PRIVACY NOTICE

TOURISM SUMMIT 2019

This Privacy Notice (hereinafter: Notice) pertains to the processing activities performed by MAGYAR TURISZTIKAI ÜGNYÖKSÉG ZRT. as well as the companies established by it: KISFALUDY2030 TURISZTIKAI FEJLESZTŐ NONPROFIT ZRT., TURISZTIKAI ÉS MARKETINKGKOMMUNIKÁCIÓS NONPROFIT ZRT., MAGYAR DIVAT ÉS DESIGN ÜGYNÖKSÉG NONPROFIT ZRT. and EXPO 2020 MAGYARORSZÁG NONPROFIT KFT. (hereinafter: Companies, Controllers), and it contains all information relating to the processing of personal data so that you are fully aware, before providing your personal data and your consent, of the purpose and conditions of the data processing, the risks and guarantees related thereto, and your rights. Participation in the event is subject to the provision of the consent, and to the transfer of personal data required for the registration and liaison with the Controllers.

By providing your personal information and by registering, you represent that you have become aware of and expressly accept the version of this Notice in effect at the time of such provision of data or information, and that you consent to the processing of such data.

Our Companies store personal information provided by you on servers operated by the Controllers and the Processors.

The purpose of this Privacy Notice is to ensure that our Companies comply with the provisions of 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 (hereinafter: GDPR) and of Act CXII of 2011 on Informational Self-Determination and Freedom of Information (hereinafter: Privacy Act). Our Companies aim to provide the Data Subject with each individual piece of information regarding the processing of personal data in a concise, transparent, intelligible and easily accessible form, using clear and plain language, and to facilitate the exercise of the Data Subject’s rights.

|  |
| --- |
| **1. CONTROLLERS AND THEIR CONTACT DETAILS:** |
|  |
| **NAME OF CONTROLLER1:** |
| Magyar Turisztikai Ügynökség Zrt. (company registration number: 01-10-041364, registered seat: H-1027 Budapest, Kacsa utca 15-23, tax number: 10356113-2-41, represented by: Dr. Zoltán Guller) |
| MAILING ADDRESS OF THE CONTROLLER: H-1027 Budapest, Kacsa utca 15-23 |
| E-MAIL ADDRESS OF THE CONTROLLER: info@mtu.gov.hu |
| PHONE NUMBER OF THE CONTROLLER: +36 1 488 8700 |
| NAME AND CONTACT DETAILS OF THE DATA PROTECTION OFFICER (DPO): Levente Papp, privacy@mtu.gov.hu |
| **NAME OF CONTROLLER2:** |
| Turisztikai Marketingkommunikációs Ügynökség Nonprofit Zrt. (company registration number: 01-10049807, tax number: 26338783-4-41, registered seat: H-1027 Budapest, Kacsa utca 15-23, represented by:  Eszter Osváth) |
| MAILING ADDRESS OF THE CONTROLLER: H-1027 Budapest, Kacsa utca 15-23 |
| E-MAIL ADDRESS OF THE CONTROLLER: info@tmu.hu |
| PHONE NUMBER OF THE CONTROLLER: +36 1 488 8700 |
| NAME AND CONTACT DETAILS OF THE DATA PROTECTION OFFICER (DPO): Levente Papp, privacy@mtu.gov.hu |
| **NAME OF CONTROLLER3:** |
| Magyar Divat & Design Ügynökség Nonprofit Zártkörűen Működő Részvénytársaság (company registration number: 01-10-049808, tax number: 26338972-4-41, registered seat: H-1027 Budapest, Kacsa utca 15-23, represented by: Zsófia Bata-Jakab) |
| MAILING ADDRESS OF THE CONTROLLER: H-1027 Budapest, Kacsa utca 15-23 |
| E-MAIL ADDRESS OF THE CONTROLLER: info@mddu.hu |
| PHONE NUMBER OF THE CONTROLLER: +36 1 488 8700 |
| NAME AND CONTACT DETAILS OF THE DATA PROTECTION OFFICER (DPO): Levente Papp, privacy@mtu.gov.hu |
| **NAME OF CONTROLLER4:** |
| Kisfaludy2030 Turisztikai Fejlesztő Nonprofit Zártkörűen Működő Részvénytársaság (company registration number: 01-10-140072, tax number: 25869628-4-42, registered seat: H-1146 Budapest, Hermina út 63, represented by: Erzsébet Mihály) |
| MAILING ADDRESS OF THE CONTROLLER: H-1146 Budapest, Hermina út 63 |
| E-MAIL ADDRESS OF THE CONTROLLER: info@kisfaludy2030.hu |
| PHONE NUMBER OF THE CONTROLLER: +36 1 488 8700 |
| NAME AND CONTACT DETAILS OF THE DATA PROTECTION OFFICER (DPO): Levente Papp, privacy@mtu.gov.hu |
| **NAME OF CONTROLLER5:** |
| EXPO 2020 Magyarország Nonprofit Korlátolt Felelősségű Társaság (company registration number: 01-09341681, tax number: 26742832-2-41, registered seat: H-1027 Budapest, Kacsa utca 15-23, represented by: Andrea  Tóth) |
| MAILING ADDRESS OF THE CONTROLLER: H-1027 Budapest, Kacsa utca 15-23 |
| E-MAIL ADDRESS OF THE CONTROLLER: info@expo2020.hu |
| PHONE NUMBER OF THE CONTROLLER: +36 1 488 8700 |
| NAME AND CONTACT DETAILS OF THE DATA PROTECTION OFFICER (DPO): Levente Papp, privacy@mtu.gov.hu |

|  |
| --- |
| **2. PROCESSORS USED:** |
| In carrying out its data processing activities, the Company uses the services of the following companies as processors: |
| HD COMMUNICATION KORLÁTOLT FELELŐSSÉGŰ TÁRSASÁG (registered seat: H-1025 Budapest,  Józsefhegyi utca 28, D. ép. 2. em. 1, company registration number: 01-09-179471)  TRENDENCY ONLINE Alkalmazásfejlesztő Zártkörűen Működő Részvénytársaság (H-1094 Budapest, Mihálkovics utca 10, company registration number: 01-10-04727)  RENDSZERINFORMATIKA KERESKEDELMI ÉS SZOLGÁLTATÓ Zártkörűen Működő Részvénytársaság (registered seat: H-1134 Budapest, Váci út 19, IV. em., company registration number: 01-10046912)  The Processors will not use the data received for their own purposes, but will only perform the processing of the data for the Controllers. |

|  |
| --- |
| **3. PURPOSE OF PROCESSING:** |
| The Controllers shall process the individual personal data of the Data Subject for the purposes of and in connection with the following objectives:  To facilitate participation in the Tourism Summit 2019 event, and to ensure the maintenance of professional liaison. |

|  |
| --- |
| **4. SCOPE OF PERSONAL DATA PROCESSED:** |
| Your last name and first name, company name, title, e-mail address and phone number.  Our event is a public press event where photos and videos may be taken/recorded of you. |

|  |
| --- |
| **5. DURATION OF PROCESSING:** |
| We will process your personal information until your consent is revoked. |

|  |
| --- |
| **6. LEGAL BASIS OF PROCESSING:** |
| The legal basis of data processing is your consent. According to Article 6 (1) (a) of the GDPR. |

|  |
| --- |
| **7. RECIPIENTS OF PERSONAL DATA AND CATEGORIES OF THE RECIPIENTS:** |
| The personal data you provide will be accessible to the Controllers and to the associates under the direct authority of the Controllers for the performance of their duties, who will manage the data in a confidential manner and in accordance with the laws, regulations and policies applicable at any time by the Controllers and Processors. Recordings made of you at our public press events may appear on various media platforms. |

|  |
| --- |
| **8. RIGHTS OF THE DATA SUBJECT** |
| Your rights regarding data processing include: |
| **RIGHT TO PRIOR INFORMATION:** |
| You have the right to be informed of facts and information relating to the data processing prior to the commencement of processing. We have created this Privacy Notice in order to assure this right. |
| **RIGHT OF ACCESS BY THE DATA SUBJECT:** |
| The Data Subject shall have the right to obtain from the Controllers confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and information: |
| **RIGHT TO RECTIFICATION:** |

|  |
| --- |
| The Data Subject may request that the Company rectify or complete any personal information of the Data Subject that is incorrect, inaccurate or incomplete. Prior to rectifying any incorrect data, the Company is entitled to verify the truthfulness or accuracy of such data. |
| **RIGHT TO ERASURE (“RIGHT TO BE FORGOTTEN”):** |
| The Data Subject shall have the right to obtain from the Controller the erasure of personal data concerning him or her without undue delay and the Controllers shall be obliged to do so.  You shall not have this right if the processing is based on a legal obligation. |
| **RIGHT TO WITHDRAWAL:** |
| If the processing is based on your consent, you have the right to withdraw your consent at any time without affecting the lawfulness of processing based on consent before its withdrawal. |
| **RIGHT TO RESTRICTION OF PROCESSING (RIGHT TO BLOCK DATA):** |
| The Data Subject has the right to request Controllers to restrict data processing in certain cases. |
| **RIGHT TO DATA PORTABILITY:** |
| The Data Subject shall have the right to receive personal data relating to him or her which he or she has made available to the Controllers in a structured, widely used, machine-readable format. |
| **RIGHT TO OBJECT:** |
| The Data Subject shall have the right to object at any time to the processing of his or her personal data on grounds relating to his/her particular situation if such processing is in the public interest or it is necessary to pursue the legitimate interests of the Controllers, including profiling. |
| **AUTOMATED DECISION-MAKING IN INDIVIDUAL CASES INCLUDING PROFILING:** |
| The Data Subject shall have the right not to be subject to a decision based solely on automated processing – including profiling – which produces legal effects concerning him or her or similarly significantly affects him or her. The Companies do not employ automated decision-making. |
| **COMMUNICATION OF A PERSONAL DATA BREACH TO THE DATA SUBJECT** |
| When the personal data breach is likely to result in a high risk to your data and/or to your rights and freedoms, the Controllers shall communicate the personal data breach to you without undue delay. |
| **RIGHT TO LODGE A COMPLAINT WITH A SUPERVISORY AUTHORITY:** |
| You shall have the right to lodge a complaint with a supervisory authority if you consider that the processing of personal data relating to you infringes the data protection regulations.  National Authority for Data Protection and Freedom of Information  Registered seat: H-1125 Budapest, Szilágyi Erzsébet fasor 22/c  Postal address: H-1534 Budapest, Pf.: 834  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:** |
| You shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning you. |
| **RIGHT TO AN EFFECTIVE JUDICIAL REMEDY AGAINST A CONTROLLER OR PROCESSOR:** |
| You shall have the right to an effective judicial remedy where you consider that your rights have been infringed as a result of the processing of your personal data in non-compliance with the law. |

|  |
| --- |
| **9. DATA SECURITY MEASURES** |
| The Companies are committed to ensuring the security of the data, and to taking technical and organisational measures and establishing procedures to ensure that the data recorded, stored or processed are protected or prevented from being destroyed or subjected to unauthorised use or unauthorised changes. The Companies shall also instruct their Processors to comply with the data security requirements.  The Controllers shall ensure that no unauthorised person has access to the processed data, and that such persons may not disclose, transmit, modify or delete the data processed. The Controllers shall do their best to ensure that the data are not accidentally damaged or destroyed. The above commitment is stipulated by the Controllers also for the employees participating in the processing activities and for the Processors proceeding on behalf of the Controllers.  The Companies shall ensure that IT data and the technical environment of the website are appropriately backed up, using the parameters necessary based on the retention period of the individual data to guarantee the availability of the data within the retention period, and at the end of the retention period they shall permanently destroy the data.  The integrity and functionality of the IT system and the data storage environment are verified by advanced monitoring techniques, and the necessary capacities are continuously provided. |

Events in the IT environment are captured using sophisticated logging features to ensure that potential incidents can be subsequently detected and legally validated.

A redundant network environment providing consistently high bandwidth is used to serve web pages, which distributes the resulting load securely across resources.

Their systems are designed to provide planned disaster resilience, deliver business continuity and, consequently, continuous service to users at high standard also through organisational and technical means.

High priority is given to the controlled installation of security enhancements and manufacturers’ updates that also ensure the integrity of their IT systems, thus preventing, avoiding and managing attempts to access or damage the system via vulnerabilities.

The IT environment is regularly tested by security testing, errors or vulnerabilities identified are corrected, and IT system security reinforcement is seen as an ongoing task.

High standards of security, including confidentiality, are set for their employees, which they also ensure through regular training, and they strive to operate planned and controlled processes in their internal operations.

Any personal data breach detected or reported to them in the course of their operation shall be investigated in a transparent, responsible and strict manner within 72 hours. Data breaches that have occurred are addressed and recorded.

When developing their services and IT solutions, they ensure that the principle of data protection by design is met, and data protection is already a high priority requirement during the design phase.

|  |
| --- |
| **10. MANAGEMENT AND NOTIFICATION OF PERSONAL DATA BREACHES** |
| A personal data breach is an event that results in the unlawful handling or processing of personal data regarding the personal data managed, transmitted, stored or processed by the Controllers; thus, in particular, in unauthorised or accidental access to, alteration, communication, deletion, loss or destruction, and accidental destruction or damage of such personal data. Persons in charge of data protection shall promptly investigate any reported or detected personal data breach and, within 72 hours of becoming aware of the personal data breach, shall make a recommendation to remedy and address such breach.  The Controllers warrant that the data will be processed in full compliance with applicable legal provisions. |

If the terms of data processing change, the Companies shall inform the Data Subjects of such changes.

|  |
| --- |
| **11. PRIVACY STATEMENT** |
| By having been informed of the content of this Notice and by accepting the Notice, you, as the Data Subject of processing, after due estimation and consideration voluntarily consent to the recording and processing of your personal data by the Controllers for the purpose and for the period specified in this Notice.  The Controllers shall only be entitled to disclose the personal data of the Data Subject to the data processing companies that the Data Subject has become aware of and accepted on the basis of this Notice. |