Georgian American University, LLC

Regulation on the Implementation of Video Monitoring

Contents

Purpose and Scope of Video Monitoring 3

Definitions of Terms 3

Purpose of Video Monitoring 4

Scope and Duration of Video Monitoring 4

Authorized Persons for Access and Processing of Video Recordings 5

Personal Data Security 5

Purpose and Scope of Video Monitoring

Georgian-American University LLC (Identification Code: 206169304, Legal/Physical Address: Tbilisi, M. Aleksidze St. No. 10) — hereinafter referred to as the "University" or the "Data Controller" —

- **Respects and acknowledges** the fundamental rights and freedoms of individuals during the processing of personal data, including the right to privacy and the inviolability of communication.
- **Assumes responsibility** to strictly comply with applicable legislation in the processing of personal data.
- **Recognizes the value and importance** of personal data and commits to rigorously maintaining its confidentiality.

Definitions of Terms

The terms used in this document carry the meanings defined by the **Law of Georgia on Personal Data Protection** and other applicable legislative acts.

1. **Georgian-American University LLC (ID: 206169304):**
   The University individually determines the purposes and means of personal data processing and performs the processing either directly or through an authorized processor.
2. **Employee or Data Subject:**
   A natural person employed by the company whose personal data is processed by the company.
3. **Personal Data or Data:**
   Any information related to an identified or identifiable employee (natural person). An employee is identifiable if their identity can be determined directly or indirectly, including through their name, surname, identification number, geolocation data, electronic communication identifiers, or physical, physiological, psychological, genetic, economic, cultural, or social characteristics.
4. **Data Processing:**
   Any operation performed on personal data, including collection, acquisition, access, organization, structuring, interconnection, storage, alteration, retrieval, use, blocking, deletion, or destruction. It also includes the disclosure of personal data through transmission, publication, dissemination, or making it otherwise accessible.

5. **Authorized Processor:**
   A natural person (excluding Georgian-American University LLC, ID: 206169304), legal entity, or public institution that processes personal data for or on behalf of the company.

6. **Video Monitoring:**
   The processing of visual data captured using technical equipment installed in public or private spaces, specifically for video surveillance and/or recording (excluding covert investigative actions).

7. **Data Processing (Video Monitoring):**
   Any operation performed on data, including collection, acquisition, access, photographing, video monitoring and/or audio monitoring, organization, structuring, interconnection, storage, alteration, retrieval, use, blocking, deletion, or destruction. It also includes the disclosure of data through transmission, publication, dissemination, or making it otherwise accessible.

Purpose of Video Monitoring

- The implementation of video monitoring at the University is conducted to fulfill legal obligations, ensure security and property protection, and safeguard minors from harmful influences. These objectives cannot be effectively achieved without video monitoring, making it the only adequate and proportionate means to achieve these goals and protect the associated benefits.

- Additionally, video monitoring serves to optimize internal logistical and technical operations within the workspace. It provides University management with the type of data necessary for the optimization of daily operations and workflow efficiency.

Scope and Duration of Video Monitoring

- The University conducts video monitoring, with some cameras operating 24 hours a day and others functioning in motion detection mode.

- Retention Period:
  Data obtained through video monitoring is stored for a period of 30 calendar days within the video monitoring system. After this period, the data is automatically deleted by the system. However, video recordings associated with disciplinary proceedings are exempt from deletion and are retained as part of the relevant documentation.

- Monitoring Areas:
  Video monitoring covers the common areas of the institution, including corridors, building entrances, several classrooms equipped with expensive equipment, examination rooms, stairwells, the cafeteria, and the University's external perimeter. The external perimeter includes outdoor spaces, gates, fences, entryways, parking lots, pathways between buildings, and the library.
- Exclusion Zones:
  Video monitoring is not conducted in changing rooms, hygiene facilities, or any other spaces where individuals have a reasonable expectation of privacy or where video monitoring would conflict with universally recognized ethical norms.

Authorized Persons for Access and Processing of Video Recordings

- System Security:
  The video monitoring system is secured with encryption functionality and equipped with an appropriate self-destruction mechanism. Camera monitors are located in a locked security room, accessible only with a key. Access to the key and the video data is restricted to authorized personnel, specifically security staff. During examination periods, the video monitoring of examination rooms is overseen by a representative of the Examination Office.
- Access Control:
  Access to the video monitoring system is protected by usernames and passwords. The University maintains a log of every instance of access to video recordings, including the time of access and the username, enabling identification of the accessing individual.
- Authorized Personnel:
  The University has designated security staff as responsible for the video monitoring system through an official order. The Head of Security has full access to the system, including administrative functions. Other personnel, such as the representative of the Examination Office, are limited to real-time monitoring capabilities during active operations.

Personal Data Security

- The University takes personal data security with the utmost responsibility and periodically implements organizational and technical measures to address potential and

associated risks in data processing (examples of such measures include: secure electronic systems: Data processing is conducted using secure and reliable electronic programs/systems.Proper server protection: Data is stored on appropriately secured servers.Physical data protection: Non-electronic data is stored using appropriate security measures.) These measures ensure the protection of personal data from incidents such as: Unauthorized or accidental damage. Loss or illegal processing, including destruction, deletion, alteration, or disclosure. Unauthorized access, retrieval, collection, or any other form of unlawful use. These efforts aim to safeguard personal data integrity and confidentiality while ensuring compliance with applicable data protection laws.

- To inform data subjects about data processing, the University has placed appropriate warning signs in visible areas within the premises. These signs include contact information for the person responsible for video monitoring.
- The University ensures that employees whose workspaces fall within the view of the video monitoring system are properly informed in accordance with established procedures.

- The University's video monitoring system includes the following access levels:

a) Real-Time (Online) Monitoring: Users with this access can only view live video footage. They are restricted from rewinding or downloading recordings to a computer or other media devices.
b) Playback and Monitoring of Recordings: Users with this access can monitor cameras in real-time and rewind or review recorded footage. However, they are restricted from downloading recordings to a computer or other media devices.
c) Downloading Recordings: Users with this access can monitor cameras in real-time, rewind and review recorded footage, and download recordings to a local network. Downloaded recordings can be provided to authorized personnel upon appropriate confirmation.
d) Technical Support Access: Users with this access can: Create new user accounts within the video monitoring system. Delete existing user accounts. Monitor electronic logs of actions performed in the system. Take actions to resolve technical issues and correct errors. Make configuration changes to the video monitoring system.

Note: A user is any individual with access to the video monitoring system. Access to the video monitoring system is granted exclusively through individual usernames and passwords to ensure accountability and security.