Rules for implementing video monitoring and audio monitoring

List of contents

1. FOREWORD ..... ERROR! BOOKMARK NOT DEFINED.

2. PROCEDURE FOR IMPLEMENTING VIDEO MONITORING ERROR! BOOKMARK NOT DEFINED.

2.1. PURPOSE, BASIS AND SCOPE OF VIDEO MONITORING . ERROR! BOOKMARK NOT DEFINED.
2.2. DURATION OF VIDEO MONITORING AND STORAGE PERIOD OF VIDEO RECORDINGS ERROR! BOOKMARK NOT DEFINED.
2.3. RULES FOR STORING AND ACCESSING VIDEO RECORDINGS 4
2.4. PROCEDURE FOR DESTRUCTION OF VIDEO RECORDINGS ..... ERROR! BOOKMARK NOT DEFINED.

3. MECHANISMS FOR PROTECTING THE RIGHTS OF THE DATA SUBJECT ERROR! BOOKMARK NOT DEFINED.

3.1. WARNING ABOUT VIDEO MONITORING 5
3.2. DATA SUBJECT RIGHTS 5

4. DISCLOSURE OF VIDEO RECORDINGS TO THIRD PARTIES ..... ERROR! BOOKMARK NOT DEFINED.

5. PROCEDURE FOR IMPLEMENTING AUDIOMOTORING.... ERROR! BOOKMARK NOT DEFINED.

5.1. PURPOSE AND BASIS OF AUDIO MONITORING ..... ERROR! BOOKMARK NOT DEFINED.
5.2. RULES FOR STORING AND ACCESSING AUDIO RECORDINGS 6
5.3. PROCEDURE FOR DESTRUCTION OF AUDIO RECORDINGS 7

6. PROCEDURE FOR RESPONDING TO AN INCIDENT ..... ERROR! BOOKMARK NOT DEFINED.

1. FOREWORD

The present Video Monitoring and Audio Monitoring Procedure (hereinafter referred to as the "Procedure") defines the procedure for implementing video monitoring in internal and external spaces of the University of Georgia LLC (Registration No. 205037137; Address: Tbilisi, Merab Kostava St. No. 77a), hereinafter referred to as the "University", the period and procedure for storing video recordings, the procedure for accessing and destroying video recordings, and information on mechanisms for protecting the rights of the data subject. In addition, this procedure regulates the procedure for implementing audio monitoring, the period and procedure for storing audio recordings, and the procedure for accessing and destroying audio recordings.

University:

- Respects and recognizes the fundamental rights and freedoms of individuals when processing personal data, including the rights to privacy and communication;
- Undertakes the responsibility to strictly comply with applicable legislation when processing personal data;
- Recognizing the value and importance of personal data, undertakes the obligation to strictly protect their confidentiality.

Definition of terms:

The terms used have the meanings defined by the Law of Georgia on Personal Data Protection and other legislative acts:

University of Georgia LLC - the person responsible for data processing, the company that individually determines the purposes and means of personal data processing and directly carries out data processing.

Data subject - any natural person about whom data is processed.

Personal data or data - any information that relates to an identified or identifiable employee (natural person). An employee is identifiable when the employee can be identified

directly or indirectly, including by name, surname, identification number, geolocation data, electronic communication identification data, physical, physiological, mental, psychological, genetic, economic, cultural or social characteristic.

Data processing - any operation performed on personal data, including their collection, getting, access, organization, grouping, interconnection, storage, alteration, restoration, retrieval, use, blocking, erasure or destruction, as well as disclosure of personal data by transmission, publication, dissemination or otherwise making available;

Video monitoring - processing of visual image data using technical means placed/installed by the University in the internal space or on the external perimeter, in particular, video surveillance and/or video recording.

Audio monitoring - processing of sound signal data using technical means placed/installed by the University, in particular, audio surveillance and/or audio recording.

2. Procedure for implementing video monitoring

2.1. Purpose, basis and scope of video monitoring

The external perimeter and internal perimeter of the building are subject to video monitoring. The purpose of video monitoring is to fulfill obligations imposed by law, the need to protect the safety of employees, the property of the university, as well as for the purposes of protecting minors from harmful influences; in certain cases, **video monitoring is carried out during exams in accordance with the established procedure**.

Video monitoring also serves the purpose of efficient logistics or technical operations of the internal workspace, providing the university management with the type of data needed to optimize daily operations. According to the University's assessment, the above-mentioned goal cannot be achieved by any means other than video monitoring, and video monitoring is an effective and proportionate means to achieve the goal.

The University conducts video monitoring only to the extent necessary in accordance with the Law of Georgia on Personal Data Protection and this Procedure.

2.2. Duration of video monitoring and storage period of video recordings

Video monitoring is carried out 24 hours a day, 7 days a week.

The University stores video recordings for a period of 2 (two) weeks, after which the video recordings are destroyed.

2.3. Rules for storing and accessing video recordings

The persons/authorized persons authorized to access the video monitoring system (NVR device, monitors, etc.) and video recordings and to take appropriate actions are

determined by the order of the rector. It is not allowed to grant access to the system to a person who is not specified in the said act.

Video recordings are stored by the university on a secure server, where access is only possible by an authorized person by entering the user name and password into the account. The university ensures that video monitoring in real mode and the video image on the monitor are accessible only to authorized persons. Access to the video recording cannot be carried out from external devices and the subject with access is obliged to log in only from the university's internal system to gain access.

In order to protect against viruses, the university uses an antivirus system and other technological means of protection to prevent illegal penetration from the Internet and computer networks.

In the event of a technical fault in the recording system being detected, the authorized person is obliged to immediately notify the IT department so that a timely response can be made to the fault.

2.4. Procedure for destruction of video recordings

Once the video recording storage period expires, the video recording is automatically deleted. It is technically impossible to restore or otherwise access the recording after it has been deleted.

3. Mechanisms for protecting the rights of the data subject

3.1. Warning about video monitoring

The University has posted a warning sign about the ongoing video monitoring in the area where video monitoring is taking place. It is necessary to post a warning sign about the ongoing video monitoring in all areas where video monitoring is being conducted and where a corresponding video camera is installed.

3.2. Data subject rights

The data subject is entitled to take the following actions in relation to his/her personal data:

- Request a copy of the video recording;
- Request information about the period (time) of data storage, and if it is impossible to determine a specific period, about the criteria for determining the period;
- Request information about whether his/her data has been transferred, the legal basis and purposes of the data transfer, as well as appropriate data protection guarantees if the data is transferred to another state or international organization;

• Request information about the identity of the data recipient or the categories of data recipients, including information about the basis and purpose of the data transfer if the data is transferred to a third party;

• Request the correction, updating and/or completion of erroneous, inaccurate and/or incomplete data.

• Request the cessation, deletion or destruction of data processing, if there are appropriate grounds.

• Request the blocking of data, if there are appropriate grounds.

• In case of violation of rights, apply to the Personal Data Protection Office or the court.

4. Disclosure of video recordings to third parties

Access to video recordings stored by the University, their viewing and, in some cases, their transfer to third parties may become necessary if there is a suspicion that the video recording reflects the fact of a crime or other violation of the law and/or is necessary within the framework of disciplinary proceedings initiated at the University/court proceedings, the body conducting the case has an interest in viewing it for the purposes of investigating a criminal case and conducting administrative offense proceedings only on the basis of a ruling of the relevant court and/or a prosecutor's decision from a representative of a law enforcement agency.

5. Procedure for implementing audiomotoring

5.1. Purpose and basis of audio monitoring

Audio monitoring is subject to incoming and outgoing telephone calls to the University hotline.

Audio monitoring is carried out on the following grounds:

• With the consent of the data subject.

Before making an audio recording, the University shall inform the data subject in an appropriate manner that his or her conversation is being recorded, and accordingly, he or she is entitled to consent to audio monitoring.

5.2. Rules for storing and accessing audio recordings

The persons/authorized persons with access to the audio monitoring system and audio recordings and performing appropriate actions are determined by the order of the rector. It is not allowed to grant access to the system to a person who is not specified in the said act.

The university ensures the protection of the audio monitoring system, in such a way that the audio recordings are stored on the server. Access to it is carried out only by an authorized person by entering the username and password into the account. Access to the audio recording cannot be carried out from external devices and the subject with access is obliged to log in only from the university's internal system to gain access.

In order to protect against viruses, the University uses an antivirus system and other technological means of protection to prevent illegal penetration from the Internet and computer networks.

In the event of a technical fault in the recording system, the authorized person is obliged to immediately notify the IT service so that a timely response can be made to the fault.

5.3. Procedure for destruction of audio recordings

The University stores the audio recording for a period of 2 (two) weeks. Upon the expiration of the storage period, the audio recording is automatically deleted. It is technically impossible to restore the said recording or otherwise gain access to it after its deletion.

6. Procedure for responding to an incident

The authorized person of the University is obliged to immediately - upon discovery of the incident - record the incident, the resulting outcome, the measures taken and, no later than 72 hours after discovery of the incident, notify the Personal Data Protection Service in writing or electronically, except in cases where it is unlikely that the incident will cause significant damage and/or pose a significant threat to the fundamental rights and freedoms of a person.