DATA MANAGEMENT INFORMATION

1. **INTRODUCTION**

The **LIGET MÁSZÓSPORT Kft**, as the Data Controller/Company, at 8200 Veszprém, Hóvirág utca 1/B. the services of the wall climbing room and the website https://www.ligetboulder.hu
in relation to visitors, users, customers, partners (hereinafter collectively referred to as Customers) processes your data in accordance with the terms of this notice (the "Notice").
The Data Controller is entitled to unilaterally amend this notice at any time in order to,
to comply with the legal provisions in force at the time, including those of the Data Controller changes related to changes to its services. For information about changes to this notice, please contact. at the same time as the change, we will inform those concerned on our website https://www.ligetboulder.hu
side.
If you have any questions about this information, please contact us at.
ligetboulder@gmail.com and we will answer your questions. This leaflet and its
can be found at the reception desk in the climbing room (on paper), as well as in the
on the website at https://www.ligetboulder.hu.
The Data Controller intends to comply fully with the applicable laws on the processing of personal data. legal requirements, so in developing the Information, the Data Controller has taken into account the following
legislation:
1. on the protection of natural persons with regard to the processing of personal data
on the free movement of such data and repealing Regulation (EC) No 95/46/EC
Regulation (EU) No 2016/679 of the European Parliament and of the Council (the "GDPR"),
2. in accordance with the Act CXII of 2011 on the right to information self-determination and freedom of information.
Act,
3. e-commerce services and information society services
Act CVIII of 2001 on certain aspects of services related to the provision of health care,
4. the 2008 Act on the Prohibition of Unfair Commercial Practices against Consumers
Act XLVII,
5. the 2008 Act on the Basic Conditions and Certain Restrictions on Commercial Advertising Activities.
Act XLVIII.
Name and contact details of the data controller, service provider:

Company name: LIGET MÁSZÓSPORT Kft.
Office: 8200 Veszprém, Hóvirág utca 1.
Tax number: 32222254-2-19
Company registration number: 19-09-523681
Website: http://www.ligetboulder.hu/
E-mail: ligetboulder@gmail.com
Phone: +36703242926

2. **DEFINITIONS**
The following terms used in this leaflet shall have the following meanings
"data processor" means a natural or legal person, public authority, agency or any
other body that processes personal data on behalf of the controller. The Data Controller shall in its activities
in this information notice, for the purposes of each processing operation, the named

It uses data processors. The Data Processor does not make any decisions on its own, but only
You are entitled to act in accordance with the contract with the controller and the instructions you have received. The Controller shall monitor
the work of the Data Processor. The Data Processor may only use an additional data processor for the
With the prior written consent of the controller, you are entitled to.;
"processing" means the automated or non-automated processing of personal data or data files
any operation or set of operations carried out in any way, such as collecting, recording, organising,
tagging, storage, transformation or alteration, retrieval, consultation, use, disclosure,
by transmission, distribution or otherwise making available, coordinating or
interconnection, restriction, erasure or destruction;
"restriction of processing" means the designation of personal data stored and the restriction of their future processing
for the purposes of;
"controller" means a natural or legal person, public authority, agency or any other body
body which, alone or jointly with others, determines the purposes and means of the processing of personal data
where the purposes and means of the processing are determined by EU or national law, the
the controller or specific criteria for the designation of the controller in the EU or national law
law may also determine;
"data breach" means a breach of security that compromises the security of data transmitted, stored or otherwise
accidental or unlawful destruction, loss or alteration of personal data processed,
unauthorised disclosure of, or access to, personal data.
"recipient" means a natural or legal person, public authority, agency or any other body
the body with whom or to which the personal data are disclosed, whether or not a third party. For that public authorities which, in the framework of an individual investigation in accordance with EU or national law
have access to personal data, they are not recipients; the data in question are not subject to the
processing by bodies must be compatible with the purposes of the processing in accordance with the applicable
data protection rules;
"cookie": a cookie is a short text file that our web server sends to your device (be it
from any computer (mobile phone or tablet) and reads it back. There are temporary
(session) cookies, which are automatically deleted from your device,
when you close your browser, and there are longer-lived cookies that last longer
will remain on your device (this depends on the settings of your device);
"data subject" means an individual who is or may be identified, directly or indirectly, on the basis of personal data
person, which must always be a specific person. Natural persons only
persons are data subjects, not legal persons, so that data protection is only applicable to
protects the data of natural persons. However, personal data include, for example, personal data of a self-employed person
or the details of a company representative (e.g. telephone number, email address, date and place of birth, etc.).
"data subject's consent" means the freely given, specific and informed indication of the data subject's wishes
based on and unequivocal statement by which the declaration or confirmation concerned
by an unambiguously expressive act, indicates his or her consent to the personal data concerning him or her
to manage data;
"third party" means a natural or legal person, public authority, agency or any other
a body other than the data subject, the controller, the processor or those

persons who, under the direct authority of the controller or processor, are responsible for the processing of personal data
are authorised to manage;
"employee" means a natural person who has a contract, employment or other legal relationship with the Data Controller
a person who is entrusted with the task of providing or performing the services of the Data Controller and
comes into contact with personal data in the course of its data processing or processing activities; or
and in relation to whose activities the Data Controller assumes full responsibility for the
data subjects and third parties.
"personal data" means data relating to an identified or identifiable natural person ("data subject")
any information; the natural person who, directly or indirectly,
in particular, an identifier such as a name, number, location data, online identifier or
a natural person's physical, physiological, genetic, mental, economic, cultural or social
can be identified by one or more factors relating to its identity. Natural persons are
and can be linked to the devices, applications, tools and
online identifiers provided by protocols, such as IP addresses and cookie identifiers,
and other identifiers such as radio frequency identification tags. In this way
may generate traces that are linked to unique identifiers and other data received by the servers
information may be used to create profiles of natural persons and
to identify that person;
'undertaking' means any natural or legal person carrying on an economic activity, regardless of the legal form of the undertaking.
including partnerships engaged in a regular economic activity, and
associations;

3. **PURPOSE AND SCOPE OF THE CODE**
The primary purpose of this Policy is to enable natural persons who come into contact with the Data Controller to.
define and comply with the basic principles and provisions governing the processing of your data
to ensure that the privacy of natural persons is protected in the relevant
in accordance with the law.
Its purpose is to ensure that the Data Controller complies in all respects with the legislation in force.
provisions on data protection.
These Rules shall apply from **10 May 2023** and shall remain in force until further notice or until revoked.
in force.
Personal scope covers:
1. to the Data Controller
2. to Employees, Partners
persons whose data are included in the processing covered by this Policy,
3. and to persons whose rights or legitimate interests are affected by the processing.

4. **PRINCIPLES GOVERNING DATA MANAGEMENT**
The Data Controller shall process personal data lawfully and fairly, in a transparent manner for the data subjects.
in the manner and for the clear and legitimate purposes set out in this Notice ("**Purpose").**
The processing is limited to the extent necessary to achieve the purposes of the Data Controller.
limited ("**data economy**"). In accordance with the principle of accuracy, the Data Controller shall ensure that the
the personal data it processes are up to date, the Data Controller will use reasonable efforts to ensure that
take steps to ensure that personal data are inaccurate for the purposes for which they are processed

without undue delay (the "**Accuracy Principle**"). The Data Controller acknowledges that the
store personal data only for the time necessary for the purposes for which it is collected ("**limited retention")**
principle"). The Data Controller shall process the data in such a way that appropriate technical or organisational
measures to ensure adequate security of personal data, including the
the unauthorised or unlawful processing, accidental loss, destruction or
damage ("**integrity and confidentiality**"). The data controller shall use the following
3 to demonstrate compliance with the Principles, an internal data management system for each of its data processing operations
keeps records ("**accountability principle**").
The principles in this notice describe our practices regarding personal data.
Our data processing principles apply to paper-based data processing and to all data processing activities carried out by the Data Controller.
a device, website, customer service platform or other online application operated by,
which refers to them by means of a link or other reference on the Internet.

5. **GENERAL INFORMATION ON DATA MANAGEMENT**
The Controller uses the personal data of the data subject for the provision of the services used by the data subject,
and to improve the user's experience. This information is provided by the controller to the
provides information on the processing of data in relation to the activities listed below:
1. On first entry to the climbing room, in connection with registration
2. Enquiries made to the company through various communication channels
in response to the
3. In connection with the processing of data via cookies on the website operated by the company.

6. **INFORMATION ON CERTAIN DATA PROCESSING**

6.1. **REGISTRATION**
Purpose of the processing:
- identifying and contacting the user
- registering the user status (lease)
- Surveillance with cameras for the protection of property and human life and limb

Data subjects: customers entering the climbing gym for sporting purposes
The data processed are: name, name of legal representative (in case of a minor), address, date and place of birth,
phone number, email address, picture of the person concerned
Legal basis for data processing: identification of the user as a customer and contact with him/her
the data subject's consent, pursuant to Article 6(1) GDPR.
Duration of data processing Until the registration of the person concerned is deleted or, in the case of a camera recording, if the recording is not used, it is deleted 10 working days after the recording
- If the recording has been requested by the Company not to be deleted by justifying a right or legitimate interest, but the request is not made, it will be deleted 30 days after the request.
Persons entitled to access the data The company provides customer service and billing
your colleagues.
Data transmission:
None
Data processors:
LIGET MÁSZÓSPORT Kft. uses Gympro Administration software for the access to which you register
some of the data you enter will be included.

The privacy notice is available on the following page:
https://ligetboulder.hu/website/resources/privacy-policy-hun.pdf

6.2. **DATA PROCESSING DURING CONTACT**

The company can be contacted through various communication channels, e.g. email, telephone, social media. When contacted by phone, the conversation is not audio-recorded.
Purpose of data processing: to serve people interested in the company's services, to answer their questions
answering questions, maintaining contact.
Data processed: personal data provided when contacting us are typically: name, email address, phone number
Legal basis for processing: the data subject's consent, pursuant to Article 6(1)(a) of the GDPR.
As contact is always initiated by the data subject, your personal data will be
is deemed to be voluntary and consent to the processing is given.
Duration of processing: until the question is answered.
Persons entitled to access the data: the company's customer service staff
employees
Data transmission: none
Data processors: none

6.3. **COOKIE MANAGEMENT**
Cookies are short text files consisting of letters and numbers that are stored by the user
visited online stores are downloaded to your computer, mobile device or other device
your browser. The cookie is between the user's device and the server hosting the website or a third party
can be installed based on a request sent to your server. Cookies are divided into 3 main groups
we can list:

Required cookies:
In order to ensure the correct functioning of the webshop, cookies must be
we use. We call cookies necessary, without which the webshop would not be able to
to function properly.
The necessary cookies may control, for example, the following functions:
- whether or not to display the login page to the visitor again
- wishlist list of products
- the current language of the shop, which can be set by the customer
- etc.

Statistical cookies:
Statistical cookies collect information about how our visitors use our website. They are
cookies cannot accurately identify the user. The information collected by statistical cookies
information includes page views, clicks, session length, the number of
date of visit, etc.

Marketing cookies:
Marketing cookies help us to provide you with a more pleasant browsing experience on the
webshop for your visitors, including personalised offers and ads
by displaying.

The Data Controller informs the persons entering and using the climbing room as data subjects that images and video footage may be taken of them and that these may be used for marketing purposes.

By accepting this information, the persons using the climbing room accept the terms of this clause. The data subject may specifically request the controller in writing to refrain from using and publishing the images.

7. **INFORMATION ON THE RIGHTS OF DATA SUBJECTS**

The right to information and access to the personal data processed:

The data subject shall have the right to receive feedback from the controller on.
whether his or her personal data are being processed and, if so, whether he or she is entitled to
to have access to your personal data and the following information:
a) the purposes of the processing;
b) the categories of personal data concerned;
(c) the recipients or categories of recipients with whom or with which the personal data are
have been or will be disclosed, including in particular to third country recipients, or
international organisations;
(d) where applicable, the envisaged duration of the storage of the personal data or, if this is not
possible, criteria for determining this period;
(e) the right of the data subject to obtain from the controller the processing of personal data relating to him or her
rectification, erasure or restriction of the processing of such personal data, and may object to the processing of such personal data
against the treatment of;
(f) the right to lodge a complaint with a supervisory authority;
(g) where the data have not been collected from the data subject, any available information concerning their source.
information;
h) the fact of automated decision-making, including profiling, and at least in these
cases, clear information about the logic used and how such
the significance of the processing and the likely impact on the data subject
has consequences.
If the transfer of personal data to a third country or an international organisation
the data subject is entitled to be informed of the transfer by the appropriate
guarantees.
The Data Controller shall provide the data subject with a copy of the personal data subject to processing.
provides. For any additional copies requested by the data subject, the Data Controller shall, at the administrative cost.
may charge a reasonable fee based on. If the data subject has submitted the request electronically,
the information is provided by the Controller in a commonly used electronic format
available, unless the data subject requests otherwise.
The right to request a copy referred to in the preceding paragraph shall not adversely affect the right of others
your rights and freedoms.

Right of rectification:

The Data Controller shall, at the request of the data subject, provide inaccurate personal data relating to the data subject without justification.
correct it without delay. Having regard to the purposes of the processing, the data subject shall have the right to.
ask for your incomplete personal data, including by means of a supplementary declaration, to be
the addition of.

Right to erasure ("right to be forgotten"):

If one of the following grounds applies, the data subject has the right to obtain, at his or her request, the following.
The controller to delete personal data concerning him or her without undue delay:
a) the personal data are no longer necessary for the purposes for which they were collected or for other
have been treated in a way that;
(b) the data subject withdraws the consent on the basis of which the processing was carried out and the processing is
has no other legal basis;
(c) the data subject objects to the processing and there are no overriding legitimate grounds for the processing or where the processing would be related to direct marketing;
d) the personal data have been unlawfully processed;
(e) the personal data are processed in accordance with the legal or regulatory requirements applicable to the controller under Union or Member State law
must be deleted in order to fulfil the obligation;
f) the collection of personal data by information society services
was made in connection with the offer.
The erasure of data cannot be initiated if the processing is necessary:
a) for the exercise of the right to freedom of expression and information;
(b) the Union or Member State law applicable to the controller which provides for the processing of personal data
or in the public interest;
(c) for preventive health or occupational health purposes, the worker
assessment of your ability to work, medical diagnosis, medical or social
providing care or treatment, or health or social systems and services
under EU or national law, or with a health professional, to manage
under a contract and the processing of those data by a professional or by a professional
under the responsibility of a person authorised by Union or Member State law or by the competent
the professional rules laid down by the competent bodies in the Member States
is bound by confidentiality, or by another person who is also an EU citizen
or in national law or by the competent bodies in the Member States
is bound by the obligation of professional secrecy laid down in the rules;
d) for reasons of public interest in the field of public health, such as serious cross-border
protection against health threats or health care, medicines and
ensure the high quality and safety of medical devices, and to ensure that EU
or under national law, which provides for appropriate and specific measures to
safeguards to protect the rights and freedoms of the data subject, in particular professional secrecy about;
(e) on the basis of the public interest in the field of public health and the processing of such data in such a way that
is carried out by or under the responsibility of a professional who is a member of the EU or a Member State
laid down by law or by the competent bodies in the Member States
is subject to the obligation of professional secrecy laid down in the rules, or
by any other person who is also authorised or empowered by EU or national law or
the confidentiality rules laid down by the competent national bodies
is subject to;
f) archiving for public interest, scientific and historical research purposes or statistical purposes,
where the right of erasure would be likely to make it impossible or seriously impair
would jeopardise that processing1; or
(g) for the presentation, exercise or defence of legal claims.

Right to restriction of processing:
At the request of the data subject, the Data Controller shall restrict processing if one of the following conditions applies.
is met:a) the data subject contests the accuracy of the personal data, in which case the restriction is limited to the
for a period allowing the data subject to check the processing of personal data
accuracy;
(b) the processing is unlawful and the data subject opposes the erasure of the data and requests instead that the data be
restrictions on the use of;
(c) the Controller no longer needs the personal data for the purposes of processing, but the personal data
the data subject needs them for the establishment, exercise or defence of legal claims; or
(d) the data subject, in relation to processing by the controller of personal data based on the public interest or legitimate interest
objected to the processing; in this case, the restriction applies for the period during which
it is not established whether the legitimate grounds of the controller override those of the data subject against legitimate grounds.
If the processing is restricted on the basis of the above, the storage of such personal data shall be
except with the consent of the data subject or for the establishment or exercise of legal claims
or the defence or protection of the rights of another natural or legal person, or
The important public interest of the Union or of a Member State may be served.

The Data Controller shall inform the data subject whose request it has limited the processing on the basis of the above, of the following.
inform you in advance of the lifting of the restriction on processing.

Right to data portability:
The data subject shall have the right to obtain from the Data Controller the information concerning him or her which he or she has made available to the Data Controller.
receive personal data in a structured, commonly used, machine-readable format,
and the right to transfer these data to another controller without the need to.
would be prevented by the controller to whom the personal data have been disclosed if:
(a) the processing is based on consent or on a contract; and
(b) the processing is carried out by automated means.
In exercising the right to data portability as set out above, the data subject shall have the right to.
- if technically feasible - request direct communication of personal data between data controllers
the transmission of.
The exercise of the right to data portability must not prejudice the right to erasure ("right to be forgotten").
That right shall not apply where the processing is in the public interest or where the processing is in the
a task carried out in the exercise of official authority vested in the controller
necessary to implement.
The right to data portability must not adversely affect the rights and freedoms of others.

Right to object:
The data subject shall have the right to object at any time, on grounds relating to his or her particular situation, to the processing of personal data
against the processing of their data by the Controller, where the legal basis for the processing is the public interest or the
The performance of a task carried out in the exercise of official authority vested in the controller,

or the need to pursue the legitimate interests of the Controller or a third party, including
profiling based on those provisions. In this case, the Data Controller may use the personal data
may no longer process the data, unless it can demonstrate that there are compelling reasons for not doing so.
justified by legitimate reasons which override the interests, rights and freedoms of the data subject
against your freedoms, or which could give rise to legal claims or
are related to the protection of.
If personal data are processed for direct marketing purposes, the data subject is entitled to,
to object at any time to the processing of personal data concerning him or her for these purposes, including
profiling, if it is related to direct marketing. If the data subject objects to the
the processing of personal data for direct marketing purposes, the personal data
may no longer be processed for this purpose.
If the processing of personal data for scientific or historical research purposes or statistical purposes
the data subject has the right to object, on grounds relating to his or her particular situation, to the
the processing of personal data concerning you, unless the processing is carried out for a reason of public interest.
is needed to carry out the task.

Right of withdrawal:
The data subject shall have the right to obtain, where the processing of personal data by the controller is based on the data subject's consent.
you may withdraw your consent at any time. Withdrawal of consent shall not affect the validity of the
the lawfulness of the processing prior to the withdrawal.

Procedure in the event of a request from a data subject concerning the exercise of the above rights:
The Controller shall, without undue delay and in any event from the receipt of the request.
inform the data subject within one month (30 days) of the rights set out in this notice.
measures taken following a request from a data subject concerning the exercise of his or her rights. If necessary,
taking into account the complexity of the application and the number of requests, this deadline is extended by two months
can be extended.
The Data Controller shall inform the applicant of the extension of the time limit, stating the reasons for the delay.
within one month of receipt of the information. If necessary, taking into account

taking into account the complexity of the application and the number of requests, this deadline is extended by two additional months (60 days)
can be extended. If the person concerned has submitted the request by electronic means, the information
will be provided electronically where possible, unless the data subject requests otherwise.
If the Data Controller does not take action on the data subject's request without delay, but
inform the person concerned, at the latest within one month of receipt of the request, of the
the reasons for non-action and that the person concerned may lodge a complaint with a
the supervisory authority and exercise your right of appeal to the courts.
The Data Controller shall provide the requested information and data free of charge, subject to the following conditions
the request is manifestly unfounded or excessive, in particular because of its repetitive nature, the
Subject to the controller providing the requested information or information or taking the requested action
charge a reasonable fee for the administrative costs of making the decision, or

may refuse to act on the request.
The Controller shall inform each recipient of any rectification it has made,
erasure or restriction of processing of personal data by or with whom or to which the personal data have been disclosed, except,
if this proves impossible or requires disproportionate effort. At the request of the person concerned, the
The Data Controller will inform you about these recipients.
Any questions you may have about your personal data stored in the system and data management, please send your request to our e-mail address. Please keep in mind that your personal data
we can only provide you with information about the processing of your personal data in your interest give or take action if you have provided credible proof of your identity.
We will always need the following information to respond to your request:

· the email address you entered when registering

· full name

· billing addresses

Please make sure to send your request from the email address you provided when registering.

8. **DATA SECURITY MEASURES**

The Data Controller and the server network operator shall store the data on the reasonably accessible with state-of-the-art hardware and software support, in particular to protect against unauthorised access,
alteration, transmission, disclosure, deletion or destruction,
and against accidental destruction or damage, thus ensuring data security. The
Data processed by the Controller shall, as a general rule, only be processed by the Controller in accordance with these Rules
its employees and other contributors involved in the achievement of specific processing purposes who are covered by their employment contract or employment relationship,
and their other contractual relations, the provisions of the law or of the Data Controller
are under an obligation of professional secrecy in respect of all information they have received.
All processing activities of the Data Controller must be accurately documented. The Data Controller shall.
all data management activities it carries out (e.g. newsletter, webshop, employees
register) must keep records. The Data Controller shall verify the lawfulness of the transfer of data keeps a register of data flows for the purpose of monitoring and informing the data subject, which include the date of transfer of the data processed, the legal basis, the recipient, the scope of the data other data specified in the legislation providing for the processing.

8.1. **SECURITY OF PERSONAL DATA PROCESSED ON PAPER**

In order to ensure the security of personal data processed on paper, the Data Controller shall take the following measures
apply:
- the data can only be accessed by those authorised to do so, and can no longer be accessed by others. are not disclosed to the public,
- the documents are kept in a well-closed, dry place with fire and property protection equipment on the premises,
- only the competent authorities have access to documents in active permanent management,
- the staff member handling the data may only leave such premises during the day,
where data processing is taking place, to lock the data media entrusted to it or close the office,
- if the personal data processed on paper are digitised, the Data Controller shall use the

applies the security rules that govern digitally stored documents and requires
and from your data processors.

8.2. **SECURITY OF PERSONAL DATA STORED DIGITALLY**

To ensure the security of personal data stored on computers or networks, the Data Controller, the take the following measures:

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

· provides ongoing virus protection on the network that handles personal data,

· prevent, by using the available computer tools and their application
unauthorised persons from accessing the network

9. Rules on camera surveillance

The Company will use the electronic surveillance system to interfere with the privacy of data subjects only to the extent necessary. The Company operates its own cameras at its headquarters, in which case the Company is the data controller. Both the live and recorded images at the Company's headquarters are handled by the Company's managing director.

The Company does not conduct electronic surveillance for any reason or in any way:

- for the purpose of monitoring the work intensity of a worker,
- with the aim of influencing the behaviour of employees at work,
- in sensitive areas, especially changing rooms, showers and toilets,
- in an area where workers spend their rest or break time, in particular in a rest room or designated smoking area,
- in a public place.

However, the Company may conduct electronic monitoring to ensure that employees and visitors comply with the provisions applicable to them in order to ensure that they work safely and without endangering health and that the climbing room is used by visitors in accordance with its intended purpose.

The Company grants the data subject the right, if his or her right or legitimate interest is affected by the recording, to request that the data not be destroyed or erased by the controller within the time limit for erasure of the recording set out above, by providing evidence of his or her right or legitimate interest. The Company shall decide on the request as soon as possible. The record thus indicated shall be saved and handed over to the person responsible for data management, who shall ensure that it is kept in accordance with the data protection and data security rules set out in this Policy. At the request of a court or other authority, the recorded recording shall be sent to the court or authority without delay. If no request is made within thirty days of the request not to destroy the recording, the recording shall be deleted.

An information notice on data processing has been prepared to inform data subjects in advance of the processing. Information pictograms are displayed at all entry points to the monitored area. The blocking of camera images may only be ordered by the person designated to supervise the data processing carried out by the Company's camera system.

Initiate camera image blocking

- a person with a right of access to the Company, if, during the inspection of the recordings, he or she discovers circumstances that jeopardise the purpose of the electronic surveillance system,
- anyone whose right or legitimate interest is affected by the recording.

The blocking is decided as soon as possible by the person designated to supervise the processing of the data by the Company's camera system (in agreement with the Data Protection Officer, if appointed or delegated).

The Company shall keep a record of all blocking of images captured by the camera, stating the time of viewing and blocking, the purpose of the blocking, the event giving rise to the blocking and the indication of the further use.

10 . **DATA SECURITY INCIDENT**

Data breach: a breach of security that could result in the loss of data transmitted, stored or otherwise processed
accidental or unlawful destruction, loss or alteration of personal data,
unauthorised disclosure of, or access to, personal data.
If the data breach is likely to result in a high risk to the rights of natural persons
and freedoms, the Data Controller shall, without undue delay and in a clear and comprehensible manner
inform the data subject of the personal data breach.
The data subject need not be informed if any of the following conditions are met:
(a) the controller has implemented appropriate technical and organisational security measures and these measures have been
measures have been applied to the data affected by the personal data breach, in particular
the measures, such as the use of encryption, that are applied to personal data
make the data unintelligible to persons who are not authorised to access it;
(b) the controller has taken further measures following the personal data breach which.
ensure that the high risk to the rights and freedoms of the data subject is no longer
is unlikely to happen;
c) the information would require a disproportionate effort. In such cases, the data subjects shall
shall be communicated by means of publicly disclosed information or similar measures,
which ensures that stakeholders are informed in an equally effective way.

11 . **REMEDIES**

a) The Data Controller can be contacted with any questions or comments related to data management at the following address.
You can contact us using one of the contact details provided in the Information Notice.
b) The National Authority for Data Protection and Freedom of Information (postal address: 1374 Budapest, Pf.
603., phone: +36-1-391-1400, email: ugyfelszolgalat@naih.hu, website: www.naih.hu) by appointment
initiate an investigation on the grounds that your personal data are being processed
is suffering or is in imminent danger of suffering damage to his or her rights; or
(c) The data subject may take the Data Controller to court in the event of a breach of his or her rights. The court may
is acting out of turn in a case. The compliance of the processing with the law is verified by the

The controller has the burden of proof. The tribunal shall have jurisdiction to hear the case. The lawsuit - the
at the choice of the person concerned, in the courts for the place where he or she is domiciled or resident
may be brought before the court of the place of residence or domicile.

Before lodging a complaint with the supervisory authority or the courts, please consult the following and in order to solve the problem as quickly as possible - contact us at
using one of the contact details.