PRIVACY POLICY

We, Attractive Line Kft., as a data controller (hereinafter: Data Controller, we) **hereby inform the data subjects** (visitors of the Website, those interested in modelling careers, the models we represent, and the contacts of our business partners) **that, respecting their data privacy and their right to information self-determination, during our data processing we act in accordance with the provisions of this Privacy Policy** (hereinafter: Privacy Policy, Policy).

I. GENERAL INFORMATION REGARDING DATA PROCESSING

1. WHAT DOES DATA PROTECTION MEAN AND WHY IS IT IMPORTANT?

Data protection is an important means of protecting the privacy.
Its purpose is to protect the informational self-determination rights of data subjects and to prevent unauthorized persons from accessing personal data.
The principles, rules, and procedures that ensure the lawful data processing and the protection of the data subjects do not actually protect the data, but its owner.

2. OUR COMMITMENT TO THE PROTECTION OF PERSONAL DATA

In the course of its business activities, the Data Controller processes the personal data of the following data subjects (hereinafter: Data Subject, Data Subjects, You):

- visitors and users of the Website,
- those interested in a modelling career,
- the models it represents,
- those interested in our services,
- contact persons of business partners who use our service.

In this Privacy Policy, and wherever your personal data is used, we provide concise, transparent and intelligible information about the method, purpose and circumstances of data management, using clear and plain language.
In all cases, the personal data made available to us will be handled in accordance with the applicable Hungarian and European Union data protection legislation and legal practice, and in all cases we will take the technical and organizational measures for ensuring the security of the processing. Respecting the basic principle of accountability, we continuously provide up-to-date and comprehensible information about our data processing activities.

In view of changes in legislation and the continuous development of jurisprudence, as well as changes in the services we offer, we reserve the right to continuously update the Privacy Policy.
The current and previous versions of the Privacy Policy are available in the footer of the website https://attractive.hu.

3. DEFINITIONS

Knowledge of the basic concepts of data protection is essential for the interpretation of this Privacy Policy. The definitions are contained in Article 4 of the GDPR, from which we highlight the following:
‘Personal data’ means any information relating to an identified or identifiable natural person ("data subject");
‘An identifiable natural person’ is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
’Data subject’ is any identified or identifiable natural person, whose personal data is processed by the controller responsible for the processing;

'Special categories of personal data' are personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, as well as genetic and biometric data for the unique identification of natural persons, health data and the sexual life or sexual orientation of natural persons; personal data which are prohibited under Article 9 (1) of the GDPR may be processed only in the exceptional cases provided for in Article 9 (2) of the GDPR, in particular with the express consent of the data subject;
'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means
'Data processing operations' are collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
'Disclosure' is making the data available to anyone;
'Deletion of data' is making data unrecognizable in such a way that their recovery is no longer possible;
'Filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;
'Restriction of processing' means the marking of stored personal data with the aim of limiting their processing in the future;
'Profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;
'Pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;
'Controller or controller responsible for the processing' is anyone who determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.
'Processor' is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
'Consent of the data subject' is any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;
'Recipient' is a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;
'Third party' is a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;
'**Personal data breach'** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

4. PURPOSE OF PRIVACY POLICY
The purpose of this Privacy Policy is to provide easily transparent and understandable information for those concerned that
o how we collect your personal data on the Website, for what purpose we use it, and according to what principles and rules we process your personal data,

o what personal data is processed during the recruitment, representation of Models and the agent activity, as well as during contact with our business partners,
o under what circumstances we may transfer your personal data to others and
o what rights you can assert in relation to the management of your personal data.

5. PERSONAL AND OBJECTIVE SCOPE OF THE GENERAL DATA MANAGEMENT INFORMATION

The personal scope of this Policy is extended
• to Website visitors and stakeholders contacting the Data Controller via the Website,
• to model candidates who come into the Data Controller's view during model recruitment and selection,
• Models represented by the Data Controller,
• to the Clients of the Data Controller, for whom the Model is mediated,
• to the business partners of the Data Controller, as well as,
• to the Data Controller and Data Processors.

In this Privacy Policy, the Data Controller provides detailed information on the essential circumstances, methods, principles, legal basis, purpose and duration of data processing related to its business activities.

6. PRINCIPLES OF DATA PROCESSING

PRINCIPLE	MEAINNG
a. Lawfulness, fairness and transparency	Data processing must be lawful, fair and transparent in relation to the data subject during the entire period of data processing.
b. **Purpose limitation**	We can only process your personal data for a clearly defined, legitimate purpose, and the collection of data and other data processing operations must be aligned with the purpose of data processing. It follows from the principle of purpose limitation that personal data can only be processed until the purpose of data processing is achieved.
c. **Data minimisation**	Only those personal data can be legally processed that are adequate, relevant and limited to what is necessary in relation to the purpose for which they are processed.
d. Accuracy	The data stored in our filing systems must correspond to reality in the entire process of data processing. If the data is inaccurate or incorrect, based on your request, we will work with you to restore the accuracy of your personal data.
e. **Storage limitation**	The principle of storage limitation means that personal data can only be stored as long as the purpose of data processing is achieved. Personal data cannot be accumulated or stored indefinitely. To this end, we determine the duration of data processing and, if this is not possible, the criteria for determining the duration.
f. **Integrity and confidentiality**	As a data controller, we treat the personal data transferred to us confidentially. Your personal data

PRINCIPLE	MEAINNG
	can only be accessed by our employees and agents who are entitled to data processing based on their job or duties. We take care of the preservation of documents and files containing personal data with technical and organizational security measures in line with the state of the art and expected of similar organizations.
g. **Accountability**	As a data controller, we must be able to prove the lawfulness of data processing, i.e. compliance with the provisions of the GDPR. For the sake of accountability, we document our data processing activities in accordance with the provisions of the GDPR. We keep a record of the transfer and publication of the necessary information, the data processing we carry out, the measures we take for the sake of data security, prevention of data breach and inquiries related to data protection.

7. PROVISIONS REGARDING DATA PROCESSING OF MINORS

The legal representative can give consent to data processing on behalf of minors who have not reached the age of 14 and those otherwise incapacitated.
A minor who has reached the age of 14, as well as a data subject with otherwise limited legal capacity, may consent to data processing with the consent or subsequent approval of their legal representative.
If the minor with limited legal capacity becomes competent, he decides on the validity of his dependent legal declarations.

The Data Controller allows people over the age of 18 to make online contact through the form on its Website.
For those under the age of 18, it is recommended to contact and provide data by e-mail and in person, where the Data Controller has the opportunity to identify the legal representative during the necessary consent and the representation of the person concerned.

8. PROCESSING OF SPECIAL CATEGORIES OF PERSONAL DATA

In the course of its general operation, the Data Controller does not collect the special categories of personal data of the data subjects, however, in individual cases, personal data may be processed that fall under the special categories of personal data according to the GDPR, because

- in accordance with the Client's special request, they contain personal data on sexual orientation (e.g. non-binary) or
- health data are included in the assessment of suitability for the Model Task.

According to Article 6 (2) of the GDPR, this data is processed by the Data Controller exceptionally and in the event that

- the data subject has given explicit consent in accordance with point a) of Article 6 (2) of the GDPR;
- processing relates to personal data which are manifestly made public by the data subject

- data processing refers to personal data that the data subject has expressly made public in accordance with Article 6, Paragraph 2, Point e) of the GDPR.

9. WHO WILL BE AUTHORIZED TO HANDLE YOUR PERSONAL DATA?

We, as the Data Controller, determine the purpose and means of processing your personal data.

DATA CONTROLLER INFORMATION:

Company name: Attractive Line Agency Limited Liability Company
Headquarters: 1137 Budapest, Jászai Mari tér 6. 2nd floor Door 5
Tax number: 13257972-2-41
Company registration number: 01-09-726163
Managing Director: Orsolya Sára Fehér
E-mail address: attractive@attractive.hu

As a data controller, we treat the personal data provided to us confidentially. Your personal data can only be accessed by our employees and agents who are entitled to process data based on their job or duties.

II. DETAILED INFORMATION REGARDING CERTAIN DATA PROCESSINGS

1. PERSONAL DATA PROCESSED DURING ONLINE CONTACT FOR THE PURPOSE OF A MODEL CAREER

Data Subjects: Users of the Website who fill out the contact form, as well as model candidates contacted by the Data Controller on social media platforms, who wish to contact the Data Controller online for the purpose of building a modeling career
Personal data processed: first name, last name, date of birth, height, e-mail address, mobile phone number, weight, chest size, city, instagram link, waist size, hip size, tiktok link, photos
Source of data: over the age of 18 the data subject, in the case of a minor between the ages of 14 and 18 the data subject with the consent of the legal representative, under the age of 14 the legal representative
Purpose of data processing: provision of personal data necessary to assess suitability for the model task for the purpose of subsequent contact and contract conclusion
Legal basis for data processing: freely given consent of the data subject ot the legal representative of the minor data subject based on Article 6, paragraph (1) point a) of the GDPR; with regard to special categories of personal data, the explicit consent of the Data Subject in accordance with Article 9, paragraph (2) point a)
The data subject has the right to withdraw his consent at any time. Withdrawal of consent does not affect the lawfulness of data processing based on consent prior to withdrawal.
Duration of data processing: until the withdrawal of the data subject, but for a maximum of six months.
Possible consequences of failure to provide data: in the absence of personal data, the fundamental suitability of the relevant model for the tasks and the need for a personal interview and additional data collection cannot be judged
Does data transfer take place: yes, for principals and foreign agencies, who process the data as independent data controllers in accordance with their own privacy policy

2. PERSONAL DATA PROCESSED DURING MODEL CANDIDATES SEARCH ON SOCIAL MEDIA

Data Subjects: social media (Facebook, Instagram, Pinterest, etc.) users contacted by the Data Controller on social media platforms
Personal data processed: first name, last name, other data provided on social media platforms (e.g. date of birth, e-mail address, mobile phone number, city, photos)
Source of data: data subjects
Purpose of data processing: az Adatkezelő közvetlen üzletszerzése a modell jelöltek közösségi médiafelületeken történő felkutatása és direkt marketing üzenettel történő megszólítása során
Legal basis for data processing: legitimate interest related to the direct business contract of the Data Controller based on Article 6 (1) point f) of the GDPR (with reference to Article 47 of the GDPR)
(Balancing test is available upon request.)
Duration of data processing: until the data subject objects, but for a maximum of 6 months
Possible consequences of failure to provide data: in the absence of processed personal data, it is not possible to expand the Data Controller's business activities or the range of models it represents based on the Data Controller's active activities, the success of model recruitment based solely on the voluntary application of model candidates depends on chance
Does data transfer take place: no (with the exception of IT data processing)

2. PERSONAL DATA PROCESSED DURING PERSONAL CONTACT FOR MODEL CAREER OBJECTIVES DATA PROCESSED FOR THE PURPOSE OF CONTACTING ONLINE RADIO

Data Subjects: those interested in a modelling career who come into personal contact with the Data Controller and provide personal data
Personal data processed: first name, last name, date of birth, height, e-mail address, mobile phone number, weight, chest size, city, Instagram link, waist size, hip size, TikTok link, photos **Source of data:** over the age of 18 the data subject, in the case of a minor between the ages of 14 and 18 the data subject with the consent of the legal representative, under the age of 14 the legal representative, a scouter that searches for models
Purpose of data processing: provision of personal data necessary to assess suitability for the model task for the purpose of subsequent contact and contract conclusion
Legal basis for data processing: freely given consent of the data subject ot the legal representative of the minor data subject based on Article 6, paragraph (1) point a) of the GDPR; with regard to special categories of personal data, the explicit consent of the Data Subject in accordance with Article 9, paragraph (2) point a)
The data subject has the right to withdraw his consent at any time. Withdrawal of consent does not affect the lawfulness of data processing based on consent prior to withdrawal.
Duration of data processing: until the withdrawal of the data subject, but for a maximum of six months.
Possible consequences of failure to provide data: in the absence of personal data, the basic suitability of the relevant model for the tasks, as well as the need for a personal interview and additional data collection cannot be assessed
Does data transfer take place: yes, for principals and foreign agencies, who process the data as independent data controllers in accordance with their own privacy policy

3. PERSONAL DATA PROCESSED FOR THE PURPOSE OF ENROLLMENT IN THE MODEL CASTING DATABASE

Data Subjects: those interested in a modelling career with whom no model agent contract is concluded, but request their inclusion in the Data Controller's model casting database for the purpose of subsequent selection and contract signing
Personal data processed: first name, last name, date of birth, height, e-mail address, mobile phone number, weight, chest size, city, Instagram link, waist size, hip size, TikTok link, photos **Source of data:** over the age of 18 the data subject, in the case of a minor

between the ages of 14 and 18 the data subject with the consent of the legal representative, under the age of 14 the legal representative, a scouter that searches for models

Purpose of data processing: provision of personal data necessary to assess suitability for the model task for the purpose of subsequent contact and contract conclusion

Legal basis for data processing: freely given consent of the data subject ot the legal representative of the minor data subject based on Article 6, paragraph (1) point a) of the GDPR; with regard to special categories of personal data, the explicit consent of the Data Subject in accordance with Article 9, paragraph (2) point a)

The data subject has the right to withdraw his consent at any time. Withdrawal of consent does not affect the lawfulness of data processing based on consent prior to withdrawal.

Duration of data processing: until the withdrawal of the data subject, but for a maximum of two years. Before the deletion, the Data Controller sends an informational e-mail about the end of the data management period. If the data subject does not give his consent, his personal data will be processed for an additional - new max. two-year period, your data will be deleted.

Possible consequences of failure to provide data: in the absence of personal data, the basic suitability of the relevant model for the tasks, as well as the need for a personal interview and additional data collection cannot be assessed

Does data transfer take place: yes, for principals and foreign agencies, who process the data as independent data controllers in accordance with their own privacy policy

4. PERSONAL DATA PROCESSED FOR THE PURPOSE OF IDENTIFYING THE LEGAL REPRESENTATIVE

Data Subjects: legal representatives of persons contacting the Data Controller for the purpose of a modelling career

Personal data processed: name, birth name, place and time of birth, ID number (ID card, passport, driver's license), address, signature, bank account number

Source of data: the data subject

Purpose of data processing: proof of legal representation of the minor model/candidate model, provision of legal representation during the model agent contract and the data processing related to the model, as well as the granting of legal representative consent

Legal basis for data processing: regarding that for the validity of the declaration of rights of minors with limited legal capacity (between 14-18 years of age), he consent of the legal representative is required and the legal representative acts on behalf of the incapacitated minor (under 14 years of age) according to paragraph (1) of § 2:12 the Civil Code, processing is necessary for compliance with a legal obligation to which the controller is subject in line with Article 6, paragraph (1) point c) of the GDPR

Duration of data processing: until the duration of the data processing for minors

Possible consequences of failure to provide data: in the absence of personal data, the Data Controller cannot identify the legal representative

Does data transfer take place: no

5. PERSONAL DATA PROCESSED FOR THE CREATION AND PERFORMANCE OF THE MODEL AGENCY AGREEMENT

Data Subjects: persons selected by the Data Controller to perform the Model Task, whose representation and management the Data Controller intends to provide based on the model agent contract

Personal data processed: first name, last name, place and time of birth, age, address, mobile number, phone number, e-mail address, height, bust, waist size, hip size, body weight, shoe size, eye colour, hair colour, dress size, acting qualifications, language skills, other agency information registration, other personal data provided as comments about leisure activities, education, sports activities, having a driver's license, likeness, casting introduction video and audio recording, references, signature, in case of application for casting: agency serial number, previous years' advertising and model appearances, in the case of a diet, a nutrition diary, bank account number, identification card number

(identity card, passport), háziorvosi igazolás a Modell Feladatok ellátására való alkalmasságról
Source of data: over the age of 18 the data subject, in the case of a minor between the ages of 14 and 18 the data subject with the consent of the legal representative, under the age of 14 the legal representative, a scouter that searches for models
Purpose of data processing: creation and performance of the model agent contract, within this framework the performance of representative, managerial and agent activities for the Model, registration of personal data necessary to assess the suitability of the given Model Task, presentation of possible offers to the Model, inclusion of the Models on the Website reference display and for the purpose of facilitating an assignment.
Legal basis for data processing: data 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 based on Article 6, paragraph (1) point b) of the GDPR
Duration of data processing: for 5 years from the termination of the contract
Possible consequences of failure to provide data: in the absence of personal data, the Data Controller cannot represent the relevant Model, and during the performance of managerial and agent activities, it is not possible to recommend the relevant Model to principals or foreign agencies
Does data transfer take place: in the case of the data subject's consent, the data will be forwarded to the client, who will handle the data as an independent data controller in accordance with its own data management information.

6. DATA OF BUSINESS PARTNERS

Data Subjects: business partners who contract with the Data Controller as individuals (in particular, but not exclusively, principals, photographers and agents)
Personal data processed: surname, first name, residential address, content of the receipt, name, address and tax number in the case of a VAT invoice, name of the service used, quantity, purchase price, payment method, other personal circumstances related to the use of the service, data on the business card
Data source: the Data Subject
Purpose of data processing: the use of the agency services of the Data Controller model, the use of the business partner's services by the Data Controller, maintaining contact, registering and distinguishing partners from each other, fulfilling payment obligations, invoicing
Legal basis for data processing: data processing is necessary for the performance of the contract [GDPR Article 6 (1) para. point b)], in the case of invoicing data, GDPR Article 6 (1) point c), the (data processing is necessary to fulfil the legal obligation of the Data Controller, with regard to Section 169 (2) of the Accounting Act).
Duration of data processing: in the case of a contract, 5 years after the termination of the contract, with regard to invoicing data, In accordance with § 169, paragraph (2) of Accounting Act, 8 years, in the absence of a contract, up to 6 months from the date of contact
Possible consequences of failure to provide data: conclusion of a contract, performance of payment obligations and invoicing are not possible in the absence of processed personal data.
Does data transfer take place: no, with the exception of data processors providing IT services and hosting services

7. CONTACTS OF THE CONTRACTUAL PARTNERS COMPANIES CONTRACTING WITH THE DATA CONTROLLER

Data Subjects: employees of third parties designated as contact persons in the performance of the contract, who contract with the data controller, or persons in a legal relationship with them for other work purposes
Personal data processed: surname, first name, e-mail address, phone number, position, other data on the business card
Source of data: contractual partner of the Data Controller

Purpose of data processing: maintaining contact, fulfilling the rights and obligations arising from the contract.
Legal basis for data processing: in order to conclude, fulfil and terminate the contract, the legitimate interest in facilitating the cooperation of the parties and implementing communication between the parties based on Article 6, paragraph (1) point f) of the GDPR.
(An interest assessment test is available upon request.)
Duration of data processing: until the business relationship with the given contractual partner is terminated or there is no change in the contact person at the given contractual partner.
Possible consequences of failure to provide data: f concluding a contract, maintaining contact and fulfilling contractual obligations is not possible in the absence of processed personal data.
Does data transfer take place: no, with the exception of data processors providing IT services and hosting services

8. PERSONAL CONTRIBUTORS OF BUSINESS PARTNERS CONTRACTING WITH THE DATA CONTROLLER AS A BUSINESS COMPANY

Data Subjects: Models designated as personal contributors in the contract
Personal data processed: first name, last name, place and time of birth, age, address, mobile number, phone number, e-mail address, height, bust, waist size, hip size, body weight, shoe size, eye colour, hair colour, dress size, acting qualifications, language skills, other agency information registration, other personal data provided as comments about leisure activities, education, sports activities, having a driver's license, likeness, casting introduction video and audio recording, references, signature, in case of application for casting: agency serial number, previous years' advertising and model appearances, in the case of a diet, a nutrition diary, identification card number (identity card, passport).
Source of data: The contractual partner of the Data Controller, the concerned Models
Purpose of data processing: contact, fulfilment of rights and obligations arising from the contract
Legal basis for data processing: the legitimate interest of the Data Controller in the performance of model agency activities and the fulfilment of assignments undertaken as a model agency based on Article 6 (1) point f) of the GDPR.
(An interest assessment test is available upon request.)
In the case of a minor, the legal basis is the consent of the data subject based on Article 6 (1) point a) of the GDPR, which must be given by the legal representative on behalf of the minor.
Duration of data processing: for 5 years from the termination of the contract
Possible consequences of failure to provide data: fulfilment of contractual obligations and model agency activity is not possible in the absence of processed personal data.
Does data transfer take place: yes, for clients, foreign agencies, contributors to the Model Task (e.g. photographers)

9. DATA PROCESSING RELATING TO PERSONS COOPERATING IN OTHER LEGAL RELATIONS RELATING TO THE PERFORMENCE OF WORK

Data Subjects: natural persons who have a contract or business relationship with the Data Controller
Personal data processed: name, address, e-mail address, mother's name, place of birth, time, tax identification number, tax number, contact information, personal identification document, passport number, bank account number of natural person contributors (suppliers) contracting with the Data Controller
Source of data: the Data Subject
Purpose of data processing: the conclusion, fulfilment, termination of the contract between the Data Controller and the data subject, the fulfilment of the statutory preservation obligation for tax documents and accounting documents, the provability of the content of the contractual relationship in the event of a claim or legal dispute
Legal basis for data processing: The legal basis for data processing in the context of the registration of the contracting party's data is the performance of the contract based on Article 6 (1) point b) of the GDPR.

With regard to the issuance and preservation of accounting documents, the legal basis for data management is the fulfilment of the legal obligation of the Data Controller based on Article 6 (1) point (c) of the GDPR.
Duration of data processing: Based on the Data Controller's obligation according to § 169 of Act C of 2000 on accounting (hereinafter: "Accounting Act"), the accounting documents for 8 (eight) years after the termination of the Contract, in the event of a legal dispute, if the at a later date, fulfilling its legal obligation for 5 (five) years after the conclusion of the legal dispute
Does data transfer take place: no, with the exception of data processors

10. PHOTOS AND VIDEOS SHOWN ON THE DATA CONTROLLER'S SOCIAL MEDIA PAGES (FACEBOOK, PINTEREST, INSTAGRAM, TIKTOK)

Data Subjects: models represented by the data controller as mother agency
Personal data processed: name, image, video recording, sound, data on previous model tasks
Data source: data subject, or the legal representative, contractual business partner
Purpose of data processing: promotion of the agency and the models represented by the data controller as a mother agency, facilitating their selection and obtaining model commissions
Legal basis for data processing: data 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 based on Article 6, paragraph (1) point b) of the GDPR
Duration of data processing: until the content is deleted from our Facebook page
Possible consequences of failure to provide data: in the absence of data provision, the Data Controller cannot publish the photos, videos and previous works of the models, and cannot promote its model agency activity on its social media pages
Will data be transferred: no, with the exception of the data transfers of the social media third parties

III. WHO CAN WE SHARE YOUR PERSONAL DATA WITH?

TRANSFERS TO RECIPIENTS ACTING AS INDEPENDENT DATA PROCESSORS

As the mother agency, the Data Controller provides both domestic and foreign representation for the data subject Models, during which the personal data of the data subjects is also transferred.
The Data Controller's clients are typically film producers, modelling agencies, advertising agencies, fashion brands, media content providers, and photographers based in the European Economic Area ("EEA") and in countries outside it.

Domestically, the personal data of the data subject Model will be transferred to the representatives of the commissioning press bodies, agencies, and fashion brands in accordance with the provisions of the Individual Agent Agreement, who will act as independent data controllers in the course of their activities.

For the purpose of finding and mediating a **foreign** Model Task, the Data Controller transfers the personal data of the data subject Model to foreign agencies with headquarters or places of business within the EEA or outside the EEA.

In the case of data transfer within the EEA, the protection of personal data is ensured by the mandatory application of the GDPR.
In the case of data transfer outside the EEA, i.e. to a third country, the application of the rules contained in Chapter V of the GDPR guarantees that the level of protection of personal data guaranteed by the GDPR is maintained.

Data transfers outside the EEA based on an adequacy decision:

In the case of data transfers to the following 3rd country, the EU Commission's adequacy decision pursuant to Article 45 of the GDPR ensures an adequate level of protection corresponding to the GDPR, which is essentially the same:

- Japan,
- United Kingdom,
- New Zealand,
- South Korea,
- Israel,
- Switzerland.

Therefore, no specific authorization is required for these data transfers.

Data transfers outside the EEA based on appropriate safeguards:

In the absence of an adequacy e decision, the Data Controller strives to ensure that the protection of personal data during data transfer outside the EEA is ensured by the appropriate safeguards contained in Article 46 of the GDPR.

The Controller will transfer Models' personal data to countries that do not have an adequacy decision, using the standard data protection clauses adopted by the Commission, in accordance with Article 46(2)(d) of GDPR.

Derogations for specific situations:

In the absence of an adequacy decision pursuant to Article 45 or adequate safeguards pursuant to Article 46 - including binding corporate rules - personal data may be transferred or re-transferred to a third country or international organization in view of the following special circumstances:

(a) *the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards; (*
(b) *the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;*
(c) *(the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;*

Based on the derogations for specific situations, data is transferred to the following countries in particular:

- Turkey
- China
- Australia
- Greece
- Singapore
- Taiwan
- Hong Kong
- South Africa
- Argentina
- USA

DATA PROCESSORS

In the course of our business activities, we must also use the services of IT (e.g. storage, IT services, web development) and other technical service providers.
The data processors will process your personal data on our behalf, strictly according to our instructions and providing appropriate guarantees.
We may also share your personal data,:
• with our accountant in order to fulfil the company's bookkeeping and accounting obligations,
• with our auditors, lawyers and other consultants when we ask them for professional advice.

EXTERNAL SERVICE PROVIDERS

In connection with the provision of the Services, the Data Controller uses external service providers in many cases, which cooperates with external service providers.
Regarding the personal data managed in the systems of external service providers, the information is contained in the privacy policy of the external service providers. The Data Controller will do everything in its power to ensure that the external service provider processes the personal data transferred to it in accordance with the law and uses them exclusively for the purposes specified by the data subject or set out in this Policy.
The Data Controller informs the data subjects about the transfer of data to external service providers within the framework of this Information.
You can read more about the cookies and social media pixels used on the website in the Cookie Policy.

IV. DATA PROCESSORS

Some personal data provided to us may be transferred to the data processors engaged by us, in view of the purpose of the data processing. The data processors process the received personal data in accordance with the provisions of the data processing contract concluded with the data controllers and may not use them for other data management purposes.
Our permanently cooperating data processors are the following:

DATA PROCESSING ACTIVITY	NAME	ADDRESS, CONTACT
Website development and maintenance services	Schalk & Co. Bt.	Address: 2531 Tokod, Béke út 32. Website: https://schalk.hu/ E-mail: kapcsolat@schalk.hu
Hosting and e-mail service	Ruffnet Zrt.	Address: 2161 Csomád, Kossuth Lajos út 47. Website: https://www.ruffnet.hu/ E-mail: info@ruffnet.hu
Accounting and payroll services	Axisdesign Kft.	Address: 1037 Budapest, Vörösvári út 107. E-mail: mathe.andras@bonatax.hu
Invoicing, automatic invoice issuance	KBOSS.hu Kft.	Address: 1031 Budapest, Záhony utca 7. Website: https://www.szamlazz.hu E-mail: info@szamlazz.hu

GENERAL CONTRACTUAL TERMS OF DATA PROCESSING BY DATA PROCESSOR

In accordance with the GDPR, the data processor undertakes to:

(a) processes the personal data only on documented instructions from the Data Controller, including with regard to transfers of personal data to a third country or an international organisation;

(b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(c) takes all measures required pursuant to Article 32 of GDPR;

(i) the pseudonymisation and encryption of personal data;

(ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience processing systems and services;

(iii) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

When determining the appropriate level of security, it is necessary to specifically take into account the risks arising from data processing, which in particular arise from the accidental or unlawful destruction, loss, alteration, unauthorized disclosure or unauthorized access to personal data transmitted, stored or otherwise managed.

d) takes measures to ensure that natural persons acting under the control of the Data Processor and having access to personal data can only process personal data in accordance with the instructions of the Data Controller;
e) the Data Controller authorizes the Data Processor in advance to use an additional Data Processor;
f) if the Data Processor also uses the services of additional data processors for specific data processing activities performed on behalf of the Data Controller, it imposes the same data protection obligations on this additional data processor through a contract or other legal act established on the basis of EU or Member State law as in the Data Processing Agreement or other legal act are included, in particular that the further data processor must provide adequate safeguards for the implementation of appropriate technical and organizational measures and thereby ensure that the data processing complies with the requirements of the GDPR. If the additional Data Processor does not fulfil its data protection obligations, the Data Processor commissioning it is fully responsible to the data controller for the fulfilment of the obligations of the additional data processor;

g) taking into account the nature of data management, with appropriate technical and organizational measures, helps the Data Controller to the extent possible to fulfil its obligations to the Data Subject under GDPR III. with regard to responding to requests related to the exercise of your rights contained in chapter;
h) assists the Data Controller in accordance with Articles 32–36 of the GDPR. (Security of data management, Notification of the data protection incident to the supervisory authority, Informing the data subject about the data protection incident, Data protection impact assessment, Preliminary consultation) in fulfilling the obligations, taking into account the nature of the data management and the information available to the Data Processor;
(i) upon termination of the provision of the data processing service, at the discretion of the Data Controller, delete or return all personal data to the Data Controller and delete existing copies, unless Union or Member State law provides for the storage of personal data;
(j) provide the Data Controller with all information necessary to verify the data deletion or copies and to enable and facilitate audits, including on-site inspections, by the Controller or another auditor appointed by him. The Data Processor shall immediately inform the Data Controller if it considers that any of its instructions violate this GDPR or the data protection provisions of the Member States or the Union.
k) reports the data protection incident to the Data Controller within 72 hours of becoming aware of it. In said notification, at least:

(i) the nature of the data protection incident must be described, including – if possible – the categories and approximate number of Data Subjects, as well as the categories and approximate number of data affected by the incident;
(ii) the name and contact details of the data protection officer or other contact person providing additional information must be provided;
(iii) the likely consequences of the data protection incident must be described; as well as
(iv) the measures taken or planned by the Data Processor to remedy the data protection incident must be described, including, where appropriate, measures aimed at mitigating any adverse consequences resulting from the data protection incident.

j) provides the Data Controller with all information necessary to verify the deletion of data and copies, and which enables and facilitates audits conducted by the Data Controller or other inspectors commissioned by the Data Controller, including on-site inspections. The Data Processor shall immediately inform the Data Controller if it believes that any of its instructions violates this GDPR or national or EU data protection provisions.

l) supports the Data Controller in fulfilling the Data Subjects' requests to exercise one or more of their rights provided for in the GDPR;
m) if the Data Processor receives a request from any Data Subject to exercise one or more of the rights provided for in the GDPR, the Data Processor informs the Data Subject to contact the Data Controller directly with the request, and at the same time informs the Data Controller of the request without delay;
n) keeps all the records required in Article 30 (2) of the GDPR and, if the processing of personal data on behalf of the Data Controller makes this possible, makes these records available to the Data Controller upon request.

The Data Processor undertakes to handle the personal data it processes exclusively in accordance with the relevant legislation.
The Data Controller is entitled to check the performance of the activity specified in the contract, and in particular the method of storing and processing the personal data of the Data Subjects, once a year at a previously agreed time.
If the Data Processor suffers damage in connection with the Data Controller's activities, the Data Controller is obliged to compensate it. If the Data Processor initiates a claim for compensation or initiates proceedings in connection with the Data Controller's activities, the Data Controller is obliged to exempt the Data Processor from compensation, imposed fines, and penalties within 30 days.

V. EXTERNAL SERVICE PROVIDERS

A. Social media platforms
Data processing within social media platforms (e.g. Facebook, Instagram page) is always subject to the respective social media's own privacy policy, rules and practices, which are continuously published on the interfaces operated by the respective service provider.

EXTERNAL SERVICE PROVIDER	PRIVACY POLICY LINK	TERMS OF SERVICE LINK
Facebook	http://www.facebook.com/full_data_use_policy https://www.facebook.com/policy/cookies/	http://www.facebook.com/legal/terms?ref=pf
Google	https://www.google.com/intl/hu/+/policy/	https://www.google.com/intl/hu/+/policy/pagesterm.htm
Instagram	https://help.instagram.com/196883487377501	https://help.instagram.com/581066165581870
Tiktok	https://www.tiktok.com/legal/page/eea/privacy-policy/hu-HU	https://www.tiktok.com/legal/page/eea/terms-of-service/hu-HU
Pinterest	https://policy.pinterest.com/en/privacy-policy	https://policy.pinterest.com/en/terms-of-service

B. Web analytics third-party companies
For the operation of our web-based services, we occasionally use the services of external web analytics and ad serving companies.
Web analytics and ad serving providers use measurement pixels in addition to cookies for the purpose of collecting information related to the measurement of user habits and the serving of advertisements.

VI. DATA SECURITY

In the course of our data processing, in order to ensure the security of personal data, in compliance with our obligations under the GDPR, we take all the technical and organizational measures and develop the procedural rules that are necessary to enforce the data security regulations.

We ensure the security of processing with technical and organizational measures that provide a level security appropriate to the risk.

We treat the personal data we process as confidential and take appropriate measures to protect against accidental or unlawful destruction, loss, alteration, damage, unauthorized disclosure or unauthorized access.

In order to protect the data files processed electronically in the various registers, an appropriate technical solution must be used to ensure that the data stored in the registers cannot be directly linked and assigned to the data subject.

Our computer systems and other data storage locations used in the provision of our services are located at your headquarters and at your data processors, in a closed room.
Our IT systems and the IT systems and networks of our partners are protected against computer-assisted fraud, espionage, sabotage, vandalism, fire and flood, as well as computer viruses, computer intrusions and denial-of-service attacks. We take care of security with server-level and application-level protection procedures.
During electronic data processing and registration, we use a computer program that meets the requirements of data security. The program ensures that only those persons who need it in order to perform their duties have access to the data under controlled conditions.

Data Controller has established and maintains a comprehensive data security system (the 'Data Security System'), which includes administrative, technical, physical and organisational measures and guarantees (including, where necessary, pseudonymisation and encryption) to ensure the confidentiality, security, integrity and accessibility of personal data and to protect them from unauthorised access, use, sharing, alteration and destruction.
Data Controller reviews the efficiency of the Data Security System or has it reviewed by an independent expert at least annually.
The Data Security System includes in particular, but is not limited to, the following measures and guarantees:
(a) Access control: Policies, procedures, physical and technical specifications and practices that
(i) physically restrict access to the IT system and paper-based documents and their storage facilities to duly authorised persons;
(ii) ensure that persons in contact with the Data Controller who need it have access to the personal data, but those who do not need it do not have access rights;
(iii) allow access only to authorised persons and prevent persons in contact with the Data Controller from disclosing personal data to unauthorised third parties; and
(iv) encrypt or decrypt personal data as necessary.
(b) Provision of information and training: It provides the staff and management of the Data Controller necessary to comply with it.
(c) Data breach management procedures: Policies and procedures for the detection and management of data breach, including the monitoring of systems, the detection of actual or attempted attacks or interventions against personal data or related systems, and the identification and response to suspected or proven data breach, reducing their adverse consequences, and documentation related to the data breach.
(d) Crisis scenario: Policies and procedures for taking steps required in the event of an emergency that damages or threatens to damage personal data (e.g. fire, vandalism, breakdown, natural disaster), including backup and data recovery plans.
(e) Restrictions on the use of devices and media: Policies and procedures regulating the procurement, installation and removal of hardware devices and electronic communications equipment at the place of business of the Data Controller and the movement of equipment within that place of business, including rules on the permanent erasure of personal data and the removal of personal data before the recycling of hardware devices and electronic communications equipment. The Data Controller prohibits and prevents the downloading or storage of personal data on portable devices.

(f) Monitoring: Hardware, software and/or procedural solutions to record and investigate operations in electronic information systems, including data security-related logging and reporting.
(g) Data integrity: Policies and procedures that ensure the confidentiality, integrity and availability of personal data and protect them from unauthorised sharing, alteration and destruction.
(h) Storage and transfer security: Technical security measures to prevent unauthorised access to personal data transmitted over an electronic network, including the encryption of personal data transmitted or stored in electronic form in systems or networks to which persons not authorised to access the personal data may also gain access.
(i) Designated Safety Officer: The Data Controller has appointed the Managing Director as its Security Officer, who is responsible for the development, operation and maintenance of the Data Security System.
(j) Testing: The Data Controller regularly tests the main controls, subsystems and procedures of the Information Security System to verify that they are properly applied and efficiently address identified threats and risks.
(k) Adaptation: The Data Controller monitors and evaluates the Data Security System and adapts it as necessary in the light of the latest technical and industry data security developments, the sensitivity of personal data, external or internal threats to the Agency or the personal data and changes in the business structure of the Agency (e.g. mergers, acquisitions, alliances, joint ventures, outsourcing, changes in information systems).

The existing security measures are sufficient to manage the risks, based on the current state of technology and the experience gained from our activities so far.

VII. RIGHTS AND OBLIGATIONS RELATING TO PERSONAL DATA BREACH

A PERSONAL DATA BREACH is when personal data or data are accidentally or unlawfully:

- destroyed,
- lost,
- altered,
- communicated unauthorized, or
- made unauthorized.

The GDPR imposes a notification obligation on the Data Controller, depending on the extent to which the incident endangers the rights and freedoms of natural persons.
Pursuant to Article 33 of the GDPR, the Data Controller is obliged to notify the incident to the competent supervisory authority without undue delay and may waive this incident only if the personal data breach is not likely to endanger the rights and freedoms of natural persons.
If the personal data breach occurs in connection with the activities of the data processor, it is obliged to notify it to the Data Controller without undue delay.
Upon the occurrence of a personal data breach, the Data Controller shall immediately take measures to remedy the personal data breach, taking into account the mitigation or prevention of any adverse consequences arising from the incident.
The Data Controller keeps a record of personal data breaches.
The purpose of the register is to enable the Data Controller to verify compliance with the GDPR during the audit of NAIH as the competent supervisory authority.
The Data Controller shall report the data breach to the NAIH without undue delay and, if possible, no later than 72 hours after the data breach became known to the NAIH, unless the data breach is likely to pose no risk to the rights and freedoms of natural persons.

The Data Controller is obliged to inform the data subject without undue delay about the personal data breach if it poses a high risk to the rights and freedoms of natural persons. If a high-risk personal data breach affecting the personal data of the data subject occurs during the data processing of the Data Controller, the Data Controller will inform the data subject of the following facts and circumstances:

description of the personal data breach,

- the name and contact details of the contact person responsible for data protection matters,
- a description of the likely consequences of the personal data breach,
- a description of the measures planned or taken by the controller to remedy the incident, including measures to mitigate any adverse consequences of the personal data breach.

VIII. RIGHTS OF THE DATA SUBJECT

The data subject may contact the Data Controller regarding the enforcement of his / her rights related to data management and his / her questions at the contact details included in this Privacy Policy.
The Data Controller shall inform the data subject of his / her actions or the reasons for their non-compliance within one month after the submission of the data subject's request (the data subject may file a complaint in this connection), this period may be extended by 2 months if necessary.
The procedure is free of charge (if justified and not excessive) and preferably electronic.
The Data Controller shall inform all recipients to whom or with whom the personal data have been communicated of any rectification, erasure or restriction of data processing, unless this proves impossible or requires a disproportionate effort. Upon request, the Data Controller shall inform the data subject of these recipients.

RIGHTS OF THE DATA SUBJECT	DETAILS
a. **Right to transparent information**	You have the right to receive clear, transparent and easy-to-understand information about how we process your personal data and what rights you can assert in relation to data processing. We fulfil this obligation in this privacy Policy.
b. **Right of access by the data subject**	You have the right to receive information about whether we process your personal data and - if we do so - which of your personal data and how we process them. The purpose of this is to make our data processing activities concerning you transparent for you, so that you can check whether we comply with the data protection legal regulations. We may deny access to your personal information only if it could reveal personal information about another person or would otherwise negatively affect another person's rights.
c. **Right to rectification**	You can ask us to take reasonable measures to correct your personal data if, in your opinion, we handle your personal data inaccurately.
d. **Right to erasure**	This right is also known as the ‘right to be forgotten’ and allows you to ask us to delete or remove your personal data if there is no compelling reason for us to continue processing it or if its use is unlawful. The

RIGHTS OF THE DATA SUBJECT	DETAILS
	right to deletion is not general, there are exceptions, e.g. if protection against legal claims justifies the processing of your personal data.
e. **Right to restriction of processing**	You have the right to "block" or disable the further use of your personal data until we have decided your request for correction or as an alternative to deletion. If processing is limited, we may still store your personal data, but we may not use it further without your consent or authorization by law. In order to comply with the restriction, we keep a list of those who have "blocked" the use of their personal data.
f. **Right to data portability**	You have the right to receive the personal data processed by us on a data carrier and forward them to another data controller - provided that the processing of your personal data is based on your consent or the contract between us, or the data processing is done in an automated manner.
g. **Right to object**	You have the right to object to the processing of your personal data on grounds related to your particular situation, if the data processing is based on a legitimate interest. In this case, we can only continue processing your personal data if we can prove that the data processing is justified by compelling legitimate grounds that take precedence over your interests, rights and freedoms, or that are related to the establishment, exercise or defense of legal claims.
h. Right to a remedy	In the event of a violation of your rights, you can contact the Hungarian National Data Protection and Freedom of Information Authority (NAIH) or a court, the method of which will be explained below.

During the exercise of the data subject's rights, we will inform you about the decisions made following your request and the planned or implemented measures without undue delay, but no later than thirty days from the receipt of the request. We provide the information through the same channel that you used when submitting the request, unless you specifically request otherwise.

IX. WHERE CAN YOU GO IF YOU HAVE A QUESTION OR WANT TO GET A LEGAL REMEDY?

If you would like to request additional information regarding the processing of your personal data or wish to exercise any of the above rights of the data subject, and if you are not satisfied with the way we have processed your personal data, please contact us!
If you have any questions or comments, you can contact the Data Controller directly:

E-mail: attractive@attractive.hu

Please provide as much information as possible to help us identify the information you are requesting, the action you want to take, and why you think it should be done.
Before evaluating your request, we may ask for additional information in order to identify you. If you do not provide the requested information and as a result we are unable to identify you, we may refuse to fulfil your request.
You can submit requests related to our services in writing by e-mail.
In the same way, we consider a request received from the e-mail address previously provided to us as a request received from the data subject.
In the case of claims submitted from other e-mail addresses and in writing, the person submitting the complaint or claim must prove his/her involvement accordingly. In the absence of proof of involvement, we are unable to assess or fulfil the request.
We usually respond to your request within one month of its receipt. We may extend this period by another two months if necessary, taking into account the complexity and number of requests you submit.
We do not charge a fee for such communications or our activities, except:
- if you request additional copies of the processed personal data, we may charge our reasonable administrative costs, or
- if you submit manifestly unfounded or excessive requests, especially due to their repetitive nature, in which case we may charge our reasonable administrative costs or refuse to fulfil the request.
Complaints, questions and requests sent to us are stored for 6 months from the date of submission and then deleted, with the exception of correspondence arising from cases that are still in progress. If a legal claim arises in the case, the data will be preserved within the time limit for its enforcement - typically 5 years (see: Act V of 2013 on the Civil Code).

Data protection authority procedure
Hungarian National Data Protection and Freedom of Information Authority
(Nemzeti Adatvédelmi és Információszabadság Hatóság)

Headquarters: 1055 Budapest, Falk Miksa utca 9-11,
Mailing address: 1374 Budapest, Pf. 603.
Phone: +3613911400
E-mail: ugyfelszolgalat@naih.hu
Website: http://www.naih.hu

Right to go to court
In the event of a perceived violation of rights related to the handling of your personal data, you can also contact the competent court (contact details here: https://birosag.hu/torvenyszekek) or the Capital Court in the capital (1055 Budapest, Markó u. 27). At the choice of the data subject, the lawsuit can also be initiated before the court of the data subject's place of residence or residence.
Proceedings against the controller must be brought before the courts of the Member State in which the controller is established (Hungary) but may also be brought before the courts of the Member State of the habitual residence of the data subject.

X. AMENDING THE PRIVACY POLICY

As a Data Controller, we reserve the right to unilaterally amend this Privacy Policy at any time.
After the amendment, the user accepts the provisions of the Privacy Policy in force at all times with the next login, in addition, there is no need to ask for the consent of individual users.

3 May, 2023