities have given the precise purpose and scope of data requested, the Service Provider shall only disclose the parts of personal data that are absolutely essential to execute the aims of the request.

6. METHOD OF PERSONAL DATA STORAGE, DATA PRIVACY

The secure storage of health services related health and personal data is done via so-called medical charts, paper based documents that the Service Provider keeps in locked filing cabinets. These data are only accessible to the Service Provider.

The Service Provider stores written communication and appointment booking related personal data online. The Joint Data Processors have access to these data.

The Service Provider also stores a copy of the invoices issued to Data Subjects on its server which is only accessible to the Service Provider.

The Service Provider shall take all the technical and organizational measures to guarantee proper security regarding data processing related risks including, among other things: (i) the use of pseudonyms and encryption of personal data; (ii) constantly ensuring the confidentiality, integrity, availability and resistance of the systems and services used to process personal data; (iii) the ability to restore the availability and accessibility of personal data in case of physical and technical incidents in a timely manner; (iv) regular efficiency testing, assessment and evaluation procedures for the technical and organizational measures implemented to guarantee secure data processing.

7. DATA PROCESSOR CONTACT INFORMATION

Fiziopont Limited Liability Company
Official seat: 1122 Budapest, Alma utca 10. Building A
Court of Registry No. Cg.01-09-185126
Registry: Budapest Court of Registration
Contact person's name: Georgina Várhelyi
Email address: info@budapestfizio.hu
Phone number :06703353351

8. Data subject's rights

8.1. General provisions

This Policy includes information regarding the Data Subject's personal data. The Data Subject may also request oral information after proving his identity with personal identification documents. The Service Provider may not refuse the Data Subject's following requests, unless the former can prove that he/she is unable to identify the Data Subject. In the event that the Service Provider has reasonable doubt regarding the identity of the natural person making the request, he/she may request further information/documentation to verify the Data Subject's identity.

The Service Provider shall inform the Data Subject of the measures taken in response to his/her request without undue delay, maximum within 1 month from the date of submitting such request. In duly substantiated cases, if the complexity or number of requests justifies it, the deadline may be extended by an additional 2 months. The Service Provider shall communicate such an extension of the deadline to the Data Subject within 1 month from receiving the request and also indicate the reasons for the delay. If the Data Subject had submitted his/her request electronically, the response to his/her request shall also be given electronically, unless otherwise requested by the Data Subject.

In the event that the Service Provider decides not to to take any measures pursuant to the Data Subject's request, he/she must inform the Data Subject of such decision without delay, maximum within 1 month from the date of receiving the request and inform him/her of the reasons thereof, as well as the Data Subject's options for legal remedies as described in section 9 of this Policy. The Service Provider shall not charge any fees for such information, communication or measures taken in response to such requests. If the Data Subject's request is clearly without grounds - especially due to its repetitive nature - or is unreasonably overstated, the Service Provider may charge a fee commensurate to the extra costs of providing the requested information or the administrative costs arising from taking the necessary measures, or may refuse to take any measures in response to the request.

8.2. Data subject rights regarding data processing

8.2.1. Right of access

The Data Subject is entitled to receive feedback on whether his/her personal data are being processed and if such data processing is happening he/she has the right to access his/her personal data and information regarding the processing thereof as described in this Policy.

The Service Provider shall provide the Data Subject access to a copy of the personal data that is the subject of processing. The Service Provider may charge a fee commensurate to the extra administrative expenses generated in case of additional copies requested by the Data Subject. If the Data Subject had submitted his/her request electronically, the response to his/her request shall also be given via a widely used electronic means, unless otherwise requested by the Data Subject.

8.2.2. Right to rectification

The Data Subject has the right to request that the Service Provider rectify any inaccurate personal data pertaining to him/her without any undue delay, or request that they be completed - with consideration to the purpose of Data Processing.

8.2.3. Right to erasure

The Data Subject has the right to request that the Service Provider erase his/her personal data without undue delay and the Service Provider is obliged to erase his/her personal data without undue delay if any of the following circumstances hold true:

(i) the personal data are no longer necessary for the purpose for which they were collected or they have been processed otherwise;
(ii) the Data Subject wishes to revoke his/her consent and the data processing has no other lawful basis;
(iii) the Data Subject objects to the processing of his/her data, and there is no overriding legitimate interest to continue this processing or the Data Subject objects to processing their personal data for direct marketing purposes;
(iv) the personal data have been unlawfully processed;
(v) the personal data have to be erased for the Service Provider to comply with a legal obligation prescribed by EU or national legal regulations;
(vi) the personal data have been collected to offer information society services to a child.

Where the controller has made the personal data public and is obliged pursuant to this Policy 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 that 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.

The obligation to erase the data shall not apply to the Service Provider to the extent that processing is necessary:

(i) for exercising the right of freedom of expression and information;

(ii) for compliance with a legal obligation or for the performance of a task carried out in the public interest; (iii) or

for the establishment, exercise or defense of legal claims.

8.2.4. Right to restrict processing

The data subject shall have the right to obtain from the Service Provider restriction of processing where one of the following applies:

(i) the accuracy of the personal data is contested by the Data Subject, for a period enabling the Service Provider to verify the accuracy of the personal data; or

(ii) the processing is unlawful and the Data Subject opposes the erasure of the personal data and requests the restriction of their use instead; or

(iii) the Service Provider 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 defense of legal claims; or

(iv) the data processing is carried out for the performance of a task carried out in the public interest or the the data processing is required for the exercise of the Service Provider's or a third party's rightful legal claims and the Data Subject has objected to processing for such purposes (in which case the restriction shall only apply for the duration of the verification whether the legitimate grounds of the Service Provider override those of the Data Subject).

Where processing has been restricted, such personal data shall, with the exception of storage, only be processed with the Data Subject's consent or for the establishment, exercise or defense of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest. A Data Subject who has obtained restriction of processing shall be informed by the Service Provider before the restriction of processing is lifted.

8.2.5. Right to be informed

The Service Provider shall inform all recipients of the rectification, erasure or restriction of data processing to whom they have disclosed the personal data, unless this proves impossible or requires disproportionate efforts. The Service Provider shall inform the Data Subject of the recipients of his/her data upon his/her request.

8.2.6. Right to object

The Data Subject shall have the right to object to the processing of his/her personal data on grounds relating to his/her particular situation, at any time if the processing is carried out for the establishment, exercise or defense of legal claims or for the protection of the rights of the Service Provider or a third party or for reasons of public interest. In such cases the Service Provider shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the Data Subject or for the establishment, exercise or defense 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 the processing of his/her personal data for such purposes. Where the Data Subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

Where personal data are processed for statistical purposes, the Data Subject, on grounds relating to his/her particular situation, shall have the right to object to the processing of his/her personal data, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

8.2.7. Right to data portability

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

a) the processing is based on consent or on a contract; and
b) the processing is carried out by automated means.

In exercising his/her right to data portability, the Data Subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible, however it may not adversely affect the rights and freedoms of others.

8.2.8. Rights in relation to automated decision making and profiling

The Data Subject shall have the right not to be subjected to a decision based solely on automated processing, including profiling, which produces legal effects concerning him/her or similarly significantly affects him/her, unless the decision (i) is necessary for entering into, or performance of, a contract between the Data Subject and the Service Provider; (ii) is authorized by law to which the Service Provider is subject and which also lays down suitable measures to safeguard the Data Subject's rights and freedoms and legitimate interests; or (iii) is based on the Data Subject's explicit consent.

The Data Subject has the right to request that the Service Provider use human intervention, as well as to express his/her or her point of view and to contest the decision.

The Service Provider does not exercise automated decision making or profiling.

8.2.9. Data breach

A data breach is a security incident in which transmitted, stored or otherwise controlled personal data are accidentally or illegally destroyed, lost, altered, disclosed to unauthorized parties or results in unauthorized access.

When the personal data breach is likely to result in a high risk to the rights and freedoms of the Data Subject, the Service Provider shall communicate the personal data breach to the Data Subject without undue delay. The communication to the Data Subject shall describe in clear and plain language the nature of the personal data breach and contain at least the following information and measures: (I) name and contact details of the contact person providing information; (ii) the probable consequences of the data breach; (iii) the measures implemented and planned by the Service Provider to remedy the data breach.

Communication to the Data Subject shall not be required if any of the following conditions are met: (i) the Service Provider has implemented appropriate technical and organizational protection measures, and those measures were applied to the personal data affected by the personal data breach; (ii) the Service Provider has taken subsequent measures which ensure that the high risk to the rights and freedoms of the Data Subject is no longer likely to materialize; (iii) communication would involve disproportionate effort.

In such cases the Data Subjects shall instead be informed via a public communication or similar measure whereby the Data Subjects are informed in an equally effective manner.

9. Remedies, liability and penalties

Any person who has suffered material or non-material damage as a result of an infringement of the Information Act shall have the right to receive compensation from the Service Provider or other data processor designated in this Policy for the damage suffered.

Any controller involved in processing shall be liable for the damage caused by processing which infringes the Information Act. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of the Information Act specifically directed to processors or where it has acted outside or contrary to lawful instructions of the Service Provider.

The Service Provider or data processor shall be exempt from liability if it proves that it is not in any way responsible for the event giving rise to the damage. Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the Data Subject.

If you have any questions, comments or problems regarding the Service Provider's data processing practices please contact the Service Provider via one of the communication channels in section 7.

In the event that the Data Subject disagrees with the Service Provider's decision he/she may initiate court proceedings (within 30 days from communication of the decision). The Service Provider is obliged to prove that his/her data processing practices are compliant with legal regulations. The suit shall be judged by the courts. The suit shall be filed at the court with jurisdiction at the Data Subject's place of residence or permanent address (depending on the Data Subject's preference).

The Data Subject also has the right to request information from the Hungarian National Authority for Data Protection and Freedom of Information regarding his/her rights and to initiate an inquiry regarding his/her grievance and its direct risks via one of the following contact points:

Hungarian National Authority for Data Protection and Freedom of Information
Official seat: 1125 Budapest, Szilágyi Erzsébet fasor 22/C.
Mailing address: 1530 Budapest, Pf.: 5.
Phone: 06.1.391.1400 Fax: 06.1.391.1410
Email address: ugyfelszolgalat@naih.hu
Website: http://www.naih.hu

10. DATA BREACH MANAGEMENT

The Service Provider' system administrator constantly monitors all warnings and alerts regarding critical network security incidents and vulnerabilities. In case of a breach the system administrator informs the Service Provider thereof and they jointly assess the breach in light of the circumstances. The Service Provider shall decide on subsequent measures and the correction of any errors in light of the severity of the breach.

An incident report shall be made in the event of a breach or in case of reasonable grounds to suspect a possible breach.

In the case of a personal data breach, the Service Provider shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority, unless he/she can prove in accordance with the principle of accountability that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where notification to the supervisory authority cannot be made within 72 hours, it shall be accompanied by reasons for the delay and the required information can also be communicated in several parts (without any further undue delays).

Reports on data breach shall be submitted to the Hungarian National Authority for Data Protection and Freedom of Information (NAIH) contact point(http://naih.hu/uegyfelszolgalat,--kapcsolat.html).

The Service Provider keeps a record of all data breach incidents describing the facts related to each incident, its effects and measures implemented to remedy them.

When the personal data breach is likely to result in a high risk to the rights and freedoms of the Data Subject, the Service Provider shall communicate the personal data breach to the Data Subject without undue delay.

The communication to the Data Subject shall not be required if any of the following conditions are met:

a) The Service Provider has implemented appropriate technical and organizational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorized to access it, such as encryption;
b) the Service Provider has taken subsequent measures which ensure that the high risk to the rights and freedoms of the Data Subject is no longer likely to materialize;
c) communication would involve disproportionate effort. In such cases the Data Subjects shall instead be informed via a public communication or similar measure whereby the Data Subjects are informed in an equally effective manner.

11. POLICY MODIFICATION

The Service Provider has made this Policy public on the Website and at the Clinic, where the effective Policy is accessible at any given time. The Service Provider may unilaterally modify this Policy at any time, however he/she is obliged to inform the Data Subjects of such changes via a communication on his/her Website at least 15 (fifteen) days prior to their coming into effect.

Date: Budapest, Friday, May 25, 2018