PRIVACY NOTICE

18-11-2021 New York

HUNGARIAN TOURISM AGENCY LTD. (registered office: Hungary, 1027 Budapest, Kacsa utca 15-23, hereinafter: Agency, Data Controller), in this case as DATA CONTROLLER, is committed to respecting the rights of the Data Owners 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.

When you accept this privacy notice by registering to our event in context of the GINOP-1.3.5-15-2015-00001 project, promoting Hungarian tourism (18-11-2021 New York, hereinafter: Event), you represent and warrant that you have read and expressly agreed to this version of this document, and you agree to give your consent to processing of your personal data.

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 Ageny will store your personal data on the servers of the Data Controllers and Data Processors.

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 2013on the Civil Code (Ptk.);

1. THE DATA CONTROLLERS

NAME OF DATA CONTROLLER:
HUNGARIAN TOURISM AGENCY LTD. (MAGYAR TURISZTIKAI ÜGYNÖKSÉG ZRT., Registration number: 01-10-041364, Registered office: Hungary, 1027 Budapest, Kacsa utca 15-23., Tax number: 10356113-4-41, Represented by: dr. Zoltán Guller)
POSTAL ADDRESS OF DATA CONTROLLER: H-1027 Budapest, Kacsa utca 15-23.
EMAIL ADDRESS OF DATA CONTROLLER: info@mtu.gov.hu
PHONE NUMBER OF DATA CONTROLLER: +36 1 488 8700
DATA PROTECTION OFFICER: Levente Papp, privacy@mtu.gov.hu

2. DATA PROCESSORS CONCERNED

Data Controller cooperates the following service provider company as concerned Data Processor:
Visit Hungary National Tourism Organisation Ltd. (reg.number: 01-10-049807, tax number: 26338783-4-41, reg.office: 1037 Budapest, Bokor utca 23-25., represented by: Ákos Kristó)

Roxer Kommunikációs Ügynökség Korlátolt Felelősségű Társaság (reg.number: 01-09-958482, tax number: 13354921-2-43, reg.office: 1114 Budapest, Bartók Béla út 35. 5 em. 2/b)

Trumarketing (reg.office: 66 Chandler Drive Wayne, NJ, USA, 07470, tax number: 82-3986617)

The Data Processors will not use the personal data for their own purposes, they only process data for the Data Controller.

3. THE SCOPE OF PROCESSED DATA

The requested data from foreign partners during the registration are the following: surname and first name; company name; position; e-mail address. The event is opened for the press, so video and photo may also can be recorded of you by press and other companies.

4. THE PURPOSE OF DATA PROCESSING

The Agency may manage your personal data for the following purposes:

- the Agency will use the personal data provided by you during the online registration to identify and ensure your participation on the Event.
- the Agency may invite you to other events in the future.
- the Agency may take photos of the event, photos of the participants, which may be used later for project documentation and event marketing purposes.
- the Agency may organize Lucky Draws.

5. DURATION TO STORE YOUR PERSONAL DATA:

The Data Controller handles the personal data of the Data Subject until the withdrawal of the consent.

6. LAWFULNESS OF PROCESSING DATA:

Data Subject has given consent to the processing of his or her personal data for one or more specific purposes, GDPR Art. 6, 1. a).

7. RECIPIENTS OF YOUR PERSONAL DATA AND RECIPIENT CATEGORIES:

The personal data provided by you can be accessed by the direct employees of Data Controller and Data Processors, so that they can perform their job-related tasks. These employees will process the data in accordance with the law and internal rules in a confidential manner. The Event is a press public event.

8. 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.

RIGTH TO WITHDRAW CONSENT

The Data Subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the Data Subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

RIGHT ERASURE, RIGHT TO BE FORGOTTEN:

The Data Subject may request the erasure of their personal data.

RIGHT TO RESTRICT PROCESSING (RIGHT OF BLOCKING):

The Data Subject may request a restriction of the processing of their personal data (blocking of data).

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 OBJECTION:

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.

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.

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.

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:
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

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 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.

9. 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.

10. COMMUNICATION OF A PERSONAL DATA BREACH

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the Data Subject without undue delay. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.