Internal Guidelines on Personal Data Processing and Protection
for Avantgarde Prague s.r.o., Jáchymova 63/3, 110 00 Praha 1, Staré Město, Business ID No.: 27221687 / Tax ID No.: CZ 27221687 (hereinafter the Guidelines).

1. Introductory Provisions

1.1. Avantgarde Prague s.r.o., Jáchymova 63/3, 110 00 Praha 1, Staré Město, Business ID No.: 27221687 / Tax ID No.: CZ 27221687 entered into the Commercial Register maintained by the Municipal Court in Prague, Section C, Entry 105547 (hereinafter the Company or Controller) engages in business activities in particular in the area of brokering trade and services, operating a travel agency and tour guide activities in the area of tourism, operating cultural, cultural/educational and entertainment facilities, organizing cultural productions, entertainments, exhibits, trade fairs, shows, sales and similar events, advertising, marketing and media representation.

1.2. The business activities involve processing the personal data of customers (client matters), business partners (suppliers and subcontractors) and/or employees of the Company.

1.3. The Company is a data controller.

1.4. The Guidelines determine the controller's rules and technical and organizational measures for the protection and processing of personal data it gathers in the course of its business in accordance with the valid and effective legislation on personal data protection, especially but not exclusively Act No. 101/2000, on personal data processing, as amended, and Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (personal data protection regulations), in order to secure personal data processing in accordance with said legislation and the principles on which it is based.

1.5. The Guideline is binding for all employees of the Company (Employee) and Authorized Persons as defined below.

1.6. The contents of the Guideline are regularly reviewed, assessed and updated, at least once a year and at other times as needed.

1.7. The Guideline is publicly available to all the controller's employees as well as natural persons and employees whose personal data the controller processes.

2. Basic Terms

2.1. According to this internal regulation and legal regulations:

2.2. "**personal data**" means any and all information on an identified or identifiable natural person (hereinafter the "data subject"); an identifiable natural person means a natural person who can be directly or indirectly identified, in particular with reference to a certain identifier such as a name, identification number, location data, network identifier or one or more particular features of the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. The personal data the controller processes under this internal regulation means the personal data of the controller's employees and other natural persons whose data the controller acquires during its work activities;

2.3. "**data subject**" means natural persons who are employees of the controller or other natural persons ("controller's clients") whose personal data the controller processes during its work activities;

2.4. "**processing**" means any operation or set of operations with personal data or sets of personal data performed with or without using automated processes, such as collecting, recording, organizing, structuring, storing, adapting or amending, searching, viewing, using, transmitting, disseminating or otherwise disclosing, aligning or combining, restricting, erasing or destroying;

2.5. "**restricting processing**" means marking the personal data stored for restriction of processing in the future;

2.6. "**records**" mean any structured set of personal data available according to special criteria;

2.7. "**controller**" means a natural person or legal entity, public authority, agency or other entity that designates, on its own or in conjunction with other entities, the purposes and means of processing personal data; if the purposes and means of said processing are designated by European Union or member state

law, said law can designate the affected controller or special criteria for designating the controller;

2.8. "**processor**" means a natural person or legal entity, public authority, agency or other entity that processes personal data for the controller;

2.9. "**IT system**" means the IT system the Controller uses to manage orders, reservations, sales and personal data processing for clients - client matters;

2.10. "**client matters**" means customers and communication with customers;

2.11. "**Mastercard's data processing agreements(s)**" means the set of rules, standards and processes that are binding for suppliers and entities working with Mastercard Europe SA, Chaussée de Tervuren 198A, 1410 Waterloo, Belgium, hereinafter "Mastercard";

2.12. "**consent**" of the data subject means any free, concrete, informed and unambiguous expression of will by which the data subject agrees to the processing of their personal data by statement or other clear confirmation;

2.13. "**supervisory authority**" means the independent public authority established by the member state pursuant to Article 51 of the Regulation. The supervisory authority for the controller is the Personal Data Protection Office, registered office Pplk. Sochora 27, 170 00 Praha 7. The same authority is the supervisory authority for cross-border personal data processing. The company's managing director is designated to take legal actions and represent the controller before supervisory authorities;

2.14. "**authorized person**" means every employee of the controller who comes into contact with or processes personal data in the course of their employment with the controller. Authorized persons must be informed of the contents of this internal regulation and a written record must be made as confirmation. Authorized persons must be informed again in the event of any change in their work classification or other change resulting in a change in duties or scope of duties for the authorized person in relation to processing personal data. Access to personal data is only granted to authorized persons who have been informed of the contents of this internal regulation;

2.15. "**responsible person**" means the employee designated by the controller to meet the controller's rights and obligations under this

internal regulation with regard to data subjects and to be a point of contact between the controller and data subjects. The responsible person is not designated to take legal actions and represent the controller before supervisory authorities.

3. Personal Data Processing Principles

3.1. Personal data processing by the controller under this internal regulation is subject to the following principles in accordance with legal regulations.

3.2. Personal data must be:

3.2.1. processed in an appropriate, lawful and transparent manner in relation to data subjects (“lawfulness, appropriateness and transparency”);

3.2.2. collected for certain, specifically stated and legitimate purposes, and must not be further processed in a manner not compatible with those purposes;

3.2.3. appropriate, relevant and limited to the scope absolutely necessary in relation to the purpose for which it is processed (“minimizing data”);

3.2.4. accurate and updated as needed; all reasonable measures must be taken to delete or correct immediately any personal data that is inaccurate with regard to the purposes for which it is processed;

3.2.5. stored in a form allowing identification of the data subject for a period longer than absolutely necessary for the purposes for which it is processed (“restricting storage”);

3.2.6. processed in a manner that ensures appropriate security for the personal data, including protection by means of suitable technical or organizational measures from unauthorized or unlawful processing and accidental loss, destruction or damage (“integrity and confidentiality”).

3.3. The controller is responsible for adherence to paragraph 1 of the internal regulation and must be able to prove adherence.

4. Sources and categories of personal data

The controller acquires personal data from the following categories of data subjects:

4.1. customers - client matters through the reservation form on the controller's website for the purposes of performing the brokered agreement;
4.2. employees and associates;
4.3. third parties, controller's company operations, taxes, accounting, suppliers, subcontractors, etc.

5. Identifying personal data

5.1. client matters – first and last name, phone number, email;
5.2. employees and associates – first and last name, date of birth, Birth ID No., address, phone number, email, account number, health insurance company;
5.3. third parties, controller's company operations, taxes, accounting, suppliers, subcontractors, etc. – company's invoicing information, first and last name, email, phone number, address.

6. Purposes and lawfulness of personal data processing

The legal basis allowing us to process the personal data depends on the purpose for which we process specific personal data. In accordance with the Regulation the controller is entitled to store personal data:

6.1. on clients (client matters) collected during the ordering process only for the purposes of performing the brokered agreement with clients ("data subjects") of the controller and especially communication with the person ordering the services and if necessary for concluding and performing the agreement on provision of services and protecting our legitimate interests directly related to concluding or performing this agreement;
6.2. in other cases for the purposes of meeting legal obligations and as necessary to protect the controller's legitimate interests directly related to concluding or performing agreements.

The controller undertakes to refrain from using any personal data for marketing purposes or passing or disclosing personal data to third parties unless it does so in accordance with generally binding legal regulations, especially for the purposes of protecting the controller's legitimate interests.

7. Disclosing and granting access to data subjects' personal data to a third party

7.1. Legal basis for processing

The legal basis for processing data subjects' personal data is the fact that processing is necessary in order to meet the controller's legal obligations according to valid legal regulations.

7.2. The controller can disclose or grant access to data subjects' personal data to a third party in accordance with this internal regulation only to the following recipients:

7.2.1. suppliers for the purposes of performing under an agreement (client matters), i.e. the end provider of a service brokered by the controller;

7.2.2. state tax authorities and other authorities and suppliers in meeting the legal obligations stipulated by relevant legal regulations;

7.2.3. suppliers and subcontractors for the purposes of performing under an agreement.

7.3. The controller does not disclose any personal data to a recipient in another country or use the personal data for marketing purposes.

8. Time of storing data subjects' personal data

8.1. In accordance with the principle of restricting storage pursuant to the general data protection regulation, data subjects' personal data can only be stored for the time necessary to meet the purpose of the processing. After that time has passed, personal data can be stored exclusively for the purposes of archiving in the public interest, for scientific or historical research, or for statistical purposes, provided that the appropriate technical and organizational measures are taken as required by the Regulation in order to guarantee the data subjects' rights and freedoms. If processing for these purposes, it is important to take care to protect the personal data from unauthorized interference in data subjects' privacy and personal life, adhere to the principle of minimizing data, and anonymize personal data as soon as possible.

8.2. According to the Regulation, personal data can be processed for the relevant time in accordance with legal regulations and is safely processed / encrypted in the IT system's electronic database.

8.3. Time of storing:

8.3.1. customers - client matters through the reservation form on the controller's website for the purposes of performing the brokered agreement: 10 years after the end of the commercial relationship;

8.3.2. employees and associates;

8.3.2.1. from the hiring process: 1 month after acquiring the personal data;

8.3.2.2. from the employment agreement: 3 years after the end of the employment relationship;

8.3.2.3. record sheets: 3 calendar years after the year to which they apply;

8.3.2.4. records regarding recipients of old-age or disability pension: 10 years after the year to which the records apply;

8.3.2.5. wage sheets or accounting records on information necessary for the purposes of pension insurance: 30 years after the year to which the records apply;

8.3.3. third parties, controller's company operations, taxes, accounting, suppliers, subcontractors, etc.;

8.3.3.1. from an agreement: 10 years after the end of the commercial relationship;

8.3.3.2. accounting records: 5 years (financial statements and annual reports 10 years);

8.3.3.3. tax documents: 10 years after the end of the tax period in which the performance was provided.

9. Security for and method of processing personal data

9.1. The controller secures the personal data and processing in accordance with generally binding regulations and instructions pursuant to this internal regulation and the instructions of the responsible person. In the event of doubts or questions over securing personal data and processing, any questions should be

raised in advance regarding the correct procedure for the responsible person and then await a decision.

9.2. Taking into account the current technologies, implementation costs, nature, scope, context and purposes of processing, as well as risks of varying degrees of likelihood and severity for the rights and freedoms of natural persons, the controller will take appropriate technical and organizational measures to ensure the level of security appropriate to the level of security considering especially the risks presented by processing, in particular accidental or unlawful destruction, theft, loss, change, and/or unauthorized disclosure of the personal data disclosed, saved or otherwise processed, or unauthorized access to the same.

9.3. For the purposes of securing personal data protection the controller introduces technical measures and rules:

9.3.1. personal data may be processed and stored only using the IT system;

9.3.2. the IT system receives regular, daily backups in case of physical or technical incidents in order to keep the personal data renewed and available;

9.3.3. processing, transmission and storage of files with personal data is subject to TLS 1.2, AES-256 bit encryption;

9.3.4. only company employees who are authorized persons have access to the IT system;

9.3.5. every employee has their own access password for the IT system generated for each specific employee;

9.3.6. access to the IT system is only permitted via computers to which the employee has access also via a generated password that must be different from the password to the IT system;

9.3.7. the Company’s password management system aims to ensure password quality (at least 10 characters forming a combination of numbers, lowercase and uppercase letters) and methods of implementation for user authentication according to the Company’s needs in order to secure access to the Company’s IT system and computers. Among other things, the password management system requires users to change their passwords regularly and sets password parameters (e.g. duration or certain required

characters), automatic signout, monitoring number of signins, automatic blocking of suspicious signin attempts, creating and archiving all logs and signins by a particular employee;

9.3.8. the password management and authorization system is regularly checked and updated, contains disciplinary procedures and instructions for what to do with employees who attempt to acquire or have acquired unauthorized access to personal data, defines reporting for accesses, access procedures and change procedures, encrypting, backup and deletion of personal data;

9.3.9. entry to the Company's premises with IT equipment is physically secured and monitored, the premises have restricted access only to authorized Processors and Authorized Persons using magnetic cards and passwords, the premises are monitored by CCTV and security alarm;

9.3.10. employees' computers must be secured with a password as described above and have an updated antivirus program, legal operating system, and licenses for all software programs used;

9.3.11. the Company has taken measures to secure internet access with active firewalls and modems;

9.3.12. personal data acquired for different reasons for different clients of the Company is stored separately and cannot be combined, compared, edited or filtered. Individual databases also cannot be edited together even with the consent of the Authorized Persons.

9.4. The Company has a contractual cooperation with Mastercard Inc. and has entered into other mutual contractual relationships undertaking to uphold and perform under the "Mastercard's data processing agreement(s)", meaning the set of rules, standards and processes that are binding for suppliers and entities working with Mastercard. All Authorized and Responsible Persons in the Company undertake in writing to uphold the conditions and procedures defined in the "Mastercard's data processing agreement(s)" attached to the internal regulation and available in its current version online at: https://www.mastercard.com/global/en/vision/corp-responsibility/commitment-to-privacy/data-processing-privacy.html.

10. Instructions and rights of data subjects

10.1. In connection with processing the personal data, the data subject has the right to clear, transparent and comprehensible information on the manner in which we store the personal data and what rights the data subject has from the perspective of:

10.1.1. purpose of processing;

10.1.2. category of affected personal data;

10.1.3. recipient or category of recipients to whom the personal data is disclosed;

10.1.4. planned period for storing the personal data;

10.1.5. all available information on the source of the personal data.

10.2. Every data subject who discovers or believes that the controller is processing their personal data in conflict with the protection of their privacy and personal life or in conflict with legal regulations is entitled:

10.2.1. to require an explanation from the controller;

10.2.2. to require the controller to correct the situation, in particular to block, complete, correct or delete the personal data; the data subject is also entitled to contact the supervisory authority, i.e. the Personal Data Protection Office;

10.2.3. if the data subject's request is legitimate, the controller must correct the defective situation without delay;

10.2.4. if the controller does not correct the defective situation, the data subject has the right to contact the supervisory authority, i.e. the Personal Data Protection Office, Praha 7, Pplk. Sochora 27, 170 00, www.uoou.cz

11. Responsible Person

The Company's Responsible Person for personal data protection is Mr. Jan Rajniš, tel: +420 602 433 333, e-mail: jan@avantgardeprague.cz, whose office is at: Jáchymova 3/63,
110 00, Praha 1.

This Internal Regulation is available at the controller's registered office in hard copy and on the controller's website in simplified form, where it represents part of the General Terms and Conditions and Payment Conditions for the controller.

Internal Regulation version as of: 25.5. 2018