Privacy Policy

The Balaton Fishing Kft. (Registered office: 8242 Balatonudvari Balaton u. 8. hereinafter referred to as the "Data Controller"), as the
www.kisleshegy.hu domain name (hereinafter referred to as the "Website") hereby publishes information on the processing of data within the framework of the services available on the Website and other services provided by the Data Controller.
Users accessing the Website (hereinafter referred to as "User") agree to all the terms and conditions set out in this Privacy Policy (hereinafter referred to as "Policy"), and are therefore kindly requested to read this Policy carefully before using the Website.

1. THE DATA CONTROLLER'S INFORMATIONS

The data controller is Balaton Fishing Korlátolt Felelősségű Társaság.

Registered office: 8242 Balatonudvari Balaton u. 8.
E-mail address: info@kisleshegy.hu
Phone: +36-30-686-5488
Tax number: 23857755-2-19
Company registration number: 12-09-009178

2. INFORMATION ON DATA PROCESSING

Reservation of accommodation

Scope of data processed:
On the booking interface available on the Website, the User has the possibility to provide his/her data in order to book a room in the accommodation operated by the Data Controller (hereinafter: Accommodation booking).

Reservation, the following personal data may be provided (data marked with * are mandatory):

- full name*;

- e-mail address*;

- telephone number*;

- number of nights*;

- billing details (billing name, billing address)*;

- number and name of guests*.

Purpose of data processing: the purpose of data processing is the administration of room reservations, the contact with the User and the registration and performance of the contract for the use of accommodation services.

Duration of data processing: the Data Controller shall process the necessary data for 5 (five) years after the booking of the accommodation in order to enforce the claims and rights arising from the contract between the User and the Data Controller pursuant to Section 6:22 of Act V of 2013 on the Civil Code. In order to comply with the retention obligation of the Data Controller, the Data Controller shall retain the name and address of the User on the accounting voucher for a period of 8 years, solely for the purpose of fulfilling the accounting obligation, pursuant to Section 169 of Act C. on Accounting (hereinafter: Accounting Act).

The legal basis of processing. The legal basis for the processing of accounting documents is the statutory provision imposing mandatory data processing, i.e. Section 169 of the Accounting Act.

Only persons over the age of 18 are entitled to submit data on the Website. Users may only provide their own personal data on the Website. If they do not provide their own personal data, the data provider is obliged to obtain the consent of the data subject.

3. RANGE OF PERSONS ENTITLED TO ACCESS PERSONAL DATA, DATA PROCESSING

The Data Controller and its Data Processors are entitled to access personal data in accordance with applicable law.

The data are processed by the following processors acting on behalf of the Data Controller:

3 in 1 Hosting Bt.,
Address: 2310 Szigetszentmiklós, Dévai utca 10/A
e-mail: admin@megacp.com

The Data Controller reserves the right to involve additional data processors in the future, which it will inform Users of by amending this Notice.

In the absence of an express legal provision, the Data Controller shall only disclose personally identifiable data to third parties with the express consent of the User concerned.

4. USER RIGHTS

Access to personal data

The Data Controller shall, upon the User's request, inform the User whether the Data Controller is processing his or her personal data and, if so, provide access to the personal data and inform the User of the following information:
- the purpose(s) of the processing;
- the types of personal data concerned by the processing;
- where the User's personal data are transferred, the legal basis and recipient(s) of the transfer;
- the envisaged duration of the processing;
- the rights of the User in relation to the rectification, erasure and restriction of processing of personal data and to object to the processing of personal data;
- the possibility of recourse to the Authority;
- the source of the data;
- relevant information on profiling;
- the names and addresses of the data processors and their activities in relation to the processing.

The Data Controller shall provide the User with a copy of the personal data subject to processing free of charge. For additional copies requested by the User, the Controller may charge a reasonable fee based on administrative costs. If the User has made the request by electronic means, the information shall be provided in a commonly used electronic format, unless the data subject requests otherwise.

The controller shall, without undue delay and at the latest within one month of the request

in an intelligible form at the request of the User. The User may submit a request for access using the contact details specified in point 1.

Correction of processed data

The User may request the Controller (using the contact details specified in point 1) to correct inaccurate personal data or to complete incomplete data, considering the purpose of the processing. The Controller shall carry out the rectification without undue delay.

Erasure (right to be forgotten), blocking of processed data

The User may request that the Data Controller delete personal data concerning him or her without undue delay and the Data Controller shall be obliged to delete personal data concerning the data subject without undue delay if one of the following grounds applies:

(a) the personal data are no longer necessary for the purposes for which they were collected or otherwise processed;
(b) the User withdraws his or her consent and there is no other legal basis for the processing;
c) the User objects to the processing of his or her personal data;
(d) the processing of the personal data is unlawful;
(e) the personal data must be erased in order to comply with a legal obligation under Union or Member State law to which the controller is subject;
(f) the personal data were collected on the basis of consent in connection with the provision of information society services to children.

If the Data Controller has disclosed (made available to third parties) the personal data and is obliged to delete it pursuant to the above, it shall take reasonable steps and measures, taking into account the available technology and the cost of implementation, to inform the data controllers that process the personal data concerned that the User has requested them to delete the links to the personal data in question or a copy or duplicate of such personal data.

Personal data need not be deleted where processing is necessary:

- for the exercise of the right to freedom of expression and information;
- to comply with an obligation under Union or Member State law to which the controller is subject to which the processing of personal data is subject or to carry out a task carried out in the public interest or in the exercise of official authority vested in the controller;
- in the public interest in the field of public health;
- for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, where a legitimate interest in erasure would probably make such processing impossible or seriously jeopardise it; or
- for the establishment, exercise, or defence of legal claims.

Restrictions on data processing

The User is entitled to have the Data Controller restrict the processing of personal data instead of rectifying or erasing it, if one of the following conditions is met:

- the User contests the accuracy of the personal data, in which case the restriction shall apply for the period of time necessary to allow the Controller to verify the accuracy of the personal data;
- the processing is unlawful and the User opposes the erasure of the data and requests instead that its use be restricted;
- the Controller no longer needs the personal data for the purposes of processing but the User requires them for the establishment, exercise or defence of legal claims; or
- the User has objected to the processing; in this case, the restriction shall apply for a period of time until it is established whether the legitimate grounds of the controller prevail over the legitimate grounds of the data subject.

If the processing is subject to restriction, such personal data shall, with the exception of storage, only be processed by the User or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or of an important public interest of the Union or of a Member State.
The Data Controller shall inform the User at whose request the processing has been restricted in advance of the lifting of the restriction on processing.

Obligation to notify the rectification or erasure of personal data or restriction of processing

The Data Controller shall inform any recipient to whom or with which the personal data have been disclosed of the rectification, erasure, or restriction of processing of the personal data, unless this proves impossible or involves a disproportionate effort. Upon request, the Controller shall inform the User of these recipients.

Right to data portability
The User has the right to receive personal data concerning him/her that he/she has provided to the Data Controller in a structured, commonly used, machine-readable format and to transmit such data to another data controller. If the User requests, the Controller may export the processed data in PDF and/or CSV format.

Right to object
The User may object to the processing of his or her personal data if the processing.
- is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller;
- necessary for the purposes of the legitimate interests pursued by the Controller or a third party;
- based on profiling.

In the event of the User's objection, the Controller may no longer process the personal data, unless the User proves that the processing is justified by compelling legitimate grounds which override the interests, rights and freedoms of the User or are related to the establishment, exercise or defence of legal claims.
Where personal data are processed for direct marketing purposes or for profiling purposes, the User has the right to object at any time to the processing of personal data concerning him or her for such purposes. If the User objects to the processing of personal data for direct marketing purposes, the personal data may no longer be processed for such purposes.

Action by the Data Controller in relation to the User's request
The Data Controller shall inform the User without undue delay, but no later than one month from the receipt of the request, of the measures taken following the request for access, rectification, erasure, restriction, objection and portability. If necessary, taking into account the complexity of the request and the number of requests, this time limit may be extended by a further two months. The Data Controller shall inform the User of the extension of the time limit, stating the reasons for the delay, within one month of receipt of the request. If the User has submitted the request by electronic means, the information shall be provided by electronic means where possible, unless the data subject requests otherwise.

If the Data Controller does not take action on the User's request, it shall inform the User without delay and at the latest within one month of receipt of the request of the reasons for the failure to act and of the right to lodge a complaint with a supervisory authority and to seek judicial remedy.

At the User's request, the information, the information and the action taken on the basis of the request shall be provided free of charge. If the User's request is manifestly unfounded or excessive, in particular because of its repetitive nature, the controller shall, subject to the provision of the information or information requested or

the administrative costs of providing the requested action, the Controller may charge a reasonable fee or refuse to act on the request. The burden of proving that the request is manifestly unfounded or excessive shall lie with the Controller.

5. DATA SECURITY

The Data Controller undertakes to ensure the security of the data, to take technical and organisational measures and to establish procedural rules to ensure that the data recorded, stored, or processed are protected and to prevent their destruction, unauthorised use or unauthorised alteration. It also undertakes to require all third parties to whom it transfers or discloses data based on the consent of the Users to comply with the requirement of data security.

The Data Controller shall ensure that the processed data cannot be accessed, disclosed, transmitted, modified or deleted by unauthorised persons. The processed data may only be accessed by the Data Controller and its employees or by a Data Processor engaged by it, and shall not be disclosed by the Data Controller to any third party not entitled to access the data.

The Data Controller shall make every effort to ensure that the data are not accidentally damaged or destroyed. The Data Controller shall require its employees involved in data processing activities to comply with such obligations.

The User acknowledges and accepts that, in the event of providing his/her personal data on the Website, even though the Data Controller has state-of-the-art security measures in place to prevent unauthorised access to or disclosure of the data, the data cannot be fully protected on the Internet. In the event of unauthorised access or disclosure of data despite our efforts, the Controller shall not be liable for any such acquisition or unauthorised access or for any damage suffered by the User as a result thereof. In addition, the User may also provide personal data to third parties who may use it for unlawful purposes or in unlawful ways.

Under no circumstances will the Data Controller collect sensitive data, i.e. data concerning racial or ethnic origin, membership of national or ethnic minorities, political opinions or party affiliations, religious or philosophical beliefs, membership of political organisations, health, medical conditions, pathological addictions, sex life or criminal records.

6) HANDLING AND REPORTING OF DATA BREACHES

A personal data breach is any event that results in the unlawful processing or treatment of personal data processed, transmitted, stored or handled by the Data Controller, in particular unauthorised or accidental access, alteration, disclosure, deletion, loss or destruction, accidental destruction or accidental damage to personal data.

The Data Controller shall notify the NAIH of a personal data breach without undue delay and no later than 72 hours after becoming aware of the personal data breach, unless the Data Controller can demonstrate that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. If the notification cannot be made within 72 hours, the notification shall state the reason for the delay and the required information may be provided in detail without further undue delay. THE NAIH

shall include at least the following information:
- the nature of the personal data breach, the number and category of data subjects and personal data;
- Name and contact details of the controller;
- the likely consequences of the personal data breach;
- the measures taken or envisaged to manage, prevent or remedy the personal data breach.

The Data Controller shall inform the data subjects of the data breach within 72 hours of the discovery of the data breach through the Data Controller's website. The notification shall contain at least the information specified in this point.

The Data Controller shall keep records of the personal data breach for the purposes of monitoring the measures taken in relation to the personal data breach and informing the data subjects. The register shall contain the following data:

- the scope of the personal data concerned; the scope and number of data subjects;
- the date of the personal data breach;

- the circumstances and effects of the personal data breach;
- the measures taken to remedy the personal data breach.

The Data Controller shall keep the data contained in the register for 5 years from the date of the data breach.

7) ENFORCEMENT OPTIONS

The Data Controller will make every effort to ensure that the processing of personal data is carried out in accordance with the law, however, if the User feels that this is not the case, he/she may write to the contact details specified in point 1.

If the User feels that his or her right to the protection of personal data has been infringed, he or she may, in accordance with the applicable legislation, seek redress from the competent bodies

National Authority for Data Protection and Freedom of Information (address: 1055 Budapest, Falk Miksa utca 9-11.; ugyfelszolgalat@naih.hu; www.naih.hu) at the court.

8) OTHER PROVISIONS

This Information Notice is governed by Hungarian law, in particular the provisions of Act CXII of 2011 on the Right of Informational Self-Determination and Freedom of Information, Act CVIII of 2001 on certain aspects of electronic commerce services and information society services, and Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Regulation (EC) No 95/46/EC (27 April 2016).

2022.03.16., Budapest