PRIVACY NOTICE

360 Design Budapest Exhibition

online registration

This Privacy Notice (hereinafter: the "**Notice**") contains all information related to the processing of personal data provided during online registration on the website www.360dbp.com for the event entitled *360 Design Budapest Exhibition* (hereinafter: the "**Event**"), organized by **HFDA Hungarian Fashion & Design Agency Nonprofit Private Limited Company** (company registration number: 01-10-049808; tax number: 26338972-2-43; registered seat: 1126 Budapest, Istenhegyi út 18.; represented by: Zsófia Jakab, Chief Executive Officer; central e-mail address: info@hfda.hu; central telephone number: +36 20 272 2351; Data Protection Officer contact: Takács, Kiss és Társai Law Firm, dpo@tkpartners.hu; hereinafter reffered to as "**Company**" or "**Data Controller**") for the purpose of ensuring that, prior to providing your personal data and consent, you are fully informed about the purpose and conditions of data processing, the related risks and safeguards, as well as your rights as a data subject.

By registering for the Event, **you, as a visitor to the Event** (hereinafter: the "**Data Subject**"), accept the provisions of this Notice and consent to the processing of your personal data.

By the act of registration and acceptance of this Notice, you declare that you have read and expressly accepted the version of this Notice in effect at the time you provided the data or information, and you consent to the processing of your personal data.

Our Company stores the personal data you provide on servers operated by the Data Controller or the Data Processor.

By providing this privacy notice, our Company aims to 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 referred to as the "**Regulation**"), as well as the provisions of Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information (hereinafter referred to as "**Info Act**"). Our Company aims to ensure that all information relating to the processing of personal data is provided to the Data Subject 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. The terms used in this Notice correspond to the definitions and interpretations set forth in the Info Act and the GDPR.

I. DEFINITIONS

1.1. **Data Controller:** HFDA Hungarian Fashion & Design Agency Nonprofit Private Limited Company.

1.2. **Data Processing**: Any operation or set of operations performed on personal data, irrespective of the procedure applied, including, in particular, the collection, recording, organization, storage, alteration, use, retrieval, transmission, disclosure, alignment or combination, restriction, erasure, or destruction of data, as well as the prevention of further use of such data. Data processing also includes the taking of photographs, audio or video recordings, and the recording of physical characteristics suitable for identifying a natural person (e.g., fingerprint, palm print, DNA sample, iris scan).

1.3. **Data Processor:** Any contractual partner of the Data Controller who, under an agreement concluded with the Data Controller (including agreements concluded pursuant to a legal obligation), processes personal data on behalf of the Data Controller.

1.4. **Data Processing**: The performance of technical tasks related to personal data processing operations, irrespective of the method and means employed, or the place of execution, provided that such technical tasks are carried out on personal data.

1.5. **Consent:** A freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear affirmative action, signify their agreement to the processing of their personal data, in whole or in part.

II. DATA CONTROLLER AND CONTACT DETAILS

2.1. **Name of the Data Controller:** HFDA HUNGARIAN FASHION & DESIGN AGENCY Nonprofit Private Limited Company

2.2. **Company registration number**: 01-10-049808

2.3. **Tax number**: 26338972-2-43

2.4. **Registered seat:** 1126 Budapest, Istenhegyi út 18.,

2.5. **Represented by:** Zsófia Jakab, CEO

2.6. **Central email address**: info@hfda.hu

2.7. **Central telephone number:** +36 20 272 2351

III. NAME AND CONTACT INFORMATION OF THE DATA PROTECTION OFFICER

3.1. **Data Protecion Officer:** Takács, Kiss és Társai Law Firm

3.2. **Registered seat:** 1054 Budapest, Szabadság tér 7. Bank Center Office Building, City Tower, 6th Floor,

3.3. **E-mail address**: dpo@tkpartners.hu

IV. DATA PROCESSORS ENGAGED

The Data Controller reserves the right to engage Data Processors during its activities, either on a permanent or an ad hoc basis. Permanent data processing may primarily take place in connection with the provision of

services under Act CXLIII of 2015 on Public Procurement, for the purposes of related administration and contract performance. In carrying out certain professional tasks, the Company engages the following entities as Data Processors:

- **MEDIATOR GROUP Kft.** (Registered seat: 1117 Budapest, Dombóvári út 25.; Company registration number: 01-09-864793)
- **Event & More Kft.** (Registered seat: 1112 Budapest, Sasadi út 134.; Company registration number: 01-09-698048)

The Data Processors do not use the personal data provided for their own purposes; they process such data exclusively on behalf of the Data Controller. The engagement of Data Processors is governed by applicable legislation, in particular GDPR and Info Act.

A Data Processor may only be engaged based on a written agreement. Upon request, the Data Controller shall provide the Data Subject with information regarding the identity of the Data Processor and the details of its data processing activities, including the operations carried out and the instructions received from the Data Controller. The rights and obligations of each Data Processor in relation to the processing of personal data are determined by the Data Controller, in accordance with the applicable legislation. The Data Controller is responsible for the lawfulness of the instructions relating to data processing operations. Within the scope of its activities and the limits set by the Data Controller, the Data Processor may carry out the processing, modification, erasure, transmission, and disclosure of personal data. The Data Processor may not engage another processor (sub-processor) in the performance of its activities. The Data Processor may not make substantive decisions regarding data processing, may only process personal data in accordance with the documented instructions of the Data Controller, may not process data for its own purposes, and is obliged to store and retain personal data strictly in line with the instructions of the Data Controller. By establishing contractual terms that provide appropriate safeguards and by implementing adequate organizational and technical measures, the Data Controller ensures that the rights of Data Subjects are protected during the activities of the Data Processors, and that Data Processors only access personal data to the extent strictly necessary for the performance of their tasks.

V. INFORMATION RELATING TO DATA PROCESSING

5.1. Scope and Purpose of Processed Personal Data

The Data Controller processes and maintains the following personal data provided during registration for the purposes of ensuring participation in the Event, its proper organization, identification of participants, and maintaining related communication:

- The Data Subject's family name and given name;
- The Data Subject's title; and
- The Data Subject's e-mail address.

The Data Controller draws the Data Subject's attention to the fact that, as the Event is open to the press, video and photographic recordings of the Data Subject may be made. Furthermore, the Data Controller may retain personal data of Data Subjects who have subscribed to newsletters, based on separate explicit consent, for the purpose of enabling the sending of such newsletters.

5.2. Duration of Data Processing

The Data Controller shall delete the personal data provided during registration following the conclusion of the Event. Personal data provided for the purpose of newsletter subscription shall be processed by the Data Controller until such consent is withdrawn.

5.3. Legal Basis for Data Processing

The legal basis for the processing of personal data is Article 6(1)(a) of GDPR, namely, the voluntary consent of the Data Subject.

VI. RECIPIENTS OR CATEGORIES OF RECIPIENTS OF PERSONAL DATA

Employees acting under the direct authority of the Data Controller and the Data Processor may access the personal data provided by the Data Subject solely for the purpose of performing their professional duties. Such employees shall handle the data confidentially and in accordance with the applicable legal requirements, as well as the internal policies and procedures of the Data Controller and the Data Processor.

By making personal data accessible to the aforementioned recipients, the Data Controller does not transfer the Data Subject's personal data to any third country outside the European Economic Area (EEA).

The Data Controller shall not transfer personal data to any recipient other than those specified above, except where such transfer is required by law, or by an order of a competent authority or a court.

VII. RIGHTS OF THE DATA SUBJECT

The rights the Data Subject is entitled to in relation to data processing are as follows:

7.1. Right to transparent information:

The Data Subject has the right to be informed of all facts and circumstances relating to the processing of their personal data prior to the commencement of such processing. This Privacy Notice has been prepared to facilitate the exercise of this right.

Upon request, the Data Controller shall provide information regarding the personal data it processes, or that is processed by a Data Processor engaged by the Data Controller, including the source of the data, the purpose, legal basis, and duration of the data processing, the name and address of the Data Processor, and the activities related to the data processing. In the event of data transfer, the legal basis and recipients of the transfer shall also be disclosed. The Data Controller shall provide this information in writing within a maximum of 30 days from the submission of the request.

7.2. Right of access by the Data Subject:

The Data Subject has the right to obtain confirmation from the Data Controller as to whether their personal data is being processed. If such processing is taking place, the Data Subject shall have the right to access the following information:

- The personal data being processed and the categories of such personal data;
- The purpose of the processing;

- The recipients or categories of recipients to whom the personal data has been or will be disclosed by the Data Controller;
- The planned storage period of the personal data, or, if not possible, the criteria used to determine that period;
- Information concerning the Data Subject's right to request the rectification, erasure, or restriction of processing of their personal data, and the right to object to the processing of such personal data;
- The right to lodge a complaint with the competent Data Protection Authority, as set out in Section 7.11 of this Privacy Notice.

Upon request, the Data Controller shall provide the Data Subject with a copy of the personal data being processed.

Where the Data Subject requests multiple copies of the information or of the aforementioned data, the Data Controller may charge a reasonable fee proportionate to the administrative costs incurred in providing such additional copies.

The Data Controller may refuse to comply with a request to the extent that the exercise of the Data Subject's right of access adversely affects the rights and freedoms of others, in particular trade secrets or intellectual property, provided that such refusal is necessary and proportionate.

Prior to fulfilling a request, the Data Controller may require the Data Subject to clarify the content of the request and to specify precisely the information or data processing activities requested.

7.3. Right to Rectification

Upon the request of the Data Subject, the Data Controller shall correct or complete any inaccurate or incomplete personal data relating to the Data Subject without undue delay. Prior to making any correction, the Data Controller may verify the authenticity and accuracy of the relevant data.

Following the fulfillment of a request to exercise the right to rectification, the Data Controller shall promptly inform all recipients with whom the Data Subject's personal data has been shared, unless such notification proves impossible or would require disproportionate effort.

7.4. Right to Withdraw Consent

The Data Subject has the right to withdraw their consent for the processing of personal data based on consent at any time. The withdrawal of consent shall not affect the lawfulness of processing carried out prior to such withdrawal.

The Data Subject may withdraw their consent at any time by submitting a request to the Data Controller in writing or electronically, including, where applicable, by using the unsubscribe link provided in newsletters.

7.5. Right to Erasure ("Right to be Forgotten")

The Data Subject has the right to request the erasure of their personal data without undue delay in the following circumstances:

- The personal data are no longer necessary for the purposes for which they were collected or otherwise processed by the Data Controller;

- The Data Subject withdraws their consent, provided that there is no other legal basis for the processing carried out by the Data Controller;
- The Data Subject objects to the processing pursuant to Section 7.8 of this Privacy Notice, and there is no overriding legitimate basis for the processing;
- The personal data of the Data Subject have been unlawfully processed by the Data Controller; or
- The Data Controller is obliged to erase the personal data in order to comply with a legal obligation under Hungarian or European Union law.

Following the fulfillment of a request to exercise the right to erasure, the Data Controller shall promptly inform all recipients with whom the Data Subject's personal data have been shared, unless such notification is impossible or would require disproportionate effort.

The Data Controller is not obliged to erase personal data where processing is necessary for the establishment, exercise, or defense of legal claims.

This right shall not apply where the processing of personal data is based on a legal obligation.

7.6. Right to Restriction of Processing („Right to Block")

The Data Subject has the right to request that the Data Controller restrict the processing of their personal data in the following circumstances:

- Where the accuracy of the personal data is contested by the Data Subject; in such cases, the restriction shall apply for the period necessary for the Data Controller to verify the accuracy of the personal data;
- Where the processing is unlawful and the Data Subject opposes the erasure of the data, instead requesting the restriction of its use;
- Where the Data Controller no longer requires the personal data for the purposes of processing, but the Data Subject requires the data for the establishment, exercise, or defense of legal claims;
- Where the Data Subject has objected to the processing; in such cases, the restriction shall apply until it is determined whether the legitimate grounds of the Data Controller override those of the Data Subject.

7.7. Right to Data Portability

The Data Subject has the right to receive the personal data they have provided to the Data Controller in a structured, commonly used, and machine-readable format, and to transmit such data to another Data Controller without hindrance from the Data Controller to which the personal data was originally provided. This right applies only where:

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

Where technically feasible, the Data Controller shall, upon the request of the Data Subject, transmit the personal data directly to another Data Controller designated by the Data Subject. The right to data portability does not impose an obligation on Data Controllers to adopt or maintain technically compatible systems.

Where the exercise of the right to data portability adversely affects the rights and freedoms of others, in particular trade secrets or intellectual property, the Data Controller may refuse to comply to the necessary and proportionate extent.

7.8. Right to Object

The Data Subject has the right to object at any time, on grounds relating to their particular situation, to the processing of their personal data where such processing is carried out for:

- The performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller; or
- The purposes of legitimate interests pursued by the Data Controller or a third party, including profiling.

The Data Controller shall not cease processing based on the objection where the processing is justified by compelling legitimate grounds that override the interests, rights, and freedoms of the Data Subject, or where processing is necessary for the establishment, exercise, or defense of legal claims.

Where the Data Controller cannot demonstrate that the processing is justified by such compelling legitimate grounds, processing shall cease and the personal data shall be deleted.

7.9. Automated Decision-Making, Including Profiling

The Data Subject has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them. The Data Controller does not engage in automated decision-making.

7.10. Notification of a Personal Data Breach

Where a personal data breach is likely to result in a high risk to the rights and freedoms of the Data Subject, the Data Controller shall notify the Data Subject of such breach without undue delay.

7.11. Right to lodge a complaint with a Supervisory Authority:

If the Data Subject believes that their personal data has been processed in violation of data protection laws, it is recommended, for faster and more efficient handling, that they first contact the Data Controller and submit a request to exercise their data subject rights prior to lodging a complaint.

The Data Subject has the right to lodge a complaint with the competent supervisory authority if they consider that the processing of personal data infringes applicable data protection regulations.

Supervisory Authority:

- **Name:** National Authority for Data Protection and Freedom of Information (hereinafter: "NAIH")
- **Registered Office:** 1055 Budapest, Falk Miksa utca 9-11
- **Mailing Address:** 1363 Budapest, Pf.: 9
- **Telephone:** +36 (30) 683-5969, +36 (30) 549-6838, +36 (1) 391 1400

- **Fax:** +36 (1) 391-1410
- **Government Gateway:** Short name: NAIH, KR ID: 429616918
- **E-mail:** ugyfelszolgalat@naih.hu

7.12. Right to an Effective Judicial Remedy Against the Supervisory Authority

The Data Subject has the right to bring proceedings before a court against a final decision issued by the NAIH.

7.13. Right to an Effective Judicial Remedy Against the Data Controller or Data Processor

Without prejudice to the right to lodge a complaint, the Data Subject is entitled to an effective judicial remedy by initiating civil proceedings if they consider that their rights have been infringed as a result of the unlawful processing of their personal data.

At the discretion of the Data Subject, proceedings may be brought before the court having jurisdiction over the Data Subject's place of residence or habitual residence. Court contact information can be found at: http://birosag.hu/torvenyszekek.

VIII. DATA SECURITY MEASURES

The Company undertakes to ensure the security of personal data and to implement the necessary technical and organizational measures, as well as procedural rules, to guarantee that collected, stored, and processed data are protected against unauthorized access, disclosure, alteration, destruction, or accidental loss. The Data Controller ensures that unauthorized persons cannot access, disclose, transmit, modify, or delete the processed personal data. The Data Controller takes all reasonable measures to prevent accidental damage or loss. These obligations also extend to employees involved in data processing and to Data Processors acting on behalf of the Data Controller. In cooperation with Data Processors, the Data Controller considers the state of the art when defining and implementing security measures. Among several possible solutions, the Data Controller selects the option that provides the highest level of protection for personal data, unless doing so would result in disproportionate difficulty. The Company ensures proper backup of IT systems and the technical environment of the website, maintaining the availability of data for the duration of its retention period and ensuring permanent deletion after expiration of that period. The integrity and operability of IT systems and data storage environments are continuously monitored using advanced monitoring techniques, with necessary capacities maintained at all times. Events occurring within the IT environment are logged using comprehensive logging functions to ensure traceability of potential incidents and to preserve evidential value for legal purposes. Redundant networks with consistently high bandwidth are utilized to serve websites, distributing loads securely across resources. Systems are designed to ensure disaster tolerance and business continuity, providing uninterrupted service through both organizational and technical measures. Priority is given to the controlled installation of security patches and manufacturer updates, maintaining system integrity and mitigating risks arising from vulnerabilities. The IT environment is regularly tested for security, and any identified vulnerabilities or weaknesses are promptly remediated. Security reinforcement is treated as an ongoing responsibility. Employees are required to adhere to high security standards, including confidentiality obligations, reinforced through regular training. Internal processes are designed and monitored to ensure controlled and secure operations. Any incidents affecting personal data, whether detected or reported, are investigated transparently and responsibly, and addressed within seventy-two (72) hours. All incidents are

recorded and managed. During the development of services and IT solutions, the Company ensures compliance with the principle of data protection by design, treating data protection as a core requirement from the outset.

IX. HANDLING AND REPORTING OF DATA PROTECTION INCIDENTS

A data protection incident is any event relating to personal data processed, transmitted, stored, or otherwise handled by the Data Controller that results in the unlawful processing or handling of such data, including, in particular, unauthorized or accidental access, alteration, disclosure, deletion, loss, destruction, or damage. Persons responsible for data protection shall immediately investigate any reported or detected data protection incident and, within seventy-two (72) hours of becoming aware of the incident, propose appropriate measures to mitigate and manage the incident. The Data Controller guarantees that all data processing is conducted in compliance with applicable legal provisions. If the conditions of data processing change, the Company shall inform the Data Subjects of such modifications in a timely manner.