

# Privacy Notice

**Hungarian Tourism Agency Ltd.** (Magyar Turisztikai Ügynökség Zrt., address: 1027 Budapest, Kacska u. 15-23, postal address: 1525 Budapest P.O. Box: 97, central phone number: +36 1 488 8722, central e-mail address: info@mtu.gov.hu , represented by László Könnyid, DPO contact: Levente Papp, e-mail address: privacy@mtu.gov.hu) (hereinafter: Agency, Data controller) is committed to respecting the rights of the visitors of its website (hereinafter: Website) to privacy and the protection of their personal data and proceeding during its operation in compliance with the General Data Protection Regulation of the European Union (hereinafter: GDPR), the Hungarian Privacy Act (hereinafter: Infotv.) and the other legal regulations, guidelines and the established data protection practice, by also taking into account the most important international recommendations on data protection.

**The Agency as Data Controller, considers the contents of this legal notice binding. It undertakes to ensure that all data processing related to its services meets the requirements set out in this notice and in all applicable legislation.**

## **THE PROCESSING ACTIVITIES OF THE AGENCY ARE IN COMPLIANCE WITH THE FOLLOWING LEGAL REGULATIONS ON DATA PROTECTION**

- Regulation of the European Parliament and of the Council (EU) 2016/679 (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, GDPR);
- Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information (Infotv.);
- Act V of 2013 on the Civil Code (Ptk.);

### **Personal data may be processed, if**

- the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract,
- processing is necessary for compliance with a legal obligation to which the controller is subject;
- processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- 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;

- is necessary for the enforcement of the legitimate interests of the Controller or a third party.

Pursuant to Article 8 (1) of the GDPR, statements of consent of data subject minors over the age of 16 shall be considered valid without the permission or subsequent approval of their legal representative, while statements of consent of data subject minors below the age of 16 are not valid without the consent of the party exercising parental supervision over the minor. The Agency has no tools to verify the accuracy and validity of the consent, its accuracy is warranted by the person granting consent.

## **THE PURPOSE OF DATA PROCESSING**

The purpose of the data processing is to ensure the safe use and secure technical operation of the Website, as well as its control.

We also wish to inform you that in relation to the functions linked through the icons of external providers shown on the Website (Facebook, Twitter, LinkedIn, Instagram) the Agency does not perform any processing activities, as in such cases the controller is the external company providing the service.

## **LAWFULNESS OF PROCESSING DATA**

Data related to the secure technical operation of the Website, including the IP address of the visitors, are processed on the legal basis of legitimate interest.

## **SCOPE OF PROCESSED DATA**

During the operation of the Website, we store the IP address of the visitors (Data Subjects) and the approximate geographical location that can be inferred from it as technical data; operating system type, features and version number; browser type and version number; activity on the Website; the exact time of the visit; time spent on the Website; the use of a function or service used on the Website; we can also create cookies on the Data Subject's device.

## **DURATION OF STORAGE OF PERSONAL DATA**

Data related to the secure technical operation of the website, including the IP address of the visitors, will be kept for 1 year.

## **RECIPIENTS OF PERSONAL DATA AND RECIPIENT CATEGORIES**

The users of the Agency and the Data Processors maintaining partner relationships and providing customer services and, in the case of technical data, the IT staff members.

## DATA PROCESSORS

The Agency uses the following services of data processor companies for different tasks:

- RENDSZERINFORMATIKA KERESKEDELMI ÉS SZOLGÁLTATÓ ZRT. (Székhely: 1134 Budapest, Váci út 19. IV. em., Cégjegyzékszám: 01-10-046912)
- VISIT HUNGARY NEMZETI TURISZTIKAI SZERVEZET NONPROFIT ZRT. (Székhely: 1037 Budapest, Bokor utca 23-25., Cégjegyzékszám: 01-10-049807)

## USE OF COOKIES

Similarly to other commercial websites, the Agency also uses the general technology known as cookies and webserver technical log files in order to obtain information about how the data subjects use the Website.

With the help of the cookies and webserver log files, the Agency can control the visits to the Website and adjust its contents to your personal need. A cookie is a small information package (file) which often carries an anonymised individual ID. When you visit a website, the website asks your computer to store that file in a part of the hard disc of your computer which is expressly used to store cookies. Each individual website you visit can send a cookie to your computer if the settings of your browser allow it. However, in order to protect your data, your browser will only allow the particular website to access only the cookie that the particular website sent to your computer, i.e., one website cannot have access to cookies embedded by other websites. In general, the browsers are configured to accept cookies. However, if you do not wish to accept cookies, you can set up your browser to reject their acceptance. In that case, some components of the website may not function effectively when you browse on it. The cookies cannot obtain other information from the hard disc of your computer and do not carry viruses.

The website uses the following cookies:

Name	Service	Purpose	Expiry	Type
_ga	<a href="#">Google</a>	Records a unique identifier, which is used by the system to compile statistics on the user's visiting habits on the website	2 years	HTTP
_ga_#	<a href="#">Google</a>	Records a unique identifier, which is used by the system to compile statistics on the user's visiting habits on the website	2 years	HTTP

For more information visit:

[https://support.google.com/analytics/topic/2919631?hl=hu&ref\\_topic=1008008](https://support.google.com/analytics/topic/2919631?hl=hu&ref_topic=1008008)

## **SAFETY OF THE DATA PROCESSED BY US**

The Agency arranges for creating backups that are suitable according to the IT data and the technical environment of the Website. The backups are stored according to the criteria applicable to the retention period of the specific data and, thereby guaranteeing the availability of data during the retention period, after which they will be finally destroyed. The IT system and the integrity and operability of the environment storing the data are checked with advanced monitoring techniques and the required capacities are provided constantly. The events of the IT environment are registered with complex logging functions, thus ensuring subsequent detectability and legal proof of any data breach. We use a high broadband, redundant network environment to serve our websites, with which any load can be safely distributed among the resources. The disaster tolerability of our systems is scheduled and guaranteed, and we use organisational and technical instruments to guarantee high-level business continuity and constant services to our users. The controlled installation of security patches and manufacturer updates that also ensure the integrity of our information systems is a key priority, thus preventing, avoiding and managing any access or harmful attempt involving the abuse of vulnerability.

We apply regular security tests to our IT environment, during which the detected errors and weaknesses are corrected because enhancing the security of our information system is a continuous task.

High-security requirements are also set for our staff, which also include confidentiality, and compliance with which is ensured with regular training. During our internal operation, we try to use well designed and controlled processes. Any personal data breach detected during our operation or reported to us is investigated transparently, with responsible and strict principles within 72 hours. The actual data breaches are all processed and recorded. During the development of our services and IT solutions we arrange for complying with the principle of installed data protection, as data protection is a priority requirement even in the design phase.

## **INFORMATION REGARDING THE RIGHTS OF THE DATA SUBJECTS**

The data subject may request information on the processing of their personal data, the rectification of their personal data and may also request the erasure of their personal data, with the exception of processing required by law.

### **Right to prior information**

The data subject has the right to obtain information regarding the facts and information about the processing, prior to its start. One of the reasons why this Privacy Notice was created was to guarantee that right.

### **Access right**

The data subject may request the Agency to:

- confirm the processing of their personal data;
- provide a copy of such data;
- provide information about their personal data, including especially the data recorded by the Agency and the purpose of their use, the parties with whom these data are shared, whether the data are transferred abroad and the method used to protect such data, the duration of storage of the data and the manner and form of submitting complaints and, finally, the source from which the agency obtained the data of the data subject.

### **Right to rectification**

The data subject may request the Agency to rectify or supplement inaccurately or incompletely recorded personal data. Prior to the rectification of any erroneous data, the Agency may inspect the authenticity and accuracy of the data subject's data.

### **Right erasure, right to be forgotten**

The data subject may request the erasure of their personal data when:

- the specific data are no longer required for the processing purposes specified when the data were collected; or
- when the data subject has withdrawn consent (if processing is based on consent); or,
- when the data subject exercises the right to objection; or,

The Agency is not obliged to fulfil the data subject's request for the erasure of their personal data when the processing of the personal data is necessary and justified for the following reasons:

- to comply with statutory obligations; or
- to enforce or protect the law or legitimate interest in court.
- Right to restrict processing (right of blocking)

### **Data portability**

The data subject may request the Agency to transfer their personal data to the party concerned in an orderly, transparent manner, legible also for information systems and to transfer the data directly to a different controller.

### **Right to object**

For reasons relating to their own situation, the data subject may object to the processing of their personal data at any time when they believe that it is required to exercise their fundamental rights. The data subject may object to the processing of their personal data for

direct marketing purposes at any time, without providing any reasoning, in which case the Agency terminates the processing within the shortest possible time.

#### **Right to withdraw consent**

The data subject can withdraw consent at any time if no other legal ground of processing applies. The withdrawal of consent does not affect the lawfulness of prior processing.

#### **Information to the data subject on any potential personal data breach**

The Agency protects the personal and other data of the data subject in compliance with the applicable laws and regulations and in proportion to the risks, uses an advanced and reliable IT environment and selects its co-operation partners with special care. It performs its internal processes in a regulated and supervised manner in order to prevent or avoid even the smallest error, problem or incident occurring during the processing of personal data and to detect, inspect and manage any event that may still happen.

If an incident relating to personal data still occurs provenly and it is likely to impose a high risk to the rights and freedoms of the data subjects, the agency undertakes to inform the data subject and the data protection authority about the personal data breach in a manner and providing the information specified in the effective data protection regulations, without any unreasonable delay.

#### **Automated individual decision-making, including profiling**

The data subject has the right to excuse themselves from the force of resolutions which are based exclusively on automated processing (including profiling) and would have an effect on them or would affect them in any other way of similarly significant extent. The Agency does not operate any procedure during which it applies automated decisions.

#### **Right to lodge a complaint with a supervisory authority**

Complaints about processing may be submitted to the Hungarian National Authority for Data Protection and Freedom of Information (NAIH):

Registered office: H-1055 Budapest, Falk Miksa utca 9-11.

Postal address: H-1363 Budapest, PO box.: 9.

Phone: (+36 1) 391-1400

Fax: +36 (1) 391-1410

E-mail: [ugyfelszolgalat@naih.hu](mailto:ugyfelszolgalat@naih.hu)

#### **Right to an effective judicial remedy against a supervisory authority**

Without prejudice to any other administrative or non-judicial remedy, each natural or legal

person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.

**Right to an effective judicial remedy against a controller or processor**

Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant (to GDPR. Article 77), each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation.

This notice is effective from 22 May 2024.