|  |  |  |  |
| --- | --- | --- | --- |
| **Title** | **RUEBOOK ON THE VIDEO SURVEILLANCE SYSTEM** | | |
| **Date** | ${vsr\_01\_a} | **Version** | 1.0 |

Data Controller: ${vsr\_01\_b}

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature of the authorized person

**Data Controller and purpose of processing**

Article 1.

The video surveillance system in terms of this Rulebook refers to the collection and further processing of personal data through video surveillance established by the data controller ${vsr\_01\_c}, (hereinafter referred to as the Data Controller), and is used for the purpose of protecting persons and property, i.e.

${vsr\_01\_d}

* ${vsr\_01\_d\_item}

${/vsr\_01\_d}

**Legislative framework**

Article 2.

The use of the video surveillance system is harmonized with the positive legislative framework, which includes the General Data Protection Regulation, the Law on the Implementation of the General Data Protection Regulation and the Law on Occupational Safety.

**Legal basis for processing personal data through video surveillance**

${vsr\_02\_a}

Article 3.

The legal basis for the processing of personal data through the video surveillance system is the legitimate interest of the data controller, which is proven by carrying out a proportionality test of the data controller's interests and the interests, rights and freedoms of the data subject.

${/vsr\_02\_a}

${vsr\_02\_b}

Article 3.

The legal basis for the processing of personal data through the video surveillance system is a legal obligation arising from the provisions of the Law on the Protection of Financial Institutions.

${/vsr\_02\_b}

**Maintenance and protection of the video surveillance system**

Article 4.

Responsible for the correct functioning of the system is the Data Controller (specify) or the data processor ${vsr\_03}.

All components of the video surveillance system must be protected from access by unauthorized persons, in such a way that the storage device is located in a secured room that can only be accessed by authorized persons, and the devices enabling access to the recordings must be additionally protected by a password.

**Authorization to access and manage video surveillance system devices**

Article 5.

The responsible person of the Data Controller is obliged to designate a person authorized to access and manage video surveillance system devices, a person authorized to grant authorization within the video surveillance system through user accounts, as well as a person who will supervise the legality of using video surveillance system recordings.

The person/persons authorized to access and manage the video surveillance system devices at the Data Controller ${vsr\_04\_a\_1} is ${vsr\_04\_a\_2}.

The person/persons authorized to grant authorization within the video surveillance system through user accounts with Data Controller ${vsr\_04\_b\_1} is ${vsr\_04\_b\_3}.

The person who will monitor the legality of the use of video surveillance system recordings by the Data Controller ${vsr\_04\_c\_1} is ${vsr\_04\_c\_2}.

${vsr\_04\_d}

**Authorization for access to real-time video surveillance / access to video surveillance recordings / exclusion and use of video surveillance recordings / remote access to the video surveillance system**

Article 6.

Access to recordings is provided locally (and/or by remote access).

The responsible person of the Data Controller is obliged to designate a person authorized to access the video surveillance system in real time, as well as a person authorized to access and exclude video surveillance recordings.

The responsible person of the Data Controller is obliged to designate a person authorized for remote access to the video surveillance system (if remote access is possible).

The person/persons authorized for remote access to the video surveillance system and the exclusion of video surveillance recordings from the Data Controller ${vsr\_05\_a\_1} is/are ${vsr\_05\_a\_2}.

${vsr\_05\_b}

**User accounts and access passwords**

Article 7.

Persons authorized to take certain actions within the video surveillance system must sign a declaration of confidentiality, be educated on the lawful handling of video surveillance recordings and access the system through their own user account and with their own password, which must contain a combination of upper and lower case letters, numbers and symbols.

Authorized persons must keep the user account access data to the video surveillance system confidential, as well as change the access code at least twice a year.

**Storage period and authorization to access the recordings**

Article 8.

Recordings are kept ${vsr\_06} days after which they are automatically permanently deleted.

Recordings relating to the access requests, setting or defending legal claims in court, administrative, arbitration or other equally valuable proceedings will be excluded and stored on a special medium until the conclusion of the proceedings.

**Access to the video surveillance system records (the retention period of records is at least the same as the retention period of video surveillance recordings)**

Article 9.

Access to the video surveillance system is recorded in such a way that the record includes the time and place of access, the type of activity and the username of the person accessing the video surveillance system.

Access to the video surveillance system records are stored. ${vsr\_07}.

Article 10.

Public authorities have the right to access video surveillance recordings within their official authority and under the conditions prescribed by law.

It is strictly forbidden to make video surveillance recordings available to unauthorized persons.

**Processor – a company that processes personal data through a video surveillance system on behalf of the controller**

Article 11.

If the personal data collected through the video surveillance system is processed by the Processor on behalf of the controller, the Data Controller is obliged to conclude a written Data Processing Agreement and give clear instructions to the Processor in relation to all relevant aspects of the protection of personal data collected by the video surveillance system in question.

**Proceedings in case of personal data breach**

Article 12.

In case of possible personal data breach related to the video surveillance system in question, all employees are obliged to act in accordance with the instructions of the Data Controller, i.e. to inform without delay the responsible person of the Data Controller on possible breach, who shall take adequate further measures and actions ( reporting to the supervisory body, reporting to data subjects, etc.)

After determining the cause of the personal data breach, an assessment of the adequacy of the applied technical, organizational and security measures for the protection of personal data will be carried out.

**Notice on the establishment of video surveillance**

Article 12.

The Data Controller is obliged to inform all its employees about the introduction of the video surveillance system and the provisions of this Rulebook.

Article 13.

Information about the processing of personal data through the video surveillance system is provided to data subjects in two ways.

The first way is to post a notification about video surveillance, in such a way that it is visible before entering the recording perimeter, and it must contain all the information referred to in Article 27 of the Law on the Implementation of the General Regulation on Data Protection.

Another way is to provide information about the processing of personal data and how to exercise the data subject's rights through the website of the controller.

**Addressing data subjects’ requests**

Article 14.

Natural persons whose personal data are being processed (shown in the recording) can submit a Request for exercising their rights under General Data Protection regulation. The request is submitted to the ${vsr\_08\_a} to the e-mail address: ${vsr\_08\_b} and/or to the address: ${vsr\_08\_c}.

The recording subject to the request will be excluded without delay, i.e. immediately upon receipt of a request that enables the identification of the respondent.

Before sharing the video surveillance footage with the data subject/applicant, the footage must be processed in such a way that it is not possible to identify third parties in the footage.

**Supervision of the lawful use of the video surveillance system**

Article 15.

Supervision of the lawful use of the video surveillance system by inspecting the video surveillance access records is carried out when necessary, at least (four) times a year.

Any use of video surveillance contrary to the provisions of this Rulebook is strictly prohibited and will be considered a violation of the work obligation and may result in the termination of the employment contract and the filing of compensation claims.

**Final provisions**

Article 16.

The Data Controller may revoke/change the content of the Rulebook at any time.

Article 17

The Rulebook enters into force on the day of its publication.