DATA MANAGEMENT STATEMENT

For the services of the climbing gym operated by Flow Climbing Zrt, as Data Controller, at 1117 Budapest, Hengermalom út 19-21, and in connection with the website https://www.flowboulder.hu, visitors, users, customers, partners (hereinafter collectively referred to as Customers) handles your data in accordance with the provisions of this information sheet (hereinafter the Information Sheet).

The Data Controller is entitled to unilaterally amend this information at any time in order to comply with the legal provisions in force at any time, including amendments related to the modification of the Data Controller's services. At the same time as the change, the affected parties will be informed about the changes to this information on our website, at https://www.flowboulder.hu.

If you have any questions about this information, please write to us at info@flowboulder.hu and we will answer your questions. This information sheet and its amendments can be found at the reception of the climbing gym (on paper) and on the website at https://www.flowboulder.hu.

The Data Controller wishes to fully comply with the legal requirements for the handling of data, so the Data Controller took into account the following legislation when creating the Information:

1. Regulation 2016/679 of the European Parliament and Council (EU) on the protection of the processing of personal data of natural persons and on the free flow of such data, as well as on the repeal of Regulation 95/46/EC (hereinafter: "GDPR"),

2. CXII of 2011 on the right to information self-determination and freedom of information. law,

3. CVIII of 2001 on certain issues of electronic commercial services and services related to the information society. law,

4. XLVII of 2008 on the prohibition of unfair commercial practices against consumers. law,

5. XLVIII of 2008 on the basic conditions and certain limitations of economic advertising activity. provisions of the law.

Name and contact details of data controller and service provider:

Company name: Flow Climbing Zrt.

Headquarters: 1124 Budapest, Pagony utca 25/A Tax number: 27833126-2-43

Company registration number: 01 10 141847

Website: http://www.flowboulder.hu/ E-mail: info@flowboulder.hu

Phone: +36202734354

2. DEFINITIONS

The following concepts in this information sheet have the following meanings

"data processor": the natural or legal person, public authority, agency or any other body that processes personal data on behalf of the data controller. The Data Controller is its activity

uses the designated Data Processors indicated in this information sheet during each data processing. The Data Processor does not make an independent decision, it is only authorized to act according to the yellow instructions agreed with the Data Controller. The Data Controller checks the work of the Data Processor. The Data Processor is entitled to use additional data processors only with the prior written consent of the Data Controller;

"data management": all operations or sets of operations performed on personal data or data files in an automated or non-automated manner, such as collection, recording, organization, segmentation, storage, transformation or modification, query, insight, use, communication, sending, distribution or other by way of making it available, coordination or connection, restriction, deletion or destruction;

"restriction of data management": marking stored personal data in order to limit future processing;

"data controller": the natural or legal person, public authority, agency or any other body that determines the purposes and means of personal data management independently or together with others; if the purposes and means of data management are determined by current or domestic law, the special considerations for appointing the data controller or the data controller are also determined by EU or domestic law;

"data incident": a breach of security resulting from the accidental or unlawful destruction, loss, alteration, unauthorized disclosure or unauthorized access to personal data transmitted, stored or otherwise handled.

"addressee": the natural or legal person, public authority, agency or any other body to whom or through which the personal data is communicated, regardless of whether it is a third party. Public authorities that have access to personal data in accordance with EU or domestic law in the context of an individual investigation are not considered

recipients; the management of said data by these public authorities must comply with the data protection rules in accordance with the purposes of data management;

"cookie": a cookie is a short text file that our web server sends to the affected device (be it any computer, mobile phone or tablet) and reads it back. There are temporary (session) cookies that are automatically deleted from your device when you close your browser, and there are longer-lived cookies that remain on your device for a longer time (this also depends on the settings of your device);

"data subject" is a person identified or - directly or indirectly - identifiable on the basis of personal data, which must always be a specified person. Only natural persons are considered affected, therefore not legal persons, thus data protection only protects the data of natural persons. On the other hand, the data of the individual entrepreneur or the representative of a company (e.g. telephone number, email address, place of birth, time, etc.) is considered personal data.

"consent of the data subject": the voluntary, specific and well-informed and clear declaration of the will of the data subject, with which the data subject indicates by means of a statement or an act clearly expressing the confirmation that he gives his consent to the processing of personal data concerning him;

"third party": the natural or legal person, public authority, agency or any other body that is not the same as the data subject, the data controller, the data processor or the persons who, under the direct control of the data controller or data processor, are authorized to process personal data they got;

"employee": a natural person in an employment, employment or other legal relationship with the Data Controller, who is entrusted with the task of providing and performing the Data Controller's services and comes into contact or may come into contact with personal data in the course of his data management or data processing tasks, and for whose activities the Data Controller assumes full responsibility in the direction of personnel and third parties.

"personal data": any information relating to an identified or identifiable natural person ("data subject"); a natural person can be identified directly or indirectly, in particular on the basis of an identifier such as name, number, location data, online identifier or one or more factors relating to the physical, physiological, genetic, mental, economic, cultural or social identity of the natural person can be identified. Natural persons can also be associated with online identifiers, such as IP addresses and cookie identifiers, as well as other identifiers, such as radio frequency identification tags, provided by the devices, applications, tools and protocols they use. This may result in traces that,

combined with unique identifiers and other information received by the servers, can be used to create a profile of natural persons and to identify that person;

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

3. PURPOSE AND SCOPE OF THE REGULATIONS

The primary purpose of these regulations is to define and adhere to the basic principles and provisions for handling the data of natural persons who come into contact with the Data Controller in order to ensure that the private sphere of natural persons is protected in accordance with the relevant legal provisions.

Its purpose is to ensure that the Data Controller complies in all respects with the data protection provisions of the applicable legislation.

These Regulations are valid from October 22, 2022 and remain in effect until further notice or withdrawal.

Personal scope covers:

1. to the Data Controller

2. for Employees and Partners

for the persons whose data is included in the data processing covered by these Regulations,

3. also to the persons whose rights or legitimate interests are affected by the data management.

4. PRINCIPLES RELATING TO DATA MANAGEMENT

The Data Controller processes personal data legally and fairly, in a transparent manner for the data subjects, for the clear and legitimate purposes specified in this information ("in accordance with the principle of purpose limitation"). Data management is limited to the extent necessary to achieve the Data Manager's goals ("data saving"). In accordance with the principle of accuracy, the Data Controller ensures that the personal data it manages is up-to-date, to this end, the Data Controller takes all reasonable measures to immediately delete or correct inaccurate personal data for the purposes of data management ("principle of accuracy"). The data controller acknowledges that personal data can only be stored for the time necessary to achieve its goals ("limited storage principle"). The data controller manages the data in such a way that the appropriate security of the personal data is ensured by applying the appropriate technical or organizational measures, including protection against

unauthorized or illegal processing, accidental loss, destruction or damage of the data ("integrity and confidentiality"). The data manager is the one presented

in order to verify compliance with the principles, it keeps internal data management records of its individual data management operations ("principle of accountability").

The principles contained in this information sheet describe our practice in relation to personal data. Our data management principles apply to paper-based data management, as well as to all devices, websites, customer service platforms or other online applications operated by the Data Controller, which refer to them via Internet links or in other ways.

5. GENERAL INFORMATION REGARDING DATA MANAGEMENT

The personal data of the data subject is managed by the Data Controller in order to provide the services used by the data subject and to improve the user's experience. This information sheet provides information on the data management carried out by the data controller in connection with the activities listed below:

1. When entering the climbing gym for the first time in connection with registration

2. Inquiries addressed to the company through various communication channels

regarding your answer

3. In connection with data management through cookies on the website operated by the company.

6. INFORMATION RELATING TO EACH DATA MANAGEMENT 6.1. REGISTRATION

The purpose of data management:

- identification of the user and contact with him

- registration of user status (pass) -

The range of stakeholders: Customers who enter the climbing gym for sports

The processed data: name, name of legal representative (in the case of minors), address, date and place of birth,

phone number, email address,

The legal basis for data management: The identification of the user as a customer and the consent of the data subject during contact with him is based on Article 6 (1) of the GDPR.

Duration of data management Until the registration of the person concerned is cancelled.

The group of persons entitled to access the data The company with customer service and invoicing

colleagues involved.

Data transmission:

There isn't

Data processors:

Flow Climbing Zrt uses GeriSoft Stúdió's software for entry, where part of the data entered during registration is entered.

The data management information is available from the following page: https://gerisoft.hu/files/Adatkezelesitajekoztato_GeriSoft.pdf

6.2. DATA HANDLING PERFORMED DURING CONTACT

The company can be contacted through several communication channels, e.g. email, telephone, social media. In the case of telephone inquiries, no audio recording is made of the conversation.

Purpose of data management: Serving those interested in the company's services, answering their questions, and maintaining contact.

The processed data: The personal data provided during contact are typically: Name, email address, phone number

Legal basis for data management: Consent of the data subject, based on Article 6 (1) point a) of the GDPR. Since the contact is always initiated by the data subject, the provision of personal data can be considered voluntary and consent to data management is given.

Duration of data management: Until the given question is answered.

The range of persons entitled to access the data: The company is entrusted with customer service

employees Data transmission: none Data processors: none

6.3. DATA MANAGEMENT RELATED TO COOKIE MANAGEMENT

Cookies are short text files consisting of letters and numbers that are downloaded to the browser of the computer, mobile device or other device by the web stores visited by the user. Cookies can be installed based on the user's device and a request sent to the server operating the website or a third party server. Cookies can be classified into 3 major groups:

Necessary cookies:

In order to ensure the correct operation of the online store, we must use cookies. We call those cookies necessary, without which the online store would not be able to function properly.

Necessary cookies can control, for example, the following functions:

- whether or not the login page should be displayed again to the visitor

- list of wishlist products

- the current language of the store, which the customer can set - etc

Statistical cookies:

Statistical cookies collect information about how our visitors use our online store. These cookies cannot accurately identify the user. Information collected by statistical cookies includes page views, clicks, length of sessions, time of visit, etc.

Marketing cookies:

Marketing cookies help the online store to provide its visitors with a more pleasant browsing experience, including by displaying personalized offers and advertisements.

7. INFORMATION ON THE RIGHTS OF THE PERSONS INVOLVED

Right to information and access to processed personal data:

The data subject has the right to receive feedback from the Data Controller as to whether his personal data is being processed, and if such data processing is underway, he is entitled to access the personal data and the following information:

a) the purposes of data management;

b) categories of personal data concerned;

c) the recipients or categories of recipients to whom or to whom the personal data has been or will be communicated, including in particular third-country recipients and international organizations;

d) where appropriate, the planned period of storage of personal data, or if this is not possible, the criteria for determining this period;

e) the right of the data subject to request from the data controller the correction, deletion or restriction of processing of personal data concerning him and to object to the processing of such personal data;

f) the right to submit a complaint addressed to a supervisory authority;

g) if the data were not collected from the data subject, all available information about their source;

h) the fact of automated decision-making, including profiling, as well as, at least in these cases, comprehensible information regarding the logic used and the significance of such data management and the expected consequences for the data subject.

If personal data is transferred to a third country or to an international organization, the data subject is entitled to receive information about the appropriate guarantees regarding the transfer.

The Data Controller provides a copy of the personal data that is the subject of data management to the data subject. For 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 Data Controller will provide the information in a widely used electronic format, unless the data subject requests otherwise.

The right to request a copy mentioned in the previous paragraph cannot adversely affect the rights and freedoms of others.

Right of rectification:

At the request of the data subject, the Data Controller shall correct inaccurate personal data of the data subject without undue delay. Taking into account the purpose of the data management, the data subject is entitled to request the addition of incomplete personal data, including by means of a supplementary statement.

For erasure (“right to be forgotten”):

If one of the following reasons exists, the data subject has the right to request that the Data Controller delete his/her personal data without undue delay:

a) personal data are no longer needed for the purpose for which they were collected or otherwise processed;

b) the data subject withdraws the consent that forms the basis of the data management, and there is no other legal basis for the data management;

c) the data subject objects to the data processing and there is no overriding legal reason for the data processing or if the data processing is related to direct business acquisition;

d) personal data were handled unlawfully;

e) personal data must be deleted in order to fulfill the legal obligation prescribed by EU or Member State law applicable to the data controller;

f) the collection of personal data took place in connection with the offering of services related to the information society.

Data deletion cannot be initiated if data management is necessary:

a) for the purpose of exercising the right to freedom of expression and information;

b) fulfillment of the obligation according to the EU or member state law applicable to the data controller requiring the processing of personal data, or in the public interest;

c) for preventive health or occupational health purposes, to assess the employee's ability to work, to establish a medical diagnosis, to provide health or social care or treatment, or to manage health or social systems and services, based on EU or Member State law or pursuant to a contract with a health professional and this data is handled by a professional or under the responsibility of a professional who is subject to the professional confidentiality obligation defined in EU or Member State law, or in the rules established by competent Member State bodies, or by another person who is also under EU or Member State law, or is subject to the obligation of confidentiality defined in the rules established by the competent Member State bodies;

d) for reasons of public interest in the field of public health, such as protection against serious health threats that spread across borders or ensuring the high quality and safety of health care, medicines and medical devices, and is done on the basis of EU or Member State law that is appropriate and specific provides for measures for guarantees protecting the rights and freedoms of the data subject, and in particular regarding professional confidentiality;

e) on the basis of the public interest affecting the field of public health and the handling of these data is carried out by a professional or under the responsibility of a professional who is subject to the professional confidentiality obligation defined in EU or Member State law, or in the rules established by the competent Member State bodies, or any other person by who is also subject to the obligation of confidentiality defined in EU or Member State law, or in the rules established by the competent Member State bodies;

f) archiving in the public interest, for scientific and historical research purposes or for statistical purposes, if the right to erasure would likely make this data management impossible or seriously endanger it1; obsession

g) to present, enforce and defend legal claims.

The right to restrict data processing:

At the request of the data subject, the Data Controller restricts data processing if one of the following conditions is met:

a) the data subject disputes the accuracy of the personal data, in which case the limitation applies to the period that allows the data subject to check the accuracy of the personal data;

b) the data management is illegal and the data subject opposes the deletion of the data and instead requests the restriction of their use;

c) the Data Controller no longer needs the personal data for the purpose of data management, but the data subject requires them to submit, enforce or defend legal claims; or d) the data subject objected to the data management in connection with the Data Controller's data management based on public interest or legitimate interest; in this case, the restriction applies to the period until it is established whether the legitimate reasons of the data controller take precedence over the legitimate reasons of the data subject.

If data processing is subject to restrictions based on the above, such personal data, with the exception of storage, will only be processed with the consent of the data subject, or for the presentation, enforcement or defense of legal claims, or for the protection of the rights of another natural or legal person, or in the important public interest of the Union or a member state can be handled.

The Data Controller informs the data subject at whose request the data management has been restricted on the basis of the above in advance of the lifting of the restriction of data management.

Right to data portability:

The data subject has the right to receive the personal data concerning him/her provided to the Data Controller in a segmented, widely used, machine-readable format, and is also entitled to transmit this data to another data controller without being hindered by the data controller whose provided the personal data if:

a) data management is based on consent or contract; and b) data management is performed in an automated manner.

When exercising the right to data portability as described above, the data subject is entitled to - if this is technically feasible - request the direct transfer of personal data between data controllers.

Exercising the right to data portability cannot violate the right to erasure ("forgetfulness"). The aforementioned right does not apply if the data processing is in the public interest or is necessary for the performance of a task performed in the context of the exercise of the public authority delegated to the data controller.

The right to data portability must not adversely affect the rights and freedoms of others.

Right to protest:

The data subject has the right to object at any time to the processing of his personal data by the Data Controller for reasons related to his own situation, if the legal basis of the data processing is the public interest or the execution of a task performed in the framework of the exercise of public authority vested in the Data Controller, or the need to assert the legitimate interests of the Data Controller or a third party, including profiling based on the aforementioned provisions. In this case, the Data Controller may no longer process the personal data, unless it proves that the data processing is justified by compelling legitimate reasons that take precedence over the interests, rights and freedoms of the data subject, or that are related to the submission, enforcement or defense of legal claims.

If personal data is processed for the purpose of direct business acquisition, the data subject has the right to object at any time to the processing of his personal data for this purpose, including profiling, if it is related to direct business acquisition. If the data subject objects to the processing of personal data for the purpose of direct business acquisition, then the personal data may no longer be processed for this purpose.

If personal data is processed for scientific and historical research purposes or for statistical purposes, the data subject has the right to object to the processing of personal data concerning him for reasons related to his own situation, unless the data processing is necessary for the performance of a task carried out for reasons of public interest.

Right of withdrawal:

The data subject has the right to withdraw his consent at any time if the Data Controller's data processing is based on the consent of the data subject. Withdrawal of consent does not affect the legality of data processing based on consent prior to withdrawal.

Procedure in the event of a stakeholder request related to the exercise of the above rights:

Without undue delay, but in any case within one month (30 days) from the receipt of the request, the Data Controller informs the data subject of the measures taken following the data subject's request regarding the exercise of the rights set out in this information. If necessary, taking into account the complexity of the application and the number of applications, this deadline can be extended by another two months.

The Data Controller shall inform the data subject of the extension of the deadline, indicating the reasons for the delay, within one month of receiving the request. If necessary, consider

considering the complexity of the application and the number of applications, this deadline can be extended by another two months (60 days). If the data subject submitted the request electronically, the information will be provided electronically, if possible, unless the data subject requests otherwise.

If the Data Controller does not take measures following the data subject's request, it shall inform the data subject without delay, but at the latest within one month of the receipt of the request, of the reasons for the failure to take action, and of the fact that the data subject may file a complaint with a supervisory authority and exercise his right to judicial redress.

The Data Controller provides the requested information and information free of charge, provided that to the extent that the data subject's request is clearly unfounded or - especially due to its repetitive nature - excessive, the Data Controller may charge a reasonable fee for the administrative costs associated with providing the requested information or information or taking the requested action , or you can refuse to take action based on the request.

The Data Controller informs all recipients of all corrections, deletions or data management restrictions carried out by it, to whom or to whom the personal data was communicated, unless this proves to be impossible or requires a disproportionately large effort. At the request of the data subject, the Data Controller informs about these recipients.

Please send any questions or requests regarding your personal data stored in the system and data management to our e-mail address. Please keep in mind that, in your interest, we are only able to provide information or take action regarding the management of your personal data if you have verified your identity.

In order to respond to your request, we always need the following information:

- your email address provided during registration
- your full name

 your billing address

Please make sure that you send the inquiry from the email address provided during registration.

8. DATA SECURITY MEASURES

The Data Controller and the operator of the server network protect the data with the most up-to-date hardware and software support that is reasonably available, in particular against unauthorized access, change, transmission, disclosure, deletion or destruction, as well as against accidental destruction and damage, thus serving data security. As a general rule, the data managed by the Data Controller can only be accessed by the Data Controller's employees and other collaborators involved in the implementation of the data management goals defined in these Rules, who, based on their employment contract, their employment relationship, and other contractual legal relationships, the legal provisions, and all, on the basis of the Data Controller's instructions, they are subject to a confidentiality obligation with regard to the data they learn. All data management activities of the Data Controller must be accurately documented. The Data Controller must keep a record of all data management activities it performs (e.g. newsletter, webshop, employee register). The Data Controller keeps a data transfer register for the purpose of checking the legality of the data transfer and for informing the data subject, which includes the date of transfer of the managed data, legal basis, recipient, definition of the scope of data, and other data specified in the legislation requiring data management.

8.1. SECURITY OF PERSONAL DATA HANDLED ON PAPER

In order to ensure the security of paper-based personal data, the Data Controller applies the following measures:

• the data can only be seen by those authorized to do so, they can no longer be accessed, they cannot be disclosed to others,

• place the documents in a well-sealed, dry room equipped with fire protection and asset protection equipment

• documents in continuous active processing can only be accessed by those in charge,

• during the day, the employee performing data management can only leave the room where data management takes place by locking the data carriers entrusted to him or by closing the office,

• if the personal data managed on paper are digitized, the Data Controller applies the security rules applicable to digitally stored documents, and demands the same from its data processors.

8.2. SECURITY OF DIGITALLY STORED PERSONAL DATA

In order to ensure the security of personal data stored on a computer or network, the Data Controller takes the following measures:

 all access to the data is logged in a traceable manner,

 constantly takes care of virus protection on the network handling personal data,

 prevents network access by unauthorized persons with the available computer technology tools and their application

9. DATA PROTECTION INCIDENT

Data protection incident: a breach of security that results in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to, personal data transmitted, stored or otherwise handled.

If the data protection incident is likely to involve a high risk for the rights and freedoms of natural persons, the Data Controller shall inform the data subject about the data protection incident in a clear and understandable manner without undue delay.

The data subject does not need to be informed if any of the following conditions are met:

a) the data controller has implemented appropriate technical and organizational protection measures and these measures have been applied to the data affected by the data protection incident, in particular those measures - such as the use of encryption - that would be unintelligible to persons not authorized to access personal data they make the data;

b) after the data protection incident, the data controller has taken additional measures to ensure that the high risk to the rights and freedoms of the data subject is unlikely to materialize in the future;

c) providing information would require a disproportionate effort. In such cases, the data subjects must be informed through publicly published information, or a similar measure must be taken that ensures similarly effective information to the data subjects.

10. REMEDIES

a) The Data Controller can be contacted with any questions or comments related to data management

At one of the contact details provided in the brochure.

b) You can initiate an investigation by filing a report with the National Data Protection and Freedom of Information Authority (address: 1374 Budapest, Pf. 603., phone: +36-1-

391-1400, email: ugyfelszolgalat@naih.hu, website: www.naih.hu) with reference to the fact that there is a direct risk of a violation of rights in relation to the processing of your personal data; respectively

c) In the event of a violation of their rights, the data subject may apply to court against the Data Controller. The court acts out of sequence in the case. The Data Controller is obliged to prove that the data management complies with the provisions of the law. The adjudication of the lawsuit falls within the jurisdiction of the court. The lawsuit - at the choice of the affected person - can be initiated before the court of the affected person's place of residence or residence.

Before filing a complaint with the supervisory authority or the court, we ask that you contact us at one of the contact details provided in order to negotiate and resolve the problem as quickly as possible.