MANAGEMENT COLLEGE

MANAGEMENT COLLEGE
"Management College" Ltd., Reg.Nr. 50203022521, educational establishment registration Nr. 3347802535, Lomonosova street 1, k-4, Riga, LV-1019,
phone 28007735, e-mail: info@mCollege.eu, www.mCollege.eu

APPROVED

At 30.10.2018.

At the meeting of the Council,

Protocol No 5

PERSONAL DATA SECURITY REGULATION

1. General Regulations

Regulations for the protection of the processing of personal Data (hereinafter - Regulations) have been established in accordance with the Law on the Processing of Personal Data, the General Data Protection Regulation.

1.1. These Regulations prescribe the general technical and organizational requirements for the processing of personal Data in the Management College Ltd. (hereinafter - the College).

1.2 The following personal Data processing is performed at the College:

1.2.1. The establishment and maintenance of the files of the learners (manual);

1.2.2. Establishment and maintenance of cases of general and academic staff (manual);

1.2.3. Records of students (electronically and manually);

1.2.4. Video surveillance.

1.3. The processing of personal Data (1.2.1, 1.2.2, 1.2.3) shall be carried out by the responsible person of the College.
1.4. The video surveillance referred to in point 1.2.4 shall be carried out by the Baltic International Academy (hereinafter - Operator), registered address Lomonosova Street 4, Riga, LV-1003).
1.5. The processing of personal Data of students, general and academic staff shall take place in accordance with the requirements of the applicable external regulatory enactments and these Regulations.
1.6. The Regulations shall be binding on all users of the College Personal Data Processing. The Regulations shall apply to all personal Data relating to an identified or identifiable natural person.
1.7. The Director of the College (hereinafter - Director) shall be responsible for the security of information at the College.
1.8. These Regulations are intended for use only within the framework of the College and their disclosure to other third parties should only be permitted with the permission of the Director of the College.

2. Technical resources provided to persons Data processing and its security

2.1. Personal Data are collected through:
2.1.1. Data provided by the person;
2.1.2. video surveillance cameras (hereinafter - video surveillance system).
2.2. The VSS (hereinafter - video surveillance system) operates continuously.

3. Classification of the processing Data

3.1. By value, the information is considered to be medium-high-value information.
3.2. After confidentiality, the information shall be treated as confidential and restricted access information.

4. Access security measures personal Data processing systems

4.1. In order to ensure the security of existing Data on the video surveillance system is installed at the College and to record all Data views and copies, the following requirements must be met:

4.1.1. records performed by the video surveillance system shall be made electronically and shall be stored not longer than 10 days from the time of the recording.

The entries are deleted automatically in chronological order from the time of the entry.

4.1.2. access rights to video surveillance systems and personal Data (records) contained therein shall be the person and director authorised by the Operator. The user's rights in relation to access to and operation of records are assigned to the responsible person;

4.1.3. manual deletion, copying or transfer to law enforcement authorities of personal Data (records) contained in the installation of any kind of video surveillance system installed at the College shall take place only upon written, substantiated request by the competent State authority.

4.2. The following cases shall be entered on the relevant registration sheets:

4.2.1. inspection of Data (records) in the video recording Data installation (including third-party inspection);

4.2.2. copying of Data (records) in the video recording equipment to other Data carriers or transmitting electronically by electronic mail;

4.2.3. Transfer of Data (records) in the video recording equipment to third parties and law enforcement authorities or transmission by electronic mail.

4.3. Access to personal Data is provided by identifying a user-specific access user name and a unique password that is known only to the responsible person and is responsible for not disclosing it.

5. Rights, Duties and Responsibilities of Users

5.1. It is the responsibility of users to familiarise themselves with the Regulations and to comply with them in their daily work.

5.2. The user shall not disclose information about the video surveillance system, computer network design and configuration installed at the College, or reveal classified information to unauthorised persons.

5.3. The user may not allow access to personal Data by other persons if he or she is not required to perform his or her direct duties and has been authorised by the Director of the College. The user may not copy files containing personal Data to external media (USB cards and/or CDs, etc.) if this is not necessary for the fulfilment of direct duties and/or has not been authorised by the College Director.

5.4. When finished, the user is required to completely turn off the computer.

5.5. The user shall be responsible for the computer equipment placed at his or her disposal, as well as the user shall be responsible for the activities performed on the computer equipment transferred to him.
5.6. The user undertakes to preserve the confidentiality of the information even after termination of the legal relationship.

6. Responsible persons

6.1.The persons responsible for technical and information resources shall have the following general obligations:
6.1.1. monitor the technical and information resources of the staff involved in the processing of personal Data;
6.1.2. ensure that employees are briefed and made aware of these Terms and are committed to maintaining and not disclosing personal Data unlawfully;
6.1.3. to ensure the compliance of the operation of the systems with the Law on Processing of Personal Data and the requirements of regulatory enactments issued on the basis thereof;
6.1.4. deny a particular user the right to access the systems if the user endangers the operation of the system or violates these Terms;
6.1.5. change user passwords;
6.1.6. record the copying, viewing and / or transfer of personal Data records to third parties;
6.1.7. Ensure that only authorized persons and users have access to the installed video camera, its computer, hard disk and other related devices.
6.1.8. to regularly inspect the condition and operation of the equipment, as well as to remedy any problems in the operation of the equipment;
6.1.9. ensure registration of necessary changes with the Data State Inspectorate;
6.1.10. inform the Operator of the System Security Incident System.

7. Procedures for investigating security incidents

7.1. Any case in which the equipment has been damaged or an unauthorized attempt to access the information has occurred, or the information or part of the equipment has been lost, shall be regarded as a safety incident.
7.2. When determining a security incident, the responsible person shall take the following actions:
7.2.1. check records regarding access to systems and stop the operation of systems until the risks and causes of the incident have been ascertained;

7.2.2. request written explanations to the persons involved and other employees;
7.2.3. clarify the causes of the incident and, if necessary, develop amendments to these Regulations by introducing additional protection requirements;
7.2.4. if necessary, disciplinary liability shall be applied to the guilty employees;
7.2.5. if a criminal offence is suspected, the responsible person shall take a decision regarding reporting to the State Police.

8. Extraordinal situations

8.1. In the event of exceptional circumstances, the protection of video surveillance systems shall take place in accordance with the Regulations on fire protection of the premises. Where possible, the technical resources to which personal Data are stored shall be supplied in a safe place.

8.2. In the event of exceptional circumstances, similar technical resources shall be used for the recovery of the video surveillance system and, if necessary, spare copies shall also be used.

9. Means by which technical resources are provided against intentional damage and unauthorized acquisition

9.1. The Security of the premises shall be provided by the Operator.
9.2. The technical resources of the systems are preserved by ensuring that the premises are locked after working hours.
9.3. In systems where personal Data is processed (server or computer storing the record), the systems may not be accessed by unauthorized persons.
9.4. The password for access to personal Data shall be known to the responsible person and to other users to whom the College has granted access.Actions in case of problems

9.5. All emergency situations (including fire, floods, accidents, etc.) must be notified immediately to the Director of the College or to a person authorised by it.

Director **L.Sprūde**