
PRIVACY POLICY

Hévízi Turisztikai Nonprofit Kft.

Privacy and data protection policy

1. The purpose and scope of the policy

- (1) The purpose of this Privacy Policy (hereinafter referred to as the "**Policy**") is to determine the legal purpose of the use of records/databases managed by **Hévízi Turisztikai Nonprofit Kft.** (hereinafter referred to as "**Data Controller**"), and to ensure compliance with the constitutional principles of data protection, the rights to informational self-determination and data security requirements, and to ensure that everyone has the right to own personal data within the framework of the law, and to learn the circumstances of the handling of data, and to prevent unauthorized access, alteration and unauthorized disclosure of data. In addition, this Policy provides information for the data subjects by presenting the Data Controller's data management practices.
- (2) The scope of this Policy covers the processing of personal and special data held by all institutional units of the Data Controller.

2. Governing legislation

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, hereinafter referred to as "**GDPR**")
- Act CXII of 2011 on informational self-determination and freedom of information (hereinafter referred to as "**Infotv.**")
- Act V of 2013 on the Civil Code (hereinafter referred to as "**Ptk.**")
- Act CXXX of 2016 on the Code of Civil Procedure (hereinafter referred to as "**Pp.**")

3. The data of the Data Controller

The Data Manager's current data are as follows:

- Name: Hévízi Turisztikai Nonprofit Kft.
- Company seat: 8380 Hévíz, Rákóczi u. 2.
- Company registry number: 20-09-071334
- Tax registration number: 23141823-2-20
- Registry court: Court of County Zala
- Phone: 06/83/540-070
- E-mail: office@hevizmarketing.hu

4. The scope of personal data handled, the purpose, duration and title of the data management

- (1) Data Controller's data management is performed on the basis of voluntary consent of the data subjects or on the basis of legal authorization. In the case of voluntary consent, the data subject may, at any time, request information on the scope of data processed and on the ways how these data are used, and may withdraw his/her consent, excluding specific cases where the data processing is performed on the basis of a legal obligation (in such cases, the Data Controller shall provide information on the further processing of the data to the data subject).
- (2) Data providers are required to provide all the data under their best efforts and accurately.
- (3) If the data provider does not provide his/her personal data, the data provider is obliged to obtain the consent of the data subject.
- (4) If the Data Controller transfers the data to data processors or other third parties, the Data Controller shall keep records of these. The data transfer record shall contain the addressee, the method, the date and the scope of data transmitted.
- (5) Data management concerning certain activities of the Data Controller:

a. Complaint handling

Legal basis for data management: consent of the data subject

The scope of data processed: name, email address, phone number, and address

The purpose of data management: complaint handling

Data transfer: none

Legal basis for data transfer: not relevant

Data processors: not relevant

Deadline for deletion of data: 5 years

The possible consequences of the failure of communication of data: failure of the service

b. Webshop customers

Legal basis for data management: contractual obligation

The scope of data processed: name, email address, phone number, and address

The purpose of data management: delivery of products ordered

Data transfer: via an IT system

Legal basis for data transfer: contractual obligation

Data processors: Csaba Nagymihály - Municipality of Hévíz Town
Barbara Prémecz - Hévíz TDM Association

Deadline for deletion of data: 5 years

The possible consequences of the failure of communication of data: failure of the service

c. Inquiry for accommodation:

Legal basis for data management: consent of the data subject
The scope of data processed: name, email address, phone number, and address
The purpose of data management: offering rates
Data transfer: via an IT system
Legal basis for data transfer: contractual obligation
Data processors: Csaba Nagymihály - Municipality of Hévíz Town
Attila Joós - Webmark Europe Kft.
Deadline for deletion of data: 6 months
The possible consequences of the failure of communication of data: failure of the service

d. Reserving accommodation:

Legal basis for data transfer: contractual obligation
The scope of data processed: name, email address, phone number, and address
The purpose of data management: providing accommodation
Data transfer: via an IT system
Legal basis for data transfer: contractual obligation
Data processors: Csaba Nagymihály - Municipality of Hévíz Town
Attila Joós - Webmark Europe Kft.
Deadline for deletion of data: 5 years
The possible consequences of the failure of communication of data: failure of the service

e. Newsletter subscribers

Legal basis for data management: consent of the data subject
The scope of data processed: name, email address, phone number, and address
The purpose of data management: providing information
Data transfer: via an IT system
Legal basis for data transfer: contractual obligation
Data processors: Csaba Nagymihály - Municipality of Hévíz Town
Attila Joós - Webmark Europe Kft.
Deadline for deletion of data: within 24 hours following the withdrawal of the consent of the data subject
The possible consequences of the failure of communication of data: failure of the service

f. Private accommodation adverts

Legal basis for data transfer: contractual obligation
The scope of data processed: name, email address, phone number, and address
The purpose of data management: accommodation-advertising service
Data transfer: via an IT system
Legal basis for data transfer: contractual obligation
Data processors: Csaba Nagymihály - Municipality of Hévíz Town
Attila Joós - Webmark Europe Kft.
Deadline for deletion of data: 5 years
The possible consequences of the failure of communication of data: failure of the service

g. Contracts of employment

Legal basis for data management: legal obligation

The scope of data processed: name, mother's name, place and date of birth, address, national insurance number, and bank account number

The purpose of data management: ensuring the payment of wages and contributions

Data transfer: Szám-Tan'77 Bt.

Legal basis for data transfer: contractual obligation

Data processors: Gergely Vecsera

Deadline for deletion of data: 1 year after the termination of the contract

The possible consequences of the failure of communication of data: failure in paying wages and contributions

h. Logging the Data Manager's website

Legal basis for data management: consent of the data subject

The scope of data processed: anonymised IP address

The purpose of data management: production of statistics

Data transfer: Google, Municipality of Hévíz Town

Legal basis for data transfer: consent of the data subject, contractual obligation

Data processors: Csaba Nagymihály - Municipality of Hévíz Town

The possible consequences of the failure of communication of data: no consequences

Data management of external service providers associated with logging:

i. Cookie management on the Data Manager's website - by type

Session and permanent cookies

Legal basis for data management: consent of the data subject

The scope of data processed: IP address, location

The purpose of data management: production of statistics, remarketing, webshop data management

Data transfer: Google, Municipality of Hévíz Town, MediaGum Kft.

Legal basis for data transfer: consent of the data subject, contractual obligation

Data processors: Csaba Nagymihály - Municipality of Hévíz Town

The competent employee of MediaGum Kft.

Deadline for deletion of data: Data management is provided until the termination of the contract between the data controller and the hosting (server) provider, or until the date when the data subject's request for cancellation is addressed to the hosting (server) provider.

The possible consequences of the failure of communication of data: webshop registration data will not be stored

Third-party cookies

Legal basis for data management: consent of the data subject

The scope of data processed: IP address, location

The purpose of data management: production of statistics, remarketing

Data transfer: Google, Municipality of Hévíz Town

Legal basis for data transfer: consent of the data subject, contractual obligation

Data processors: Csaba Nagymihály - Municipality of Hévíz Town
Deadline for deletion of data: Data management is provided until the termination of the contract between the data controller and the hosting (server) provider, or until the date when the data subject's request for cancellation is addressed to the hosting (server) provider.

The possible consequences of the failure of communication of data: no consequences

Web camera streaming

Data Controller streams a live webcam image at <http://www.heviz.hu/hu/webkamera>, where images are updated every 3 seconds. The place of recording: Festetics Square, Hévíz

A warning sign informs the passers-by about the streaming of images on the spot.

The camera images are not recorded.

The name of the company providing the web camera services: ONLINECAMERA BT., contact information:

<https://onlinecamera.net/kapcsolat>

5. Rights and remedies of the data subjects

- (1) Data subjects may request information from the Data Controller at any time in writing about the way their personal data are managed, may indicate their need for cancellation or modification, and may withdraw their previously granted consent at the contact details provided in Section 3.
- (2) Data subjects may not exercise their right of cancellation in case of mandatory data processing required by law.
- (3) **Content of the right to information:** Based on the data subject's request, the Data Controller shall provide the data subject with the information listed in Articles 13 and 14 of the GDPR on the processing of personal data, and the guidance under Articles 15-22 and 34 in a concise, comprehensible form.
- (4) **Content of the right of access:** At the request of the data subject, the Data Controller shall provide information on whether the data controller is processing any data associated with the data subject. If the Data Controller is processing data on the data subject, the data subject is entitled to access:
 - a. The personal data relating to him/her;
 - b. the purpose(s) of data management;
 - c. the categories of personal data involved;
 - d. the persons with whom the data of the data subject have been or will be communicated;
 - e. the duration of data storage;
 - f. the right to rectify, cancel and limit data management;
 - g. the right to apply to a court or a supervisory authority;
 - h. the source of the data processed;

- i. profiling and/or automated decision making, or details of their application, practical effects;
 - j. transmission of the data processed to a third country or to an international organization.
- (5) In the case of a data request as described above, the Data Controller shall provide the data subject with a copy of the data he/she manages in accordance with the request. Upon request, it is possible to ask the Data Controller to send the requested information by electronic means.
- (6) For each additional copy, the Data Controller requests an administration fee of HUF 500 a page.
- (7) The deadline for submitting the requested data is 30 days from the receipt of the request.
- (8) **Right to rectification:** The data subject may request the correction of inaccurate data, relating to him/her, managed by the Data Controller.
- (9) **Right of cancellation:** If any of the following reasons apply, the Data Controller shall delete the data relating to the data subject as soon as possible, but not later than five working days:
 - a. The data was unlawfully processed (without legal authorization or personal consent);
 - b. data management is unnecessary for the original purpose;
 - c. the data subject withdraws his/her consent for data management and the Data Controller has no other legal basis for data management;
 - d. the data in question were collected in connection with the provision of information society services;
 - e. personal data must be deleted in order to fulfil the legal obligations of the Data Controller.
- (10) Data deletion cannot be performed by Data Controller if data management is required for any of the following:
 - a. Additional data management is required to comply with the legal requirements for the Data Controller;
 - b. the exercise of the right to freedom of expression and information;
 - c. public interest;
 - d. archiving, scientific, research or statistical purposes;
 - e. enforcing or protecting legal claims.
- (11) **The right to restrict processing of data:** If any of the following reasons apply, the Data Controller limits the data management at the request of the data subject:
 - a. The data subject contests the accuracy of the data relating to him/her. In this case, the restriction refers to the time during the accuracy and correctness of the data in question is reviewed credibly;

- b. data processing is unlawful, but the data subject omits deletion and only requests a restriction on data management;
 - c. data is no longer needed for data management, but the data subject requests them to be retained for the purpose of enforcing or protecting his/her legal needs;
- (12) If the Data Controller introduces a restriction on any data managed, the Data Controller will only handle the data concerned for the duration of the limitation, if:
- a. The data subject gives his/her consent to it;
 - b. it is necessary to enforce or defend legal claims;
 - c. it is necessary to enforce or protect the rights of another person;
 - d. it is necessary to validate public interest.
- (13) **The right to withdraw consent:** The data subject is entitled to withdraw the consent given to the Data Controller at any time in writing. In the event of such a request, the Data Controller shall immediately and permanently delete any data that has been handled in relation to the data subject, and the further storage of which is not required by law or is not required to enforce or protect legitimate interests. The withdrawal shall not affect the legality of data management performed until the withdrawal of the consent.
- (14) **The right to data portability:** The data subject is entitled to request the Data Controller to transmit the data relating to him in a commonly used computer-readable format to another data controller. The Data Controller will execute the request as soon as possible, but not later than 30 days.
- (15) **Automated decision making and profiling:** The data subject has the right not to be subject to a decision based solely on automated data management (e.g. profiling) that would have a legal effect on him/her or would otherwise adversely affect him/her. This entitlement is not applicable if:
- a. data management is essential for the conclusion or performance of a contract between the data subject and the Data Controller;
 - b. the data subject expressly agrees to use such a procedure;
 - c. its application is permitted by law;
 - d. it is necessary to enforce or protect legal claims.

6. Contacts

Upon contacting the Data Controller, the Data Controller stores the e-mail and its contents (especially the sender's name, address, date, and attachments) for five years and then deletes them.

7. The way and provision of data storage

- (1) The Data Controller archives the data he/she manages in paper form at its headquarters, stores the data of the current year at the accounting department , and in electronic form on the computers operating at its headquarters, and in the case of hévíz.hu on the server (Server owner: Municipality of Hévíz, server location: Budapest, Hungary).
- (2) Exceptions to paragraph (1) are the data stored at the data processors of the Data Controller, the place of storage of which is located at the headquarters of the data processors.
- (3) For its operation, Data Controller uses an IT system that ensures that:
 - a. the accuracy and consistency of data is verified (data integrity);
 - b. the authenticity of the data is assured (authenticity of data management);
 - c. the data are accessible to those entitled (availability);
 - d. the data are protected against unauthorized access (data confidentiality).
- (4) Data protection covers, in particular:
 - a. unauthorized access;
 - b. modification;
 - c. transmission;
 - d. deletion;
 - e. disclosure;
 - f. accidental damage;
 - g. accidental data loss;
 - h. or becoming inaccessible due to the change in the technology used.
- (5) In order to protect the electronically managed data, the Data Controller uses a solution providing an appropriate level of security in the state of the art. When assessing compliance, particular emphasis is placed on the extent of risk arising from data management at the Data Controller. IT protection ensures that stored data cannot directly be attributable to or linked to data subjects (unless permitted by law).
- (6) In the course of data management, the Data Controller ensures that:
 - a. the person authorized can have access to the data when s/he needs it;
 - b. only those who are authorised can have access to data;
 - c. the accuracy and completeness of the data and the processing method is protected.
- (7) Data Controller and his/her data processors, if used, always provide protection against fraud, espionage, viruses, burglary, vandalism, and natural disasters affecting their IT systems. Data Controller (and data processor) uses server-level and application-level security procedures.
- (8) Messages forwarded to the Data Controller over the Internet, in any form, are subject to network threats that lead to information modification, unauthorized access, or other

illegal activities. However, to prevent such threats, the Data Controller will do everything that is reasonably practicable and can be expected from the state of the art. To this end, the systems used are monitored to record security deviations, to obtain evidence of a security incident and to investigate the effectiveness of precautions.

8. Procedural rules

- (1) If the Data Controller receives an application under Articles 15 to 22 of the GDPR, the data controller shall inform the data subject in writing as soon as possible and not later than 30 days of the action taken on the request.
- (2) If the complexity of the application or other objective circumstances justifies it, the above deadline may be extended once, up to a maximum of 60 days. The Data Controller shall notify the data subject in writing of the extension of the deadline, together with the appropriate justification for the extension.
- (3) The Data Controller provides the information free of charge unless:
 - a. the person concerned repeatedly requests information/measures on essentially unchanged content;
 - b. the application is clearly unfounded;
 - c. the request is exaggerated.
- (4) In the cases referred to in paragraph (3), the Data Controller is entitled to:
 - a. refuse the application;
 - b. make the execution of the request subject to payment of a reasonable fee.
- (5) If the applicant requests the transfer of data on paper or on an electronic media (CD or DVD), the Data Controller shall provide a copy of the relevant data free of charge in the requested manner (unless the chosen means poses technically disproportionate difficulties). The Data Controller charges an administration fee of HUF 500 a page / CD-DVD for each additional copy.
- (6) The Data Controller shall notify any person with whom the data concerned has previously been disclosed about any rectification, cancellation or restriction that has been made unless it is impossible to provide the information or it requires a disproportionate effort.
- (7) If requested by the data subject, the Data Controller provides information about the persons to whom the data of the data subject have been transmitted.
- (8) The data controller shall respond to the request in electronic form, unless:
 - a. the data subject asks for the answer in a very different way and it does not cause unreasonably high extra costs for the Data Controller;
 - b. the Data Controller does not know the electronic contact details of the data subject.

9. Damages

- (1) If any person suffers material or non-material damage as a result of a breach of data protection legislation, he/she is entitled to claim compensation from the Data Controller and/or the data processor. If the Data Controller and Data Processor(s) are involved in committing the violation, they are jointly and severally liable for the damage.
- (2) The data processor shall be liable for damages incurred only if he or she has violated the provisions of the relevant data protection legislation specifically designed for data processors or if the damage has been caused by non-observance of the Data Controller's instructions.
- (3) The Data Controller and any data processors are only liable if they cannot prove that they are not responsible for the event or circumstance that caused the damage.

10. Remedies

- (1) If the data subject considers that his/her rights have been violated by the Data Controller and/or data processors, he/she is entitled to apply to the **court** with jurisdiction in accordance with the Civil Procedure Code. The court shall accord priority treatment to the case.
- (2) If the data subject wishes to complain about data management, he/she can do so at the National Authority for Data Protection and Freedom of Information. Contact details: headquarters: 1125 Budapest, Szilágyi Erzsébet fasor 22 / C.; mailing address: 1530 Budapest, P.O. Box: 5., Phone: 00 36-1/391-1400; fax: 00 36-1/391-1410; e-mail address: ugyfelszolgalat@naih.hu; website: www.naih.hu.

11. Administrative cooperation

- (1) The Data Controller, when receiving a formal request from the authorized authorities, shall provide the specified personal data on a mandatory basis.
- (2) The Data Controller shall only transmit data in the cases referred to in paragraph (1) which are strictly necessary for the purpose specified by the requesting authority.

Done: In Hévíz, 22nd May 2018

Table of contents

1.	The purpose and scope of the policy	1
2.	Governing legislation.....	1
3.	The data of the Data Controller	1
4.	The scope of personal data handled, the purpose, duration and title of the data management ..	2
5.	Rights and remedies of the data subjects	5
6.	Contacts.....	7
7.	The way and provision of data storage	8
8.	Procedural rules	9
9.	Damages	10
10.	Remedies	10
11.	Administrative cooperation.....	10