REPUBLIC OF ALBANIA
PERSONAL DATA PROTECTION COMMISSIONER
OFFICE OF THE COMMISSIONER

INSTRUCTION

No. 3 of 05 March 2010

ON

CCTV SURVEILLANCE SYSTEM IN BUILDINGS AND OTHER PREMISES

Pursuant to Law No 9887, dated 10 March 2008 *"on the protection of personal data"*, Decisions of the Assembly of the Republic of Albania No 211, of 11 September 2008 "On the appointment of the data protection Commissioner", No 225, of 13 November 2008 "on the approval of the organizational structure and salary scales of the employees of the office of the commissioner for the protection of personal data" an in implementation of obligations arising from paragraph *"c"* of point 1 of Article 30 and letter *"ç"* and *"f"* of point 1 of Article 31 of the abovementioned law;

I HEREBY INSTRUCT

One of the most important tools of processing personal data is CCTV surveillance. Data are considered to be processed through this means if besides the images which were captured by the video cameras; users of such equipment have also recorded information or have collected information which serves for the identification of individuals.

The data stored in recording devices, sounds of images are personal data, provided that one individual can be directly or indirectly identified based on such recordings (for example when it is possible to indirectly identify one person from the sound recordings). An individual is identifiable, if the image in which he is registered reveals his distinctive traits (especially his face) and enables full identification when such features are compared with other available data. Personal data in their entirety consist of identification of those factors that make it possible to connect a particular person with a behaviour captured by a video surveillance system.

The processing of personal data through CCTV surveillance is lawful when:

a) it is required for the fulfilment of duties provided for in separate laws (such as the Law on Albanian State Police). In such cases it is important to act in conformity with the provisions of such law;

b) the data subject gives his or her consent, but practically this is possible only in very restricted cases, when the identification of a group of persons which are within the camera coverage area is made explicit;

c) the data subject does not give his or her consent, but when provisions of article 6 of the Law on data protection (hereinafter the Law) are implemented.

Obligations of a controller which uses CCTV surveillance:

The system of video surveillance cameras should not abound intrusion in the privacy of individuals. A video recording system can be installed basically, if the goal can not be achieved in another way (a property, for example, can be protected from theft by using a lock). Moreover, the installation of CCTV surveillance systems is unacceptable in premises which are used exclusively for private purposes (such as showers, toilets, dressing rooms). Of course it is possible to offer data subjects the opportunity to choose between alternatives (it is possible, for example, to monitor the dressing rooms of a swimming pool provided that some space is reserved for dressing and it is not monitored).

Specifying the target goal. The purpose of recordings should be clearly specified and in compliance with the legal interests of the controller (e.g. protection of property against theft). Video recordings can be used only for the investigation of an occurrence which brought the violation of such interests which are protected by law. The lawfulness of the use of video recordings for other purposes should be limited to an important public interest, e.g. fight against crime.

Retention of recorded data should be determined. The retention period of recorded data should not exceed the maximum allowed time for the accomplishment of the purpose for which such data were recorded. Data should be retained within a period of 24 hours for example, if the property is under continuous surveillance, or for a longer period, **but not exceeding 7 seven days and after this period, data must be deleted** (longer periods are justified only in case of official holidays). This is not applicable for recordings made by the police in compliance with a separate law. Only in the event of a security incident, such data must be made available to executive authorities, courts or other similar institutions.

Security measures must be such as to protect the recording systems and transmission equipment which store the recorded data, protecting them from unauthorized or

accidental access, change, destruction, loss or unauthorized processing (see article 27 of the law)

It is important that personal information be kept safe and not misused or corrupted in any way. Safety is not only related to physical security measures, although they are very important. Safety also has to do with the organization of work in such a way as to minimize risk, for example, by ensuring that the personnel views the data only when it is necessary to perform their work properly and also by training the staff on what they need to do and what not.

Data subjects must be clearly informed about the existence and functioning of a CCTV surveillance system, by putting up a notice in the monitored area (see article 18), with the exception of cases when a special right or obligations arising from a special law are being exercised.

Other rights of the data subject must be guaranteed, respectively the right to access and the right to refuse processing of personal data (see article 12 of the law).

Office of the Commissioner must be notified about the processing of personal data, except cases when such processing is made in compliance with a separate law (see DCoM No.1232, **of 11 December 2009** and article 21 of the Law).

Installation and use of video surveillance systems and the processing of personal data must be in compliance with the fundamental human rights, the right to a private and family life. Such rights are enshrined in article 12 of the Charter of Fundamental Rights and by article 8 of the European Convention for the protection of Human Rights, as well as the data protection law.

The CCTV surveillance system and its connection with the intrusion in the private life. Use of CCTV may be considered reasonable or appropriate to achieve the objectives of the controllers, but always without prejudice to the protection of fundamental rights and freedoms of individuals.

A correct interpretation of the privacy concept is also important. The concept of private and family life is applicable not only in spaces such as bedrooms, toilets or entrance in the apartment building. Privacy does also imply a certain inviolable sphere for the individuals and their relatives. In a closed space such as an apartment where a person spends the majority of his or her life, the degree of privacy is undoubtedly bigger.

Controllers and processors (authorized persons) who during the exercise of their duties come to know the content of the data of video surveillance system, are bound to preserve the confidentiality and credibility even following termination of service or data collection. These data are not disseminated, except when provided by law (article 28 of the Law).

The following cases provide important information:

a) Official or business premises

Both, the public and private sector may install video surveillance cameras at the entrance of a building used as business premises, if this is necessary for the security of the persons and property, to ensure the monitoring of entrances to and exits from the building, or if due to the nature of work, there is a potential threat for the employers. The decision can be taken by a competent official body, the office manager or by other competent persons. The written decision needs to explain the reasons why CCTV cameras are going to be used. CCTV cameras may be installed also in compliance with provisions of the law or other acts. ***All employees who perform their work-related activities under the surveillance of cameras, must be notified in writing by the employer.*** *CCTV data systems must include recordings of individuals (footage and sound) date and time of entry and exit from the building as well as name and last name of the person, address of their temporary or permanent residence, job title, number and type of personal identity document and reason of entry into the building.*

b) Apartment buildings

Nowadays, the majority of people live who live in apartment buildings might decide to install security cameras. In order to install such cameras, the written consent of more than 70% of the inhabitants of the building must be given. The surveillance cameras in apartment buildings are installed only for the protection and security of persons and property, therefore it is allowed to monitor only the entrances and common areas. It is prohibited to use surveillance cameras for the monitoring of apartment owners or their activities, entrance into specific apartments. It is also prohibited to enable viewing of recorded data through individual TV sets, public televisions, internet or other telecommunication means which are capable of transmitting such recordings.

c) Work place

Surveillance cameras may be installed in the work place only in compliance with the conditions and manner prescribed by law. They may be installed only in specific cases, when this is necessary for the security of persons and property, for the protection of secret data or commercial secrets and when this purpose cannot be achieved through other more reasonable means. Therefore, security cameras may be installed only at work places which need to be monitored for security reasons. It is prohibited to monitor the work place, especially cabinets, drawers, elevator and sanitary facilities. Prior to installation of video surveillance equipment, employers of both public and private sector, must consult the representative of trade unions as well as notify their employees that the premises are protected by CCTV.

For the implementation of this Instruction, there will be a continuous cooperation and we will provide legal assistance both through the arrangement of efficient controls as well as by making available publications for a better understanding of the data protection law and the supervisory authority the Commissioner for the Protection of Personal Data.

This instruction enters into force on 5 March 2010 and is published in our official website, www.kmdp.al.

COMMISSIONER

FLORA ÇABEJ (POGAÇE)