



R E P U B L I C OF ALBANIA
RIGHT TO INFORMATION AND PERSONAL DATA PROTECTION
COMMISSIONER

GUIDELINE

No.03, dated 30.04.2025

ON

PROCESSING PERSONAL DATA FROM VIDEO SURVEILLANCE SYSTEMS

Pursuant to article 82, paragraph 1, letter “d”, article 85, paragraph 1, and article 97, paragraph 2, of Law no. 124/2024 “On Protection of Personal Data” (hereinafter referred to as “the Law”), the Information and Data Protection Commissioner, hereby issues the following

GUIDELINE

Article 1

Personal data processing

1. Data stored in a video surveillance system such as images or sounds¹ (hereinafter referred to as “CCTV system”) are personal data, provided that an individual can be directly or indirectly identified based on these recordings. An individual is identifiable if the image or sound recorded in these systems reveals distinguishing characteristics of that individual such as face, physical features, voice data, etc., enabling full identification when compared with other available data.
2. The installation and use of CCTV systems that process personal data must comply with fundamental human rights, such as the right to private and family life and the right to personal data protection².
3. Recordings stored in a CCTV system that contain personal data may not be disseminated, except in cases provided for by law.

¹ When the CCTV system includes this element too.

² These rights are foreseen in article 8, of the European Convention of Human Rights and in the Law.

Article 2

Preliminary conditions for the lawful camera supervision

1. The processing of personal data through CCTV systems constitutes a serious interference with the private life of an individual. The controller may process such data only when legitimized under article 7 of the Law.
2. The data controller must ensure that the consent of the data subject is obtained, but in practice this is only possible in very limited cases, when the identification of a group of persons within the camera area is clearly made. In most cases, the controller finds it impossible to identify in advance the individuals who will pass through the monitored area, in order to first ensure their "consent". In this case, the controller is legitimized to install CCTV systems, if this processing is necessary for the fulfilment of a legal obligation³ or its legitimate interests⁴. In any case, it must guarantee that there is no other less intrusive way in the lives of the data subjects to fulfil the purpose.
3. The lawful interest in the operation of a CCTV system means that:
 - a) the controller has the right to decide who is allowed to enter and remain within the area under surveillance (right to the environment);
 - b) the use of a CCTV system must be justified by a specific need to protect the rights of the controller or third parties, such as the risk of theft or a threat to the physical or mental safety of persons staying within the supervised area;
 - c) the purpose of the recording must be clearly specified and in accordance with the lawful interests of the controller (e.g. protection of property against theft);
 - ç) data processing by means of a CCTV system may only be permitted if the purpose for which the system was installed cannot be achieved in any other way;
 - d) the installation of a CCTV system is prohibited in premises used exclusively for private purposes such as toilets, showers, changing rooms, etc.
4. Since the data processing is carried out for the purposes of the legitimate interests of the controller, it is essential to take into account the interests of the data subjects, so that CCTV system data are not accessible to unauthorized persons. Under these conditions:
 - a) the data must be stored for the shortest possible period;
 - b) the circle of persons having access to the recorded data must be limited and kept as narrow as possible;
 - c) any access obtained to the recorded data must be documented, for the purposes of a possible subsequent control. The data recorded for risk prevention, such as the reason for installing the CCTV system, shall not be used for other purposes, except in cases provided for by law, e.g. for important public interests such as the fight against crime.

³ Article 17, paragraph 1, letter "c", of Law no. 124/2024 "On Personal Data Protection".

⁴ Article 7, paragraph 1, letter "dh", of Law no.124/2024 "On Personal Data Protection".

5. Before the start of the processing of personal data by means of the CCTV system, it must be taken and documented by an internal act by the decision-making body of the controller, determining the following points:

- a) the type, specifications of the cameras and their placement in accordance with the purpose for which they will be used. The position of the cameras must not be in a way that images are obtained from environments that are not compatible with the purpose of the surveillance;
- b) the exact areas that will be under surveillance; e.g. monitoring and recording of images in private environments is prohibited;
- c) real-time surveillance and transmission of images recorded by the CCTV system, via the internet or electronic communication services, where persons can be easily identified, is prohibited.

Article 3

Storage time period

1. The storage time period of recorded data shall not exceed the period necessary to fulfil the purpose for which the data were recorded.
2. In general, data may be kept:
 - a) for a period of 72 hours⁵;
 - b) for a longer period, if the controlled premises are not under continuous surveillance, however, not more than 30 days⁶;
 - c) for longer periods when provided for by a special normative/regulatory act.
3. After the end of the legal time period of storage of the records, the controller shall take measures to erase these data. If, in the event of a security incident, the CCTV system data must be made available to the competent authorities within the meaning of the Law.

Article 4

Camera surveillance in residential buildings

1. CCTV systems may be installed in residential buildings only with the approval of at least 75% of the residents, in accordance with the legislation in force on the administration of condominiums in residential buildings.
2. Surveillance and recording of images or sounds from CCTV systems in common areas of residential apartment buildings is permitted only for the purposes of protecting the safety of people and property.
3. It is prohibited to make images of residents and their activities, recorded in common areas of residential buildings by means of the CCTV system, available to third parties, except in cases where this is required by the competent authorities.

⁵ Cases where this time period applies relate to the systems which are continuously supervised by one person, such as in the penitentiary institutions or when a security guard contracted for this purpose supervises the respective screen.

⁶ These time periods may extend for public holidays.

4. The controller is obliged to place in the premises monitored by cameras, the standard model of the information board for surveillance with the CCTV system, approved by the Commissioner, which is attached to this Guideline.

Article 5

Security measures

1. Security measures should protect recording systems and transmission equipment that store recorded data, protecting them from unauthorized or accidental access, alteration, destruction, loss or processing⁷.
2. Personal data should be kept secure and not misused or compromised by unauthorized persons. Security is not only related to physical security measures, but also to organizing work in such a way as to minimize risk, for example, by ensuring that personnel have access to personal data only to the extent necessary to perform their job. Each employee should be regularly trained on the secure use of personal data and clearly understand the responsibilities and limitations that they have, in accordance with the requirements of the Law.
3. Controllers, processors and authorized persons who, during the performance of their duties, become aware of the content of data recorded by the CCTV system are obliged to maintain confidentiality even after the completion of their work, for the controller or processor.

Article 6

Rights of the data subjects

1. The rights of data subjects are provided for in Part II, Chapter II, of the Law.
2. Data subjects must be clearly informed of the existence and purpose of a CCTV system, by placing a notice in the monitored area⁸. Exceptions are only admissible when provided for by specific legislation.
3. All other rights of the data subject must be guaranteed, in accordance with the provisions of articles 13 to 20 of the Law, in particular the right of access, the right to object and the right to erasure.
4. If a data subject requests access to his or her video surveillance data, these data may not be erased by the controller after receipt of such a request. In case the granting of access is to be fulfilled by showing the recorded material to the data subject, the data protection interests of third parties must be taken into account, by making it possible to anonymize the video by obscuring their image.

⁷ As per articles 22, 28 and 29 of the Law, no.124/2024 “*On Personal Data Protection*”.

⁸ Article 13, of the Law no. 124/2024 “*On Personal Data Protection*”.

Article 7

Final provisions

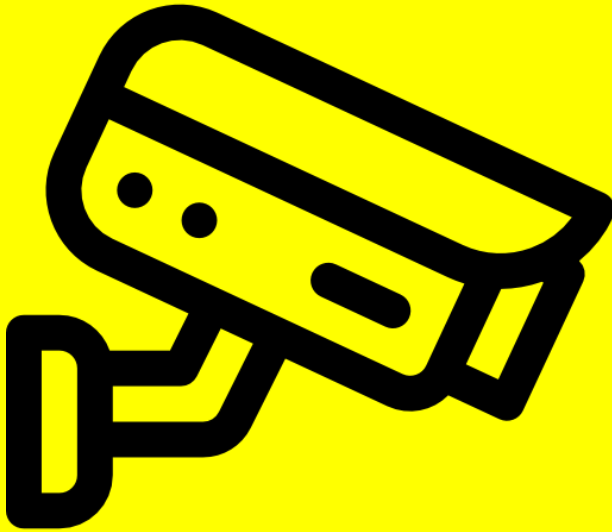
1. All public and private controllers/processors in the territory of the Republic of Albania are responsible for implementing this Guideline.
2. Failure to implement the requirements of this guideline constitutes a violation of the Law and is sanctioned in accordance with the provisions of article 94 of this Law.
3. Guideline no. 3, dated 05.03.2010 “On the Processing of Personal Data with Video Surveillance System in Buildings and other Environments”, shall be repealed.

This Guideline shall enter into force upon publication in the Official Gazette.

COMMISSIONER

Besnik Dervishi

CAMERA SURVEYED AREA



The purpose of processing your images is to ensure the safety of the individual, property, and public safety.

*Personal data subject, may exercise their rights according to the Law no. 124/2024
"On Protection of Personal Data" at:*

(Name of controller)

(Controller contacts)

In case of misuse of personal data through the video-surveillance system, the subjects are entitled to complain to:

Information and Data Protection Commissioner.

Your data will not be processed for a longer time period then necessary for processing and shall be kept under security measures with access limited to authorized personnel

Green line.: 0800 20 50

www.idp.al

info@idp.al

