PRIVACY NOTICE

HUNGARIAN FASHION AND DESIGN AGENCY LTD. (MDDÜ MAGYAR DIVAT ÉS DESIGN ÜGYNÖKSÉG NONPROFIT ZRT., Registration number: 01-10-049808, Office: H-1126 Budapest, Istenhegyi út 18, Tax number: 26338972-2-43, 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 visitors of its website (hereinafter: Website) 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.

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 2011on the Right of Informational Self-Determination and on Freedom of Information (Infotv.);
• Act V of 2013on the Civil Code (Ptk.);

Personal data may be processed, if

• the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
• processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract,
• processing is necessary for compliance with a legal obligation to which the controller is subject;
• processing is necessary in order to protect the vital interests of the data subject or of another natural person;

• 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 controller;
• is necessary for the enforcement of the legitimate interests of the Controller or a third party.
Pursuant to Article 8 (1) of the GDPR, statements of consent of data subject minors over the age of 16 shall be considered valid without the permission or subsequent approval of their legal representative, while statements of consent of data subject minors below the age of 16 are not valid without the consent of the party exercising parental supervision over the minor. The Agency has no tools to verify the accuracy and validity of the consent, its accuracy is warranted by the person granting consent.

THE PURPOSE OF DATA PROCESSING

The purpose of data processing is to ensure the safe use and technical operation of the Website and to be able to control it. When visiting the Website, the Data Controller collects technical data necessary for the use of the website, as well as data for the purpose of generating traffic statistics.

We also wish to inform you that in relation to the functions linked through the icons of external providers shown on the Website (Facebook, Twitter, LinkedIn, Instagram) the Agency does not perform any processing activities, as in such cases the controller is the external company providing the service.

THE LEGAL BASIS OF DATA PROCESSING

In the context of statistical cookies, the legal basis for data processing is your consent (Article 6. (1) (a) GDPR). We treat cookies that are strictly necessary for the operation, as well as data related to the secure technical operation of the Website -including the IP address of visitors- in accordance with the legitimate interest (Article 6. (1) (f) GDPR).

TERMS OF PROCESSING DATA

We store the information related to the secure technical operation of the website - including the IP address of the visitors- for 1 year.

SCOPE OF PROCESSED DATA

During the operation of the Website, we treat IP address of the visitor's computer or mobile device as technical data, the approximate geographical location that can be deduced from it; operating system type, features, and version number; browser type and version number; activity on the Website; the exact date of the visit; the time spent on the Website; use of a feature or service used on the Website. We also place cookies on the computer or mobile device used for viewing. If you refuse to accept cookies, the site will only handle anonymized, non-personally identifiable information (such as Google Analytics to generate traffic statistics).

DURATION OF STORAGE OF PERSONAL DATA

The data processed with consent shall be processed until the consent is withdrawn if no other legal ground of processing applies. The withdrawal of consent does not affect the lawfulness of prior processing.

RECIPIENTS OF PERSONAL DATA AND RECIPIENT CATEGORIES

The users of the Agency and the Data Processors maintaining partner relationships and providing customer services and, in the case of technical data, the IT staff members.

DATA PROCESSORS

The Agency uses the following services of data processor companies for different tasks:

- MEDIATOR GROUP KFT. (headoffice: 1117 Budapest, Dombóvári út 25., reg. number: 01-09-864793,)
- GOOGLE LLC (USA - Google Data Protection Office, 1600 Amphitheatre Pkwy Mountain View, California 94043)
- HUNGARIAN TOURISM AGENCY LTD. (reg. number: 01-10-041364, headoffice: 1027 Budapest, Kacsa utca 15-23.)

USE OF COOKIES

Similarly to other commercial websites, the Agency also uses the general technology known as cookies and webserver technical log files in order to obtain information about how the data subjects use the website.

With the help of the cookies and webserver log files, the Agency can control the visits to the Website and adjust its contents to your personal need. A cookie is a small information package (file) which often carries an anonymised individual ID. When you visit a website, the website asks your computer to store that file in a part of the hard disc of your computer which is expressly used to store cookies. Each individual website you visit can send a cookie to your computer if the settings of your browser allow it. However, in order to protect your data, your browser will only allow the particular website to access only the cookie that the particular website sent to your computer, i.e., one website cannot have access to cookies embedded by other websites. In general, the browsers are configured to accept cookies. However, if you do not wish to accept cookies, you can set up your browser to reject their acceptance. In that case, some components of the website may not function effectively when you browse on it. The cookies cannot obtain other information from the hard disc of your computer and do not carry viruses.

Used cookies on the Website:
Necessary category:

Necessary cookies help make a website usable by enabling basic functions like page navigation and access to secure areas of the website. The website cannot function properly without these cookies.

COOKIE NAME	PROVIDER	TYPE	EXPIRE
language	360dbp.com	http	1 year

Statistical category
Statistic cookies help website owners to understand how visitors interact with websites by collecting and reporting information anonymously.

COOKIE NAME	PROVIDER	TYPE	EXPIRE
_ga	google	http	2 years
_gat	google	http	1 year
_gid	google	http	1 day

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

SAFETY OF THE DATA PROCESSED BY US

The Agency arranges for creating backups that are suitable according to the IT data and the technical environment of the Website. The backups are stored according to the criteria applicable to the retention period of the specific data and, thereby guaranteeing the availability of data during the retention period, after which they will be finally destroyed. The IT system and the integrity and operability of the environment storing the data are checked with advanced monitoring techniques and the required capacities are provided constantly. The events of the IT environment are registered with complex logging functions, thus ensuring subsequent detectability and legal proof of any data breach. We use a high broadband, redundant network environment to serve our websites, with which any load can be safely distributed among the resources. The disaster tolerability of our systems is scheduled and guaranteed, and we use organisational and technical instruments to guarantee high-level business continuity and constant services to our users. The controlled installation of security patches and manufacturer updates that also ensure the integrity of our information systems is a key priority, thus preventing, avoiding and managing any access or harmful attempt involving the abuse of vulnerability. We apply regular security tests to our IT environment, during which the detected errors and weaknesses are corrected because enhancing the security of our information system is a continuous task. High-security requirements are also set for our staff, which also include confidentiality, and compliance with which is ensured with regular training. During our internal operation, we try to use well designed and controlled processes. Any personal data breach detected during our operation or reported to us is investigated transparently, with responsible and strict principles within 72 hours. The actual data breaches are all processed and recorded. During the development of our services and IT solutions we arrange for complying with the principle of installed data protection, as data protection is a priority requirement even in the design phase.

INFORMATION REGARDING THE RIGHTS OF THE 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.

PROCESSING AND REPORTING DATA BREACHES

Data breach is any event that, in connection with personal data processed, transferred, stored or managed by the Controller, 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 Controller warrants that the data is processed in full compliance with the provisions of the effective legal rules.

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

The document is valid from 01/11/2024.