

PRIVACY NOTICE

360 Design Budapest Exhibition online registration

HUNGARIAN FASHION AND DESIGN AGENCY LTD. (HFDA Ltd., registered office: Hungary, 1027 Budapest, Kacsá utca 15-23, central phone number: +36 1 488 8722, central e-mail address: info@hfda, central phone number: +36 30 302 6146, represented by Zsófia Jakab, DPO contact: Levente Papp, e-mail address: privacy@mtu.gov.hu, hereinafter: Agency, 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.

This Privacy Notice contains all information related to the processing of your personal data provided during your online registration in order to fully understand the purpose and conditions of the data processing, the risks, guarantees and your rights associated with it, before giving your personal data and consent.

Accepting this privacy notice when you sign up to 360 Design Budapest Exhibition (hereinafter: Event) at www.360dbp.com, you declare that you have carefully read and expressly agreed to this version of this document, and you (hereinafter: Data Subject) 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 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.);

1. THE DATA CONTROLLERS

NAME OF DATA CONTROLLER:

HUNGARIAN FASHION AND DESIGN AGENCY LTD. (MAGYAR DIVAT ÉS DESIGN ÜGYNÖKSÉG NZRT., Registration number: 01-10-049808, Office: 1027 Budapest, Kacsá utca 15-23., Tax number: 26338972-4-41, Represented by: Zsófia Jakab)

POSTAL ADDRESS OF DATA CONTROLLER: H-1027 Budapest, Kacsá utca 15-23.

EMAIL ADDRESS OF DATA CONTROLLER: info@hfda.hu

PHONE NUMBER OF DATA CONTROLLER: +36 30 302 6146

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:

- HUNGARIAN TOURISM AGENCY LTD. (reg. number: 01-10-041364, headoffice: 1027 Budapest, Kacsá utca 15-23., tax number: 10356113-4-41)
- MEDIATOR GROUP KFT. (headoffice: 1117 Budapest, Dombóvári út 25., reg. number: 01-09-864793,)

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 YOUR PERSONAL DATA

Name and e-mail address of the Data Subject for the registration or the newsletter subscription process.

4. THE PURPOSE OF DATA PROCESSING

The Data Controller handles certain personal data of the Data Subject for the purpose of ensuring participation and successful conduct of the Event, and also for communication in connection with the Event. In case of subscribing to the newsletter, the Data Controller processes the data of the Data Subject in order to ensure the possibility of sending newsletters on the basis of a separate express consent.

5. DURATION TO STORE YOUR PERSONAL DATA:

The Data Controller will delete the registration data of the Data Subject 30 days after participating in the Event. In case of subscribing to the newsletter, the data controller keeps a

record of the personal data processed in connection with it until the withdrawal of the consent.

6. LAWFULNESS OF PROCESSING DATA:

The lawfulness of processing data is your consent, Article 6. (1) a) of the GDPR, also in the case of event registration, and subscription to the newsletter.

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 control and process the data in accordance with the law and internal rules in a confidential manner. The event is open to the press, so members of the press may take photos of you within the framework of legal regulations and use them for the purpose of providing information and publicity about the event.

8. SECURITY OF DATA PROCESSED BY US

Our Companies are obliged to ensure data security, to take the technical and organisational actions as well as to work out the procedural rules ensuring that the collected, stored and processed data are protected; furthermore, they prevent the annihilation, the unauthorised usage and the unauthorised modification of such data. They also oblige their Processors to comply with the data security requirements.

The Controllers ensure that unauthorised persons may not access, disclose, forward, modify or erase the processed data. The Controllers do their best to ensure that the data is not damaged or destroyed, not even accidentally. The Controllers also impose the above obligation on their employees participating in data processing and on the processor(s) acting on behalf of the Controllers.

Our Companies ensure proper data backup according to the technical environment of the Website, which they operate with the necessary parameters based on the storage period of each data, thus guaranteeing the availability of the data within the storage period, and they finally erase them upon the expiry of the storage period.

The integrity and operability of the IT system and the data storage environment are checked with advanced monitoring techniques, and the necessary capacities are continuously provided.

Events in the IT environment are recorded by using complex logging functions, thus ensuring the subsequent detection and legal proof of potential incidents.

They use a redundant network environment that continuously provides high bandwidth to serve the websites, securely distributing the upcoming loads among our resources.

They ensure the planned disaster resilience ability of their systems, ensuring the continuity of business operations and thus the continuous service of users at a high level, with organisational and technical means.

Priority is given to the controlled installation of security patches and vendor updates that also ensure the integrity of IT systems, thus preventing, avoiding and addressing attempts to gain access or cause damage by exploiting vulnerabilities.

The IT environment is regularly inspected through security testing, any detected errors or vulnerabilities are corrected and supporting the security of the IT system is considered as an ongoing task.

They set high security standards for their employees that also include confidentiality, they ensure their fulfilment through regular training and strive to operate planned and controlled processes with regard to their internal operations.

Any incidents involving personal data detected or reported during operations are investigated in a transparent manner, in accordance with responsible and rigorous principles, within 72 hours. Incidents that have occurred are processed and recorded.

When developing their services and IT solutions they ensure that the principle of built-in data protection is met and data protection is treated as a priority already in the planning phase.

9. INFORMATION ABOUT THE RIGHTS OF DATA SUBJECTS

RIGHT TO TRANSPARENT INFORMATION:

You have the right to receive notification about the facts and information related to data processing prior to starting the data processing. We have also created this Privacy Notice to ensure this right.

RIGHT OF ACCESS BY THE DATA SUBJECT:

The Data Subject shall have the right to obtain from the Controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the following information:

- the processed personal data and the category of personal data, the purpose of data processing;
- the recipients or categories of recipient to whom the personal data have been, or will be disclosed by the Controller;
- the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period.

RIGHT TO RECTIFICATION:

The Data Subject may request the Company to rectify or complete any personal information that is incorrect, inaccurate or incomplete. Before rectifying the erroneous data, the Company may verify the truthfulness or accuracy of the data involved.

RIGHT OF WITHDRAWAL:

In the case of data processing based on the Data Subject's consent, the Data Subject may withdraw his/her consent at any time, which does not affect the lawfulness of data processing based on consent before the withdrawal.

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 Controller is obliged to do so. You do not have this right in the case of data processing based on a legal obligation.

RIGHT TO RESTRICTION OF PROCESSING (RETENTION RIGHT):

The Data Subject shall have the right to obtain from the Controller restriction of processing in the following cases:

- if the accuracy of the personal data is contested by the Data Subject, for a period enabling the controller to verify the accuracy of the personal data;
- if the processing is unlawful and the Data Subject opposes the erasure of the personal data and requests the restriction of their use instead;
- if the Controller no longer needs the personal data for the purposes of the processing, but they are required by the Data Subject for the establishment, exercise or defence of legal claims;
- if the Data Subject has objected to processing pending the verification whether the legitimate grounds of the Controller override those of the Data Subject.

RIGHT TO DATA PORTABILITY:

The Data Subject shall have the right to receive the personal data concerning him or her, which he or she has provided to the Controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where: The Data Subject shall have the right to data portability if:

- the processing is based on the data subject's consent or on the consent to processing specific categories of the personal data for one or more specific purposes, or on a contract pursuant to Article 6 (1) (b) GDPR, and
- the processing is carried out by automated means.

RIGHT TO OBJECT:

The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on GDPR point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

AUTOMATED INDIVIDUAL DECISION-MAKING, INCLUDING PROFILING:

The data subject should 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 otherwise significantly affects him or her. The Company does not use automated decision making.

COMMUNICATION OF A PERSONAL DATA BREACH TO THE DATA SUBJECT:

If a potential data breach is likely to pose a high risk to your data, rights and freedoms, the Controller will notify you about the data breach without undue delay.

RIGHT TO LODGE A COMPLAINT WITH A SUPERVISORY AUTHORITY:

In the event where the Data Subject suffered a harm concerning the processing of his or her personal data, it is advisable to contact the Controller before lodging the complaint and submit a request to exercise the relevant data subject's right in order to handle the matter more quickly and efficiently.

You shall have the right to complain to a supervisory authority if you consider that the processing of personal data violates the data protection laws.

National Authority for Data Protection and Freedom of Information

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

Mailing address: 1363 Budapest, Pf.: 9.

Phone number: +36 (30) 683-5969, +36 (30) 549-6838, +36 (1) 391 1400

Facsimile number: +36 (1) 391-1410

Official electronic address: Short name: NAIH, KR ID: 429616918

E-mail: ugyfelszolgalat@naih.hu

RIGHT TO AN EFFECTIVE JUDICIAL REMEDY AGAINST A SUPERVISORY AUTHORITY:

You have the right to an effective judicial remedy against a legally binding decision of the supervisory authority concerning you.

RIGHT TO AN EFFECTIVE JUDICIAL REMEDY AGAINST DATA CONTROLLERS OR DATA PROCESSORS:

Without prejudice to the right to lodge a complaint, the Data Subject shall have the right to an effective judicial remedy by instituting civil proceedings if, in his or her opinion, his or her rights have been violated as a result of the improper processing of his or her personal data. The Metropolitan Court has jurisdiction to hear the case, but the data subject may also choose to bring the case before the court having jurisdiction over his or her place of residence.

10. PROCESSING AND REPORTING DATA BREACHES

Data breach is any event that, in connection with personal data processed, transferred, stored or managed by the Controllers, results in the unlawful management or processing of personal data, thus specifically unauthorised or accidental access, alteration, disclosure, erasure, loss or annihilation as well as accidental destruction and injury. The data protection officer immediately investigates the reported or detected data breach and, within 24 hours from

becoming aware of the data breach, makes a proposal for eliminating and managing the data breach.

The Controllers warrant that the data is processed in full compliance with the provisions of the effective legal rules.

Should the data processing conditions change, our Companies will inform the participants about the modifications.

The document is valid from 11/09/2023.