Annex No. 2

Privacy Notice

Contact, Registration, Newsletter Subscription

This Privacy Notice (hereinafter referred to as the "Notice") contains all relevant information regarding the processing of your personal data provided during registration for contact purposes. Its aim is to ensure that, prior to giving 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 and accepting this Notice, you declare that you have read and explicitly accepted the version of this Privacy Notice in effect at the time of providing your data, and you give your consent to the processing of your personal data in connection with the contact registration.

By ticking the consent checkbox for newsletter subscription and accepting this Notice, you declare that you have read and explicitly accepted the version of this Privacy Notice in effect at the time of providing your data.

Our Company informs you that newsletter subscription is not a prerequisite for registration.

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

With this Notice, our Company aims to comply with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter: the Regulation or GDPR) on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, which repealed Directive 95/46/EC, as well as with the provisions of Act CXII of 2011 on the Right of Informational Self-Determination and Freedom of Information (hereinafter: the Info Act). Our Company strives to provide every piece of information regarding the processing of personal data to the Data Subject in a concise, transparent, intelligible, and easily accessible form, using clear and plain language. Furthermore, we aim to facilitate the exercise of the Data Subject's rights. The terms used in this Privacy Notice correspond to the definitions and interpretations set out in the Information Act and the Regulation (GDPR).

1. DATA CONTROLLER AND CONTACT INFORMATION

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)

POSTAL ADDRESS OF THE DATA CONTROLLER: 1126 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

2. DATA PROCESSOR USED:

In the course of performing its data processing activities, the Company uses the services of the following entities in the capacity of Data Processor:

MEDIATOR GROUP KFT. (Company registration number: 01-09-864793 Registered office: 1117 Budapest, Dombóvári út 25.)

The Data Processors do not use the received data for their own purposes; they process the data solely on behalf of the Data Controller.

USE OF COOKIES

Like many other commercial websites, the Agency also uses the common technology known as cookies, as well as technical log files of the web server, in order to obtain information about how Data Subjects use the Website.

The use of cookies and web server log files allows the Agency to monitor Website traffic and tailor the content of the Website to your personal needs.

A cookie is a small package of information (file) that often carries an anonymised unique identifier. When you visit a website, the website requests permission from your computer to store this file in a section of your hard drive that is specifically designated for storing cookies.

Each website you visit is able to send cookies to your computer if your browser settings allow it. To protect your data, however, your browser only allows the specific website to access the cookie that it has sent to your computer, meaning that one website cannot access cookies sent by other websites. Browsers are typically configured to accept cookies.

However, if you do not wish to accept cookies, you can adjust your browser settings to reject cookies. In this case, some elements of the website may not function properly while you browse. Cookies cannot retrieve any other information from your computer's hard drive and do not carry viruses.

The website uses the following cookies:

Necessary category:

Necessary cookies help make the website usable by enabling basic functions such as page navigation and secure access.

The website will not function properly without these cookies.

COOKIE NAME	SERVICE PROVIDER	TYPE	EXPIRATION
PHPSESSID	hfda.hu	http	Session

Statistical category:

Statistical cookies help website operators understand how visitors use the site by collecting anonymous information.

COOKIE NAME	SERVICE PROVIDER	TYPE	EXPIRATION
_ga	google	http	400 days
_ga_B1SMWY8Q6M	google	http	400 days
_gat_gtag_UA_129752036_1	google	http	1 day

_gid	google	http	1 day

Further information:

https://support.google.com/analytics/topic/2919631?hl=hu&ref_topic=1008008

3. PURPOSE OF DATA PROCESSING:

The purpose of data processing is to ensure the possibility of contact with the Data Subject and general communication.

The Data Controller keeps the Data Subject's data for the purpose of providing the opportunity for newsletter subscription, based on explicit consent, in the case of subscribing to the newsletter.

4. SCOPE OF PERSONAL DATA PROCESSED:

The personal data required for contact registration and newsletter subscription are as follows: name, email address, and phone number.

5. DURATION OF DATA PROCESSING:

The Data Controller will process the personal data provided by the Data Subject during the registration for the Tender until the completion of the tender process, and the personal data related to the newsletter subscription will be processed until the consent is withdrawn (i.e., when the Data Subject unsubscribes from the newsletter).

6. LEGAL BASIS FOR DATA PROCESSING:

The legal basis for data processing is the voluntary consent of the Data Subject in the case of applying for the Tender and subscribing to the newsletter.

7. RECIPIENTS OF PERSONAL DATA AND CATEGORIES OF RECIPIENTS:

Authorised employees under the direct supervision of the Data Controller and the Data Processor may access your personal data solely for the purpose of performing their job-related duties. These individuals handle the data in a confidential manner in accordance with the applicable legal requirements, internal policies, and procedural rules in effect at both the Data Controller and the Data Processor. The event forming part of the Tender is open to the press; therefore, members of the media may take crowd photographs of you within the framework of legal regulations, and may use such images for the purpose of providing information about the event.

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 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 rectification or supplementation of personal data that is incorrect, inaccurate, or incomplete. Before making any corrections, the Data Controller may verify the accuracy and authenticity of the data in question.

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 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 and on grounds relating to their particular situation, to the processing of their personal data where 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 where the processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or a third party, including profiling based on those provisions. 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 Company does not apply automated decision-making.

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

If a potential data breach is likely to result in a high risk to your personal data, rights, and freedoms, the Data Controller shall notify you of the data breach without undue delay.

RIGHT TO LODGE A COMPLAINT WITH A SUPERVISORY AUTHORITY:

If the Data Subject has a grievance concerning the processing of their personal data, it is advisable to contact the Data Controller and submit a request to exercise the relevant data subject rights before filing a complaint, to ensure quicker and more efficient resolution.

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

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.

This Privacy Notice is effective from 13 January 2025.