Pursuant to the provisions of the Act on the Implementation of the General Data Protection Regulation (OG 42/2018) of 9 May 2018 and the provisions of Regulation (EU) No. 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and the free movement of such data, **BRIJUNI RIVIJERA D.O.O.**, Marulićeva 1, Pula, PERS. ID. NO. (OIB): 39582496872 on 26 January 2021 as the Data Controller adopts the following

RULES

ON THE USE OF VIDEO SURVEILLANCE SYSTEMS (consolidated text)

Article 1

Video surveillance in terms of the provisions of these Rules refers to the collection and further processing of personal data, which includes creating a video footage that forms part or is intended to form part of the storage system based on the provisions of the **Act on the Implementation of the General Data Protection Regulation (OG 42/2018), hereinafter the Act** and the provisions of Regulation (EU) No. 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and the free movement of such data, hereinafter referred to as: the Regulation.

Article 2

These Rules on the use of video surveillance systems regulate and define the following:

a) purpose and scope of the personal data collected,
b) manner and time of storage and
c) use of recorded data for the purpose of reducing risks and increasing protection and security of the persons who are in the premises of the Data Controller and especially the control of entrances and exits to and from the working premises and in order to reduce the exposure of workers to the risk of robbery, burglary, violence, theft.

When collecting, storing, keeping and using the data collected by video surveillance, the Data Controller is obliged to protect the data in accordance with the Regulation and the Personal Data Protection Act, as well as the related by-laws.

Article 3

The video surveillance system is implemented solely for the purpose of protecting:

a) persons who are in official and other premises (control of entrances and exits to and from the working premises),
b) property,

with the aim of reducing the exposure of employees and property to the risk of robbery, burglary, violence, theft, damage, destruction, etc...

The video surveillance system (data processing via video surveillance) must not conflict with or override the interests of the subjects.

The video footage taken by the video surveillance system may only be used for the purposes referred to in paragraph 1 of this Article.

Article 4

The video surveillance system:

a) covers the following areas:
- the main entrance area to the campsite where the video surveillance covers the entrance ramp
- the official entrance to the reception facility where the video surveillance covers a flat area in front of the entrance
- the internal working premises of the reception facility where the video surveillance includes the reception lobby
- the main entrance area to the restaurant terrace
- the main entrance area to the bar area
- the main entrance area to the kitchen area
- the eco island in the campsite area in the immediate vicinity of the sanitary facilities of internal markings 1 and 2

b) must not encroach upon the surrounding public space,
c) must not cover work areas for rest, personal hygiene or changing clothes.

Article 5

Monitoring public areas through video surveillance is allowed only to public authorities, legal entities with public authority and legal entities performing public service, solely:
- if prescribed by law,
- if necessary for the performance of the tasks and duties of a public authority, or
- for the protection of life and health of people and property.

The provisions of this Article do not preclude the application of Article 35 of the General Data Protection Regulation to the systematic monitoring of a publicly accessible area on a large scale.

Article 6

The recorded data shall be recorded and stored for a maximum of seven days from the date of being recorded, and after the specified deadline the video footage shall be permanently deleted, unless a longer storage period is prescribed by law or other legal regulation or if needed as evidence in court, administrative, arbitration or other equivalent proceedings.

In case of justified need, and for evidence purposes, in each individual case it may be decided that the data is kept longer than the time specified in the previous paragraph of this Article.

Video footage proving a violation of the purpose of surveillance shall be stored for one year from the date of storage for as long as it is needed.

Article 7

The Data Controller is obliged to indicate that a facility or an individual room in it or the external area of the facility is under video surveillance.

The marking from the notice must be displayed in a visible place, visible at the latest when entering the perimeter of the recording, or when entering the monitored area.
The notice referred to in the previous paragraph of this Article of these Rules should contain all relevant information in accordance with the provisions of Article 13 of the Regulation, and in particular a simple and understandable picture with the text providing subjects with the following information:

a) that the space is under video surveillance,
b) data on the Data Controller,
c) contact details through which the subjects may exercise their rights.

The data on persons collected by the technical protection system outside their legal purpose may not be used.

Insight into video footage (access to personal data collected through video surveillance) is allowed only to the responsible persons of the Data Controller and persons specially appointed by the Data Controller, who may not use the video footage contrary to the established purpose referred to in Article 2 of these Rules.

Article 8

The Data Controller must establish an automated recording system for recording access to video surveillance footage, which will include:
- time and place of access,
- identification of persons who accessed the data collected through video surveillance.

Article 9

The video surveillance system must be protected from access by unauthorized persons.

Access to the data referred to in paragraph 1 of this Article shall be granted to the competent state authorities within their scope of performing activities determined by law.

Article 10

The processing of personal data of employees through the video surveillance system may be carried out only for the purpose and under the conditions determined by a special decision of the Data Controller, taking into account whether the conditions established by the regulations governing safety at work are met and if the employees have been individually notified in advance on such measure and if the employer informed the employees before making the decision on setting up a video surveillance system.

Article 11

The Data Controller may monitor public areas through video surveillance only if it is necessary for the performance of tasks and duties of public authorities or for the protection of human life and health and property.

The provisions of the previous paragraph of this Article do not preclude the application of Article 35 of the Regulation, which refers to the systematic monitoring of a publicly accessible area on a large scale.

Article 12

This consolidated text of the Rules includes the Rules on the Use of Video Surveillance Systems of 16 July 2018, the Amendments to the Rules on the Use of Video Surveillance Systems of 18 September 2019 and the Amendments to the Rules on the Use of Video Surveillance Systems of 26 January 2021.

Director
Sanja Bežan