Pursuant to the provisions of the Act on the Implementation of the General Data Protection Regulation (OG 42/2018) dated 9 May 2018 (hereinafter referred to as: the Act) and the provisions of the General Data Protection Regulation (EU) No. 2016/679 of the European Parliament and the Council dated 27 April 2016 on the protection of natural persons with regard to the processing of personal data and the free movement of such data (hereinafter referred to as: the Regulation), **BRIJUNI RIVIJERA D.O.O.**, Marulićeva 1, Pula, VAT ID NO (OIB): 39582496872, as the data controller, on 15 July 2018 adopts the following

PERSONAL DATA PROTECTION

RULEBOOK

Article 1

The Rulebook shall govern the following

a) protection of individuals-natural persons with regard to the processing of their personal data (hereinafter referred to as: the data subject) in relation to the collection, processing, use and safekeeping of personal data,
b) responsibilities of the company BRIJUNI RIVIJERA D.O.O. as the data controller (hereinafter referred to as: the data controller),
c) rights of the data subject, and
d) implementation of organizational, personnel and technical measures for the protection of personal data,

with a view to ensure the implementation of the Regulation (EU) No. 2016/679 of the European Parliament and the Council dated 27 April 2016 on the protection of natural persons with regard to the processing of personal data and the free movement of such data.

Definitions of the terms relevant to the provisions of this Rulebook in relation to the Regulation

Article 2

"Personal data" means any information relating to a natural person who has been identified or is identifiable. An identifiable person is a person that 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. Personal data includes name, address, e-mail address, IP and MAC address, GPS location, RFID tags and web site cookies, phone number, photo, video footage of natural person, personal identification number, biometric data (fingerprint and iris recognition), genetic data, data on education and professional qualifications, salary data, credit information, bank account information, health information, sexual orientation, voice and any other data related to the real person, i.e. the owner of the personal data, which data may be used directly or indirectly to identify precisely that person.

"Processing" means any operation or set of operations that is performed on personal data or on personal data sets, whether or not by automatic means, such as collecting, recording, organizing, structuring, storing, adapting or modifying, retrieving, inspecting, using, disclosing by

transmission, dissemination, or otherwise making available, alignment or combination, blocking, erasure or destruction.

"Data Controller" means a natural or legal person, public authority, agency or other body which alone or jointly with others determines the purpose and means of processing personal data;

"Data Processor" means a natural or legal person, public authority, agency or other body processing personal data on behalf of the controller;

"Recipient" means a natural or legal person, public authority, agency or other body to which personal data is disclosed, whether or not a third party;

"Third Party" means a natural or legal person, public authority, agency or other body which is not data subject, controller, processor nor a person authorized to process personal data under the direct responsibility of the data controller or data processor;

"Consent" means 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;

"Storage System" means any structured set of personal data available under specific criteria, whether centralized, decentralized or scattered on a functional or geographical basis;

"Personal Data Breach" means a breach of security resulting in accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to personal data that has been transferred, stored or otherwise processed;

"Identifiable Person" means a person whose identity can be determined (directly or indirectly), in particular on the basis of an identification number or one or more features specific to his or her physical, psychological, mental, economic, cultural or social identity.

"Special Category of Personal Data" refers to racial or ethnic origin, political views, religious or other beliefs, trade union membership, health or sex life and personal data on criminal and misdemeanour proceedings.

Article 3

The data controller:

1. processes personal data of data subjects in a manner that is accurate, complete and up-to-date in all records in which the data is stored, irrespective of their form of keeping,
2. the personal data of the data subject:
    a) is collected by the data controller only
        – for the purpose the data subject is familiar with, as stated at collection, and
        – for the purpose of fulfilling its legal and other obligations in accordance with its activity
    b) is processed by the data controller only for the purpose for which the data has been collected, i.e. for the purpose that matches the purpose of its collection.
3. uses the personal data of the data subject only during the time necessary for accomplishing a particular purpose, unless a special law provides for a longer period

of time and, after the expiration thereof, has to be erased, unless a special law provides otherwise,
4. must provide technical measures for the protection of personal data,
5. must ensure the storage and archiving of personal data in the manner and within time limits complying with special legal regulations and by-laws that determine the time of keeping personal data, its erasure or destruction, and the conditions for their archiving.

Article 4

The data controller may, based on a contract in written form, entrust certain activities related to data processing within its scope of work to another natural or legal person (*data processor*).

The activities related to personal data processing may only be entrusted to the data processor who is registered for performing such activity and who provides sufficient guarantees with regard to the implementation of appropriate protection measures regarding personal data or classified information if he or she meets the requirements laid down in special regulations governing the field of information security.

Article 5

The data controller, based on a decision, appoints a responsible person and his/her replacement for each data processing operation specified in the preceding Article of this Rulebook, who shall be accountable to the data controller for the acts of employees within the processing department in accordance with the provisions of this Rulebook and responsible for the communication and provision of information to the data protection officer.

Article 6

Where another natural or legal person may have or has access under the contract to the personal data that the data controller collects and processes, such business relationship shall be governed by special provisions of the contract in accordance with the Regulation in the part relating to data confidentiality, protection against breach with the protection measures included.

Article 7

The data controller collects personal data relating to:

- employees, children and spouses of employees,
- bodies of a trading company (members of the board of directors, assembly, supervisory board (if any)),
- external associates,
- users of core business activity,
- business clients,
- members of the loyalty club (if any),
- contractual users.

Article 8

The data controller is obliged to handle personal data in accordance with positive legal regulations (laws, regulations, collective and other binding agreements, ordinances, etc.) governing the collection, processing and safekeeping of personal data of the data subject.

Article 9

In cases where personal data are not collected based on applicable legal regulations or contracts, the data controller shall, when collecting personal data, obtain consent for collecting and processing personal data from the data subject.

In the event the data controller processes the data based on a legitimate interest pursuant to the Regulation, the data controller is obliged to perform a balancing test to justify the legitimate interest.

Article 10

During the first contact with the data subject, the persons collecting personal data from the data subjects on behalf and for the account of the data controller are obliged to submit to the data controller:

a) Privacy Statement or
b) other document describing and informing the data subject on his/her rights, and in the event that consent is needed for the purpose of processing any of the data, they are obliged to obtain it, in compliance with the consent form.

After the Privacy Statement and the consent have been submitted to the data subject, the certificates of receiving the Privacy Statement and the consent will be handed over to the immediate superior or other person appointed by the latter at the end of the working day in order to be recorded in the central system of obtained consent forms and their archiving.

The consents will be kept for as long as the personal data which they refer to are kept, and after the need for their safekeeping ceases, they will be physically destroyed and the responsible person will make a record on their destruction and/or the data will be returned to the data subjects, all in accordance with the decision of the data controller.

If the data subject declares that a certain right is not clear to him or her or requests further clarification, the person collecting the data on behalf and for the account of the data controller is obliged to provide them to the data subject.

Article 11

If the data controller has not received the personal data from the data subject, at first communication the employees or the persons contacting the data subject on behalf of the data controller must provide the data subject with the following information:

a) identity and contact details of the data controller and the data controller's representative, as well as the contact details of the data protection officer,
b) purpose of processing for which the personal data are intended and the legal basis for processing,
c) category of the personal data being processed,
d) categories of recipients,
e) intention, if any, to transfer the data to a third country or an international organization,
f) period of storage, i.e. the criteria for determining the period,
g) if the processing is based on legitimate interests inform the data subject on the legitimate interest of the data controller,

h) right of accessing the personal data and correcting or erasing such data or restricting the processing related to the data subject and the right to object to the processing and the right to transfer the data,
i) right to withdraw consent,
j) right to file an objection with a competent body,
k) source of personal data,
l) information on whether there is automated processing of personal data.

Article 12

When processing personal data, the data controller is obliged to pay particular attention to the following deadlines and obligations:

- When the processing is based on the consent of the data subject, the data controller is obliged to obtain the personal data processing consent and must at all times be able to prove that the data subject gave the consent for his/her personal data to be processed,

- The data controller is obliged to submit, without delay and within one month at the latest, to the data subject all information regarding the processing of his/her personal data, which he/she is entitled to in accordance with the General Regulation. In case of complexity and multiple requests, the deadline may be extended by an additional two months, in which case it is necessary to inform the data subject thereof within one month of receipt of the request with an explanation for extending the deadline,

- In cases when the data has not been received from the data subject, the data controller is obliged to provide the data subject with information on the processing of his/her personal data in accordance with the provisions of the General Regulation, at the time of the first communication with the data subject and within one month from receiving the personal data at the latest,

- The data controller is obliged to inform the data subject of his/her right to object at the time of the first communication with the data subject,

- In the event of personal data breach, the data controller shall notify the supervisory authority without delay and no later than within 72 hours after having become aware of the breach. In case of delays in reporting, it is necessary to provide the supervisory authority with the reasons for the delay,

- In the event of personal data breach which, according to the data controller, is likely to cause a high risk to the rights and freedoms of the individual, the data controller is obliged to notify the data subject thereof without delay,

- When it is likely that certain processing will cause high risk for the rights and freedoms of the data subject, the data controller is required to carry out an assessment of the effect on data protection before any data processing starts,

- Where, on the basis of the assessment of the effect on data protection it has been established that processing, without additional risk mitigation measures, would result in a high risk for the rights and freedoms of the individual, the data controller shall consult the supervisory authority,

- The data controller is obliged to erase all personal data (or anonymize it) when the purpose for which they were collected is finished, when the consent of the data subject has been withdrawn, or when the contractual relationship ceased and in all other cases in accordance with the General Regulation and no later than upon the expiration of all legal obligations related to the safekeeping of personal data, unless an enforcement procedure for unpaid claims has been initiated or if a complaint has been made with regard to the product or service within the prescribed deadline, until the final completion of the complaint proceedings in accordance with the applicable regulations,

- In cases when an amendment, modification or erasure of the personal data was made at the request of the data subject, the person to whom the personal data relate and the recipients of the personal data have to be informed thereof within 30 days of the correction.

Article 13

The requests in which the data subject requests any of his/her rights from the data controller under the Regulation must be made in writing.

The data controller is obliged to respond to the request of the data subject in the shortest possible time, but no later than within one month from the date of receiving the request.

When submitting the request, it is necessary to determine the identity of the person who submits the request by inspecting his/her ID card or passport.

It is not possible to act upon the request before clearly identifying the data subject's identity.

The data controller must not convey any personal data to the person before determining his/her identity.

Technical protection measures

Article 14

The data controller is obliged to ensure that only authorized persons have access to personal data at least in the following way:

a) to regularly modify passwords used to unlock computers, at least once every three months,
b) computer unlocking passwords are kept in a safe manner and can be accessed only by persons put in charge of processing based on the data controller's decision,
c) passwords by the number of characters and complexity provide the highest level of protection,
d) to prevent the expired passwords from being reused,

e) there is a system that will alert the data controller in the event of unauthorized access to personal data,
f) after a certain number of failed attempts to enter an incorrect password, the computer is automatically locked.

Article 15

The data controller is obliged to ensure the protection of the IT system, by ensuring that the IT network and systems are protected from:

- fire
- floods,
- loss of power,
- unauthorized access,
- and use antivirus protection,
- encryption and
- pseudonymization of data where possible as well as other appropriate measures to ensure the highest level of information security.

In order to avoid unauthorized access to personal data, the data in writing is stored in filing folders, locked cabinets, safes, and the data in the computer is protected by assigning a username and password known to employees who process the data, and for further security and confidentiality measures the data is stored on portable storage medium and backed up on a server.

Data protection officer

Article 16

The data controller will appoint a data protection officer.

The data protection officer may also be a person who is not an employee of the data controller.

The data protection officer reports directly to the responsible person of the data controller and may not receive instructions from other data controller's employees and is in charge of direct contact with the competent supervisory authority.

The data controller is obliged to publicly disclose the contact details of the data protection officer on its website and in any other appropriate way.

Article 17

The data protection officer must have the skills and expertise that imply:

a) expertise in national and European laws and practices in the field of personal data protection, including a deeper understanding of the Regulation,
b) active understanding of the implementation of the processing operations,
c) understanding of information technologies and the security of personal data,
d) knowledge of the business management system and work organization of the data controller,
e) ability to promote the culture of personal data protection within the data controller's business activity.

Article 18

Depending on the nature of the processing operations of the said business activity and the size of the data controller, the data protection officer shall be provided with the following:

a) active support by the senior management to the data protection officer's function,
b) sufficient time for the data protection officer to fulfil his/her duties,
c) adequate support regarding financial resources, infrastructure (premises, facilities, equipment) and, where appropriate, staffing,
d) official notification of the appointment of data protection officer addressed to all persons,
e) access to other departments within the organization so that the data protection officer can receive the necessary support, contributions or information from these departments,
f) continuous training.

Article 19

The data controller shall not:

a) give instructions to the data protection officer on how to perform his/her tasks,
b) dismiss the data protection officer or punish him/her for performing his/her duties,
c) allow a conflict of interest in relation to other possible tasks and duties.

The data protection officer shall not be:

a) a legal representative of the data controller,
b) a person who collects and processes personal data,
c) head of department for marketing, publicity,
d) head of the human resources department,
e) head of the IT department,
f) or any other person with a senior management position or a person who in his/her position determines the purpose and manner of processing personal data.

Appointment of an external data protection officer

Article 20

The data controller may designate and appoint an external natural or legal person who is not employed with the data controller to be the data protection officer based on a contract on performing the operations of a data protection officer pursuant to the Regulation and this Rulebook, in particular taking into account the provisions of the preceding articles of this Rulebook relating to data protection officers.

The external data protection officer must guarantee to the data controller that he/she possesses the professional knowledge, necessary resources and reliability for implementing technical and organizational measures that, when processing personal data under the contract, apply in accordance with the regulations in the field of personal data protection, the Regulation and this Rulebook, directly or indirectly through external professional associates.

Records of processing activity

Article 21

The data controller as well as the data processor, if any, pursuant to Article 30 of the Regulation must make and maintain a record of processing activities where he/she will show the following information:

a) name and contact details of the data controller
b) name and contact details of the data protection officer;
c) processing purposes;
d) description of categories of data subjects,
e) description of categories of personal data;
f) categories of recipients to which the personal data have been or will be disclosed,
g) deadlines for erasing different categories of data;
h) general description of the technical and organizational safety measures referred to in Article 32, paragraph 1. 2.

The record referred to in the above paragraph of this Article of the Rulebook must be made in writing, including the electronic form.

The obligations referred to in this Article of the Rulebook shall apply to:

a) a legal person employing more than 250 persons,
b) if the data processing conducted is likely to cause a high risk to the rights and freedoms of the data subjects,
c) if the processing is not temporary and if it involves specific categories of data referred to in Article 9 (1) of the Regulation or
d) in case of personal data regarding criminal convictions and punishable offences

The person authorized to represent the data controller will appoint a responsible person to keep records of processing activities.

Privacy impact assessment

Article 22

The data controller shall make a privacy impact assessment in the event of the conditions set out in the Regulation which require an assessment of the impact on privacy to be made when processing special categories of personal data as well as where it has been established that personal data may cause a high risk to individuals' rights and freedoms.

In case of new types of processing that, by means of new technologies and taking into account the nature, scope, context and purpose of processing, could cause high risk to individuals' rights and freedoms, prior to the processing, the data controller is obliged to make and assessment of the impact of the foreseen processing operations on the protection of personal data.

When evaluating the impact on privacy, the data controller is required to seek advice from the data protection officer.

Storage and safekeeping of personal data

Article 23

With regard to the manner of storage of archival material and time of its safekeeping, the data controller has to comply with the legal regulations and the general act, which cover personal data of the data subject regarding the manner and time of storage and safekeeping, technical protection measures as well as premises and equipment of the premises the data is stored in.

The employee records are kept starting from the date of employment and are ceased to be kept on the date of termination of employment. The personal data of employees are documents of permanent value that are kept under the statutory regulations and the general act on the protection of archival and registry materials with document retention deadlines.

The records of members of company's bodies (members of the board of directors - director, supervisory board, assembly) are kept starting from the date of their appointment/entry in the court register, and are ceased to be kept on the date of termination of their mandate/leaving the company. This personal data represent documents of permanent value that are kept under the statutory regulations or the general act.

The records of citizens and external associates shall be kept from the moment of filing an application or from the moment of concluding a contract, and shall cease to be kept upon the realization of the purpose for which the data was collected. The data is kept in compliance with the legal regulations or the general act.

Providing personal data to other users

Article 24

The personal data collected and processed by the data controller are provided to other users based on a written request if this is necessary for the performance of activities within the legally established activity of such a user.

Prior to giving personal data to other users, the data controller shall inform the data subject thereof (verbally, electronically).

A special record is kept of the personal data given to other users, the other user and the purpose for which the data is given.

Responsibility of the person collecting and processing personal data

Article 25

The professional and administrative staff of the data controller who collects and processes personal data (appointed and designated by the data controller) is responsible for:

a) acting in accordance with the Regulation, the Rulebook and other acts and decisions relating to personal data of data subjects,

b) taking all personal data protection measures necessary to protect personal data against accidental loss or destruction, unauthorized access or unauthorized changes, unauthorized disclosure and any other misuse,

which omission constitutes a particularly serious misconduct for which an extraordinary termination of employment may be imposed on the perpetrator.

The aforementioned persons are obliged to sign a Statement of Confidentiality that will bind them to do the following:

a) keep confidential all personal data that they have the right and the authorization to access and that are contained in personal data collections
b) use personal data exclusively for a specific (prescribed) purpose
c) use personal data only as long as necessary to achieve the purpose for which they have been collected and will not process them further for any other purpose
d) they will not deliver/make available the personal data, which they have the right and authorization to access, in any other way to third parties (unauthorized persons), and
e) keep confidential all personal data even after the termination of the authorization to access such data.

Other provisions

Article 26

The following shall apply to matters not covered by this Rulebook: the provisions of the Regulation (EU) No. 2016/679 of the European Parliament and the Council dated 27 April 2016 on the protection of natural persons with regard to processing personal data and free movement of such data, the Act on the Implementation of the General Data Protection Regulation (OG 42/2018) dated 9 May 2018 as well as other positive legal regulations of the Republic of Croatia relating to the implementation of the Regulation or relating to personal data.

Article 27

The Rulebook shall enter into force 8 days after being published on the notice board.

Director
Sanja Bežan