HUNGARIAN FASHION AND DESIGN AGENCY

PRIVACY NOTICE

FOR SUBSCRIPTION TO NEWSLETTERS

This Privacy Notice (hereinafter referred to as the "Notice") relates to the data processing activities carried out by HFDA NONPROFIT ZRT. (hereinafter referred to as the "Company" or "Data Controller") and contains all information regarding the processing of personal data. Its purpose is to ensure that you, as the Data Subject, are fully informed—prior to providing your personal data—about the purpose and conditions of data processing, the associated risks and safeguards, as well as your rights in connection with the processing of your personal data.

Subscribing to the newsletter is voluntary; therefore, please consider the information provided in this Notice before granting your consent. Submitting your consent to the Data Controller is a condition for subscription.

By providing your personal data and completing the subscription, you declare that you have read and expressly accept the version of this Notice in effect at the time of providing your 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.

1. DATA CONTROLLER AND CONTACT DETAILS

NAME OF THE DATA CONTROLLER:

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, CEO, central email address: info@hfda.hu, central telephone number: +36 30 179 5709)

POSTAL ADDRESS OF THE DATA CONTROLLER: 1026 Budapest, Istenhegyi út 18.

EMAIL ADDRESS OF THE DATA CONTROLLER: info@hfda.hu

PHONE NUMBER OF THE DATA CONTROLLER: +36 30 179 5709

NAME AND CONTACT INFORMATION OF THE DATA PROTECTION OFFICER: Takács, Kiss és Társai Law Firm 1054 Budapest, Szabadság tér 7. Bank Center Office Building, Citi Tower, 6th Floor, dpo@tkpartners.hu

2. THE DATA PROCESSOR USED:

In the course of its data processing activities, the Data Controller engages the following companies in a data processor capacity:

- MEDIATOR GROUP KFT. (company registration number: 01-09-864793, tax number: 13622215-2-43, registered office: 1117 Budapest, Dombóvári út 25.)

The Data Processor does not use the data for its own purposes but solely processes the data on behalf of the Data Controller.

3. PURPOSE OF DATA PROCESSING:

The Data Controller processes certain personal data of the Data Subjects for the purpose of building a database required for sending marketing and professional newsletters and for communication purposes.

4. SCOPE OF PERSONAL DATA PROCESSED:

The name and email address of the Data Subject (subscriber).

5. DURATION OF DATA PROCESSING:

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

6. LEGAL BASIS FOR DATA PROCESSING:

The voluntary consent of the Data Subject.

7. RECIPIENTS OF PERSONAL DATA OR CATEGORIES OF RECIPIENTS:

The personal data provided by you may be accessed by employees directly under the control of the Data Controller and Data Processor for the purpose of fulfilling their job duties. These employees will handle the data confidentially and in accordance with applicable legal requirements, as well as internal rules and procedures, both at the Data Controller and Data Processor.

8. RIGHTS OF THE DATA SUBJECT

The rights you are entitled to in relation to data processing are as follows:

RIGHT TO TRANSPARENT INFORMATION:

You have the right to receive information about the facts and details of data processing before the processing begins. We have created this Privacy Notice to ensure this right.

RIGHT OF ACCESS BY THE DATA SUBJECT:

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

- the personal data being processed and the categories of personal data, as well as the purposes of the processing;

- the recipients or categories of recipients to whom the personal data have been or will be disclosed;

- 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 has the right to request the Data Controller to rectify or complete any personal data that is inaccurate, incorrect, or incomplete. Before rectifying any incorrect data, the Data Controller may verify the accuracy and truthfulness of the data provided.

RIGHT TO WITHDRAW CONSENT:

Where processing is based on the Data Subject's consent, they have the right to withdraw that consent at any time. Such withdrawal shall not affect the lawfulness of processing based on consent before its withdrawal.

The Data Subject may withdraw their valid consent to data processing at any time by notifying the Data Controller in an informal manner or by using the unsubscribe link provided in the newsletter.

THE RIGHT TO ERASURE ("RIGHT TO BE FORGOTTEN"):

The Data Subject has the right to request the erasure of their personal data without undue delay, and the Data Controller is obliged to comply with such a request. However, this right does not apply where data processing is based on a legal obligation.

RIGHT TO RESTRICTION OF PROCESSING (RIGHT TO BLOCKING):

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

• if the Data Subject contests the accuracy of the personal data, processing shall be restricted for a period enabling the Data Controller to verify the accuracy of the data;

• if the processing is unlawful and the Data Subject opposes the erasure of the data and instead requests the restriction of its use;

• if the Data Controller no longer needs the personal data for the purposes of processing, but the Data Subject requires it for the establishment, exercise, or defence of legal claims;

• if the Data Subject has objected to the processing, in which case processing shall be restricted pending the verification of whether the Data Controller's legitimate grounds override those of the Data Subject.

RIGHT TO DATA PORTABILITY:

The Data Subject has the right to receive the personal data concerning them, which they have provided to the Data Controller, in a structured, commonly used and machine-readable format. Furthermore, the Data Subject has the right to transmit this data to another data controller without hindrance from the Data Controller to which the personal data was originally provided. This right shall apply where:

• the processing is based on the Data Subject's consent or on a contract pursuant to Article 6(1)(b) of the GDPR, or on the consent given for the processing of special categories of personal data for one or more specific purposes; and

• the processing is carried out by automated means.

RIGHT TO OBJECT:

The Data Subject has the right to object at any time to the processing of their personal data for reasons related to their particular situation, if the 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 Data Controller, or if the processing is necessary for the legitimate interests pursued by the Data Controller or a third party, including profiling. In such a case, the Data Controller shall no longer process the personal data unless it 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 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 Controllers do not use automated decision-making.

NOTIFICATION OF THE DATA SUBJECT IN CASE OF A DATA BREACH:

If a data protection incident is likely to result in a high risk to your data, rights, and freedoms, the data controllers will inform you of the incident without undue delay.

RIGHT TO LODGE A COMPLAINT WITH A SUPERVISORY AUTHORITY:

If the Data Subject has a grievance regarding the processing of their personal data, it is advisable to contact the Data Controller prior to submitting a formal complaint, in order to facilitate a quicker and more efficient resolution of the matter.

You have the right to lodge a complaint with a supervisory authority if you believe that the processing of your personal data infringes data protection laws.

National Authority for Data Protection and Freedom of Information

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

Postal address: 1363 Budapest, P.O. Box 9

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

Fax: +36 (1) 391-1410

Official contact details: Short name: NAIH, KR ID:429616918

Email: 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 THE DATA CONTROLLER OR DATA PROCESSOR:

Without prejudice to your right to lodge a complaint, you have the right to an effective judicial remedy through civil proceedings if you believe that your rights have been infringed as a result of the unlawful processing of your personal data. The case shall fall under the jurisdiction of the Budapest Metropolitan Court, although you may also bring the proceedings before the competent court of your place of residence.

9. DATA SECURITY MEASURES

The Company undertakes to ensure the security of personal data and implements the necessary technical and organisational measures, as well as establishes the procedural rules required to protect the recorded,

stored, and processed data. These measures are aimed at preventing the destruction, unauthorised use, and unauthorised alteration of personal data. The Company also requires the Data Processor to comply with data security requirements.

The Data Controller ensures that unauthorised persons do not have access to, cannot disclose, transmit, modify, or delete the processed data. The Data Controller takes all reasonable measures to prevent the accidental damage or destruction of the data. This obligation extends to all employees involved in data processing and to the Data Processor acting on behalf of the Data Controller.

The Company ensures appropriate data backups for IT data and the technical environment of its website. These backups are operated in accordance with the parameters determined by the respective data retention periods, guaranteeing availability during the retention period and ensuring that data are permanently deleted upon expiry.

The integrity and operability of the IT systems and data storage environment are monitored using advanced techniques, and the necessary capacities are continually maintained.

Events occurring in the IT environment are logged using comprehensive logging functionalities, thereby enabling the subsequent investigation of potential incidents and providing legally valid proof if necessary.

The Company employs a continuously high-bandwidth, redundant network environment to support the operation of its websites, ensuring that arising loads are securely distributed across available resources.

The Company ensures the disaster resilience of its systems through planned measures and provides for business continuity and, thereby, continuous user service at a high level using both organisational and technical tools.

It places high priority on the controlled installation of security patches and manufacturer updates that ensure the integrity of its IT systems, thus preventing, avoiding, and addressing attempts to exploit vulnerabilities for unauthorised access or damage.

The IT environment is regularly subjected to security testing. Any identified errors or vulnerabilities are corrected, and the continual strengthening of IT security is treated as an ongoing responsibility.

Strict security expectations, including confidentiality obligations, are established for employees, and their compliance is supported through regular training. In its internal operations, the Company strives to maintain planned and controlled processes.

Any incidents affecting personal data, whether detected internally or reported to the Company, are investigated transparently, responsibly, and rigorously within 72 hours. All such incidents are appropriately managed and recorded.

In the development of its services and IT solutions, the Company ensures compliance with the principle of data protection by design, treating data protection as a key requirement from the planning stage onwards.

10. HANDLING AND REPORTING OF DATA PROTECTION INCIDENTS

A data protection incident shall be deemed to mean any event concerning personal data processed, transferred, stored or otherwise handled by the Data Controller which results in the unlawful processing of such personal data. This includes, in particular, unauthorised or accidental access, alteration, disclosure, deletion, loss or destruction, as well as accidental destruction or damage. The persons responsible for data protection shall immediately investigate any reported or detected data protection incident. Within 72 hours of becoming aware of the incident, they shall propose measures for its elimination and for managing its consequences.

The Data Controller guarantees that all data processing is carried out in full compliance with the applicable legal provisions.

Should the conditions of data processing change, the Company shall inform the Data Subjects of such changes.

11. DATA SECURITY MEASURES

The Company undertakes to ensure the security of personal data and implements the necessary technical and organisational measures, as well as establishes the procedural rules required to protect the recorded, stored, and processed data. These measures are aimed at preventing the destruction, unauthorised use, and unauthorised alteration of personal data. The Company also requires the Data Processor to comply with data security requirements.

The Data Controller ensures that unauthorised persons do not have access to, cannot disclose, transmit, modify, or delete the processed data. The Data Controller takes all reasonable measures to prevent the accidental damage or destruction of the data. This obligation extends to all employees involved in data processing and to the Data Processor acting on behalf of the Data Controller.

The Company ensures appropriate data backups for IT data and the technical environment of its website. These backups are operated in accordance with the parameters determined by the respective data retention periods, guaranteeing availability during the retention period and ensuring that data are permanently deleted upon expiry.

The integrity and operability of the IT systems and data storage environment are monitored using advanced techniques, and the necessary capacities are continually maintained.

It records events occurring within its IT environment using complex logging functions, thereby ensuring the subsequent detectability of any potential incidents and their legal traceability.

The Company operates a continuously high-bandwidth, redundant network environment to support the operation of its websites, ensuring that arising loads are securely distributed across available resources.

It ensures the disaster resilience of its systems in a planned manner, and provides for business continuity — and thus the continuous service of its users — at a high level through both organisational and technical means.

It places high priority on the controlled installation of security patches and manufacturer updates that ensure the integrity of its IT systems, thus preventing, avoiding, and addressing attempts to exploit vulnerabilities for unauthorised access or damage.

The IT environment is regularly subjected to security testing. Any identified errors or vulnerabilities are corrected, and the continual strengthening of IT security is treated as an ongoing responsibility.

High security expectations, including confidentiality obligations, are set for its employees, the fulfilment of which is ensured through regular training. In terms of internal operations, it strives to maintain planned and controlled processes.

Any incidents affecting personal data, whether detected internally or reported to the Company, are investigated transparently, responsibly, and rigorously within 72 hours. All such incidents are appropriately managed and recorded.

During the development of its services and IT solutions, it ensures compliance with the principle of data protection by design, treating data protection as a key requirement already at the planning stage.

12. HANDLING AND REPORTING OF DATA PROTECTION INCIDENTS

A data protection incident shall be deemed to mean any event concerning personal data processed, transferred, stored or otherwise handled by the Data Controller which results in the unlawful processing of such personal data. This includes, in particular, unauthorised or accidental access, alteration, disclosure, deletion, loss or destruction, as well as accidental destruction or damage. The persons responsible for data protection shall immediately investigate any reported or detected data protection incident. Within 72 hours of becoming aware of the incident, they shall propose measures for its elimination and for managing its consequences.

The Data Controller guarantees that all data processing is carried out in full compliance with the applicable legal provisions.

Should the conditions of data processing change, the Company shall inform the Data Subjects of such changes.

This Notice is effective from 1st March 2025.