



OFFICE OF THE PERSONAL DATA
PROTECTION INSPECTOR

Recommendations for Conducting Video Surveillance

These recommendations are designated for all data controllers¹ carrying out video surveillance and are aimed at fulfilment of the requirements under the Law of Georgia on Personal Data Protection and implementation of European standards.

Video Surveillance System

Video surveillance system is defined as visual/audio monitoring of a space, event, activity or a person by means of electric device.

Video surveillance system may operate in recording (making records) and real-time data transfer (streaming) modes. Video surveillance may be carried out not only for video-streaming, but also for recording and transfer of photo records and thermal images.

Recommendations do not refer to cases of use of analog systems such as audio/video conferencing and recording/broadcasting of public events.

Video Records Containing Personal Data

A record made by means of video surveillance system is considered to be personal data when:

- It is possible to identify face of a person depicted in it (direct identification)

Or,

- It is impossible to identify facial features of a person, but items and/or human behavior patterns recorded by the system, if compared with other data, may allow identifying a person (indirect identification). For instance, in case of a vehicle driver damaging other vehicle, recorded plate number will be used to establish identity of

¹ Public institution, individual or legal entity, which determines purpose and means of data processing (collection, storage, transfer, etc.);

the owner of the vehicle (requesting information about the owner of a vehicle), by whose fault the damage occurred.

Purpose of Video Surveillance

With regards to video surveillance, critical importance is given to the purpose of video monitoring, and not to technical specifications of the system. The Law of Georgia on Personal Data Protection clearly defines the purposes that may be achieved by means of video surveillance, though the regulation is different in consideration of the specifications of a building and space.

Video surveillance is allowed in streets and public transport, for achievement of the following goals:

- Crime prevention;
- Protection of person's safety and property;
- Protection of public order;
- Protection of juveniles from detrimental influence.

Term "street" includes parks, squares, playgrounds, public transport stations/stops, and other public gathering areas.

Video surveillance of buildings of public and private institutions is allowed for the following purpose:

- Protection of person's safety and property;
- Protection of juveniles from detrimental influence;
- Protection of secret information.

Video surveillance system may be used to monitor the outside perimeter and entrance of the building.

At workplace, video surveillance system can be installed only in exceptional cases, if it is necessary for the purpose of protection of person's safety and property, for protection of secret information, if such purposes could not be fulfilled otherwise. In such case, legal requirement towards the principle of proportionality is imperative and requires the data controller to justify the use of video surveillance system.

Video surveillance of fitting rooms / locker rooms and restrooms is prohibited!

When using video surveillance system at workplace, all employees of the institution must be informed in writing about the video surveillance and his/her rights. It is desirable to arrange an informative meeting with the employees before installation of video surveillance system and to explain the necessity for control, the goal, the scope and rights of the employees.

At residential building, video surveillance system can be used only for the purpose of protection of safety of persons and property. In order to install video surveillance system, written consent of more than half of the owners of the building must be obtained. All residents of the building must be informed about presence of video control.

At residential building, video surveillance system can only be used to monitor the entrance and common space (hall, staircase cell, area adjacent to elevator). Entrance to individual apartment can be monitored only if so decided by the owner of such apartment or on the basis of his/her written consent; monitoring of apartments is prohibited.²

Principles of Carrying out Video Monitoring

For the purpose of the law, video surveillance is considered as one of the means of monitoring of space and behavior, and not as the only mean. As video surveillance is considered to be a radical form of intrusion into privacy, data processor needs to realize the threat and justify the necessity for use of the system. In particular, the following must be assessed:

- Real need and purpose of data processor;
- System's impact on the person's right to privacy;
- Possibility to achieve the purpose via other means.

Video surveillance must be used only for the purposes prescribed by the law and it is prohibited to use it for other purposes. For instance, use of video surveillance system, installed at educational institution for protection of property, is prohibited for controlling the educational process by academic personnel.

In any space, video surveillance must be carried out in compliance with the principle of proportionality. Data controllers should use video surveillance system only in cases when it is otherwise impossible to reach the goal or if it takes disproportionate amount of effort.

In case of use of video surveillance that allows video as well as audio monitoring, compliance with the principle of proportionality is of particular importance, and data controller is obliged to justify the need for audio monitoring.

Data collected as a result of video surveillance (including records and photos) must be stored for the term that serves specific purpose.

² This rule does not apply to data processing for personal purposes and cases when owner/proprietor of the apartment carries out video surveillance of his/her own apartment.

Parameters of Video Surveillance

Parameters of video surveillance system must correspond to the purpose of its application, must be adequate to the purpose and proportionate. In order to implement the principle in practice, data processor must pay attention to the following circumstances:

Number of video cameras, their location and resolution must correspond to the purpose of video recording, specifics of the organization's operation, total area of the building, room structure, etc. The system must be located in a way to achieve the purpose by means of controlling the minimum space. If the purpose can be served by low resolution video cameras and there is threat of collecting excessive amount of data (including special category data) beyond the scope of the purpose, preference must be given to such equipment.

Real time monitoring must be carried out only by persons with special authorization (e.g. security personnel) and the images on the monitors/displays must not be available to others.

If video surveillance image of a specific area is broadcasted on the monitors, in real time and in the same area (e.g. waiting rooms, shops, chemist's), then only the people present in the area must be able to see the images on the monitors, as they are able to observe the process without such monitors. For instance, a person in one section of the shop must be able to see the image of video surveillance of the same section.

Data Security

Any data controller is obliged to take organizational and technical measures for data security.

Data security includes combination of technological, organizational and procedural measures for recording, real time data transfer, archiving, creating backup copies, storage and access to data. It is desirable for the organization's internal regulations to correspond to the standards established by the law of Georgia on Informational Security.

Data controller must establish the rule of storage of video records, according to data categories, with indication of specific time period.

When applying security measures, it is important, that:

Used technical means allow for protection of personal data. Preference must be given to the system, which reduces the risk of unauthorized access to records (for instance, by means of encryption).

Transfer of the record or real time image from the device to the server must be done by observing the requirement of completeness and continuity of the information.

Access to video records (including access to the video surveillance control room) must be given to limited number of persons, based on their official duties.

During video surveillance, data processor is fully responsible for data processing and security, including the cases when video surveillance, record storage, security management is assumed by contractor organization; therefore, it is important to precisely describe parties' rights and obligations and scope of responsibility in the contract.

In case if video surveillance is conducted in the building, private and public organizations are obliged to create a file system for video record storage. Besides records (images/voice), the system should include the information about the date, place and time of data processing.

Warning Signs

While conducting video surveillance, data processor is obliged to place a warning sign in a visible area (see appendix), with the location, inscription and image visible for every person in the controlled area.

If the area of video control is large, it is possible to locate several warning signs in the area or one sign –at the entrance.

Appendix:

Sample warning signs:

