apdcat

Agència Catalana de Protecció de Dades

# INSTRUCTION 1/2009

of 10 February, on the processing of personal data using cameras for video surveillance purposes.

(DOGC Nº. 5322, of 19.02.2009)

February 2009

Dr. Esther Mitjans
Director of the Catalan Data Protection Authority

*As the body in Catalonia charged with overseeing the right to the protection of data, one of the functions of the APDCAT is to issue instructions and recommendations which help adapt the processing of personal data to current regulations.*

*In this respect, it is important to remember that images, irrespective of the type of medium on which they may be found, constitute data of a personal nature and as such are guaranteed by the fundamental right to data protection.*

*In recent times, one of the concerns expressed to the APDCAT by citizens is that of the increase in video surveillance and how this may affect their rights and freedoms.*

*The right to the protection of data, like any other right, is not absolute. In other words, it is subject to limitations, such as public security or the rights of third parties. These limitations must however provide guarantees to avoid the right disappearing in the face of other rights and interests in play.*

*The Authority has drawn up this Instruction on the processing of personal data using cameras for the purposes of video surveillance with the intention of furthering compliance with current obligations, especially in those aspects that have generated most doubts in terms of application both for the public as well as for data controllers. Moreover, the issue may also affect such other rights as the freedom of expression, freedom of movement, the right to non-discrimination and, in short, human dignity itself. Prior deliberation must be given to the constitutional rights in play and to identifying social impact in order to minimise unwanted consequences for both individuals and society as a whole. An assessment of the suitability of installing video surveillance and the existance of a legitimate reason exists to do so are necessary to minimise risks. Video surveillance can only be considered constitutionally legitimate if it is proportionate, necessary and appropriate, and it must be impossible to achieve the same end employing less intrusive measures.*

*The Instruction places special emphasis on people's right to be informed of the existence of video surveillance systems; a right which includes, where necessary, being informed that voice is also being recorded.*

*Esther Mitjans Perelló*

*Director of the Catalan Data Protection Authority*

*Barcelona, 10 February 2009*

# INDEX

# *Instruction 1/2009, of 10 February, on the processing of personal data using cameras for video surveillance purposes*

The proliferation of video surveillance devices, not only for public or private security reasons but also for such other purposes as traffic regulation and control, workplace supervision or the monitoring of certain public services, has given rise to the adoption of various initiatives at the international level. These have also had to encompass the evolution of the technical means of acquiring images, with possibilities of identification, manipulation and large-scale dissemination, as well as ever-lower financial costs. Examples include Opinion 4/2004, of 11 February, by the Article 29 Working Party established in Directive 95/46/EC relating to the processing of personal data using surveillance by video camera; the International Conference of Data Protection Authorities in London in 2006; and the opinions adopted on 17 March and 2 June 2007 by the Venice Commission at the Council of Europe headquarters regarding video surveillance in public places and video surveillance in private spaces, which have underlined the need to adapt the use of these surveillance mediums to the requirements of privacy.

According to the definition of personal data in article 3.a) of Organic Law 15/1999, of 13 December, on the Protection of Personal Data (LOPD), the image and voice are considered personal data and thus fall within the scope of this Organic Law. Nonetheless, the absence in data protection legislation of specific provisions with respect to the acquisition and processing of images and, when appropriate, voice, makes it necessary to define the principles and guarantees established in the LOPD in this area by means of an instrument which, like this Instruction, clarifies the applicable legal framework. It falls within the Catalan Data Protection Authority's scope of action to establish legal certainty in this matter, along with a more detailed definition of those issues that may require further explanation.

Mention should be made of the regulation of video surveillance processing carried out by the national security forces as a contribution to people's harmonious coexistence, the fight against violence, and the peaceful use of thoroughfares and public spaces, as well as for the prevention of crime, misdemeanours and infractions connected with public security. Organic Law 4/1997, of 4 August, on the public security forces' use of video systems in public places was implemented in Catalonia by Decree 134/1999, of 18 May, on the regulation of video surveillance by the Generalitat police force and the local police forces of Catalonia, and by the Order of 29 June 2001 on regulation of the mediums by which information is provided on the existence of permanent video cameras installed in public places by the Generalitat police force and the local police forces of Catalonia. With respect to this and by virtue of the referral made in article 2.2 of the aforementioned Organic Law, data protection regulations, and consequently this Instruction, are only applicable to those questions which are not specifically regulated in that legislation, such as the obligation to create the corresponding file and notify the Catalan Data Protection Register of same in those instances provided for in that specific regulation that are not subject to registration in the Register. Such questions also include the application of security measures and exercise of the rights of rectification and objection.



A separate section will address the processing of images for traffic control, regulation, monitoring and disciplinary purposes which, by virtue of the Eighth additional provision of Organic Law 4/1997, is expressly subject to legislation on data protection and the protection of the right to honour, privacy and one's own image, in the framework of that Law.

Processing individuals' image and voice for surveillance reasons may amount to an infringement of certain fundamental rights regulated in Title I of the Spanish Constitution, essentially the rights to honour, privacy and one's own image and the right to the protection of personal data, but also to such other rights as that of freedom of movement, non-discrimination and, in short, human dignity itself (sentence of the ECHR of 28 January 2003 and 4 March 2008). While it may be necessary to admit the possibility of resorting to video surveillance when one or more of the legally provided circumstances is given (article 6.2 LOPD), in such cases the quality of the data and, specifically, the principle of proportionality, acquire special significance. In the light of the latter principle, an intrusive measure such as the one we are analysing can only be considered constitutionally legitimate if it proves to be proportionate through a triple analysis examining the need for that measure, its suitability and its proportionality, in the strictest sense of the word. That is to say, the same purpose cannot be achieved using measures which are less intrusive or which involve fewer risks for people (sentence of the ECHR of 28 January 2003, the sentences of the Constitutional Court 37/1998, 98/2000 and 186/2000, among many others).

Aware of the difficulty encountered by those responsible for data files and processing when attempting to consider the benefits, risks and implications that video surveillance may produce for the different rights in play, this Instruction sets out to provide further elements of judgement and valuation for the people who must decide about the installation of such systems.

Precisely with this in mind, special mention should be made of the provision contained herein regarding creation of a report prior to approval of the file, as a tool with which to conduct a comprehensive and systematic analysis of the characteristics of the processing to be carried out and of the circumstances that apply. The report fulfils not only a formal function of justifying the reasons for the measure but also enables a careful evaluation before taking the decision to proceed, thus offering a guarantee for the individual and ensuring the measure's appropriateness for achievement of the public interest.

In addition, reference should also be made to inclusion of the possibility, during the video surveillance system deployment process, of requesting a report from the Catalan Data Protection Authority as a tool to help achieve compliance with data protection legislation in the processing that will be carried out.

However, existence of one of the legally authorising circumstances and fulfilment of the principle of proportionality are not in themselves sufficient for the legitimate use of cameras for video surveillance purposes. The capturing and subsequent processing must also be carried out in accordance with guarantees which ensure respect for people's rights and minimise the risks produced.

With regard to people's rights as recognised in data protection legislation, this Instruction places special emphasis on the right of individuals to be informed of the existence of these surveillance systems. Recognised in a general manner in the LOPD, the right acquires special connotations which require adaptation of the legal provisions in this specific circumstance in order to enable their compliance. This Instruction also establishes special procedures for exercising the rights of access, rectification, cancellation and objection.

On the other hand and in order to minimise risks, set out herein are the provisions necessary to adapt security measures provided in data protection legislation to the special nature of data processed using these systems. Such measures will, in principle, be those applicable to automated processing, though in the case of recording systems which do not employ digital technology despite the use of technical devises, the implementation of measures provided for non-automated processing will be more adequate due to the more limited nature of processing operations inherent in analogical technology. Given that the image and voice are considered identifying data, applicable security will, in principle, be at the basic level. Notwithstanding this, when one or more of the circumstances in the processing carried out is especially relevant and requires application of medium or high-level security measures, the corresponding level must be applied.



This Instruction is issued in accordance with that provided in article 5.1.c) of Law 5/2002, of 19 April, of the Catalan Data Protection Authority, and article 15.1.e) of Decree 48/2003, of 20 February, approving the Statute of the Catalan Data Protection Authority. In its processing, the Instruction has been submitted for public information, for reports from the Security Secretariat of the Department of Institutional Relations and Participation, the Catalan Institute for Women, the Data Protection Advisory Council of Catalonia and the Legal Advice Commission, complying with that established in articles 63 and 64 of Law 13/1989, of 14 December, on the Organisation, Procedure and Legal System of the Administration of the Generalitat of Catalonia.

In virtue of the aforesaid and in accordance with the opinion of the Legal Advice Commission, I issue the following Instruction 1/2009, of 10 February, on the processing of personal data using cameras for video surveillance purposes.

Instruction:

## *Chapter I. General provisions*

### **Article 1** *Objective*

1.1 This Instruction applies to the processing of personal data consisting in the images and, when appropriate, voices of identified or identifiable individuals for the purposes of video surveillance using cameras or other analogous technical mediums.

1.2 Without prejudice to the applicability when appropriate of legislation on data protection and on the protection of the right to honour, privacy and one's own image, the following are excluded from this Instruction:

a) The capturing of images whose definition or characteristics do not enable the identification of specific individuals.
b) The capturing of images with video entry-phone systems, provided they are activated solely during the time necessary to identify the persons asking to be admitted to the building and the images are not recorded.
c) The capturing of images exclusively for the purposes of journalism.
d) The installation of fake cameras which are not able to capture images.
e) The processing of images or images and sounds for purposes other than that of video surveillance.

### **Article 2** *Definitions*

The following definitions apply for the purposes of this Instruction:



a) Processing: The acquisition, including for live viewing or broadcasting, recording, modification, communication, storage and subsequent elaboration of images and, when appropriate, voices, irrespective of the medium employed, as well as their deletion, blocking and cancellation.
b) Capture: The acquisition of images and when appropriate, voices, including for live viewing or broadcasting, irrespective of the device employed.
c) Storage: The recording on a reproducible medium of all or part of an image or voice.
d) Identifiable person: A person is considered identifiable when he or she may be identified directly through an image of their body or voice, or indirectly through other images, such as codes, identifiers, registration numbers or other means which, alone or in relation with other data, enable the identification of an individual without this requiring disproportionate time or effort.
e) Video surveillance: The capturing of images and when appropriate, voices, through a system of permanent or mobile cameras whose purpose is the surveillance and monitoring of buildings, installations, vehicles or other public or private spaces for reasons of public or private security, traffic control, employment monitoring, assurance of the normal operation of certain public services, monitoring of people's habits, conduct or condition, and for other similar reasons.
f) Camera: Device, apparatus or sensor designed to capture, print or reproduce still or moving images and sounds, when appropriate, irrespective of whether they are recorded or not and of the medium on which they are recorded.
g) Video surveillance camera system: The information system made up of one or more cameras and other elements installed for one same purpose by a Controller. The system includes the cameras, as well as the mediums designed to monitor, record, transmit or process the images or voices.
h) Disassociation of images: Processing of images by means of computer programs or tools or other techniques which, applied over an image or voice, prevents them from being associated with a specific person.

### **Article 3** *Subjective scope*

3.1 This Instruction applies to all bodies, organisations and entities connected with or dependent on the public institutions of Catalonia, the Administration of the Generalitat, the local authorities of Catalonia, the Catalan

universities and the public law corporations that carry out their functions exclusively in Catalonia which, in accordance with article 156 of the Statute of Autonomy of Catalonia, form part of the scope of authority of the Catalan Data Protection Authority.

It also applies to the individuals or legal entities that, on the basis of any agreement, contract or legal provision, manage public services or exercise public functions, provided that in the latter case the processing is carried out in Catalonia and is related to matters which fall within the competence of the Generalitat of Catalonia or the Catalan local authorities.

3.2 This Instruction applies to the data processing carried out by the entities mentioned in the preceding section, irrespective of whether all or part of such processing is performed by a third party on the instructions of one of those entities. In such cases, data protection legislation provisions concerning the party responsible for the data processing shall apply.

### **Article 4** *Applicable rules*

4.1 The processing to which this Instruction refers is governed by that established both in Spanish legislation and in that of the Generalitat of Catalonia in the field of data protection and other applicable legislation, as well as by that established herein.

4.2 The processing of personal data consisting in images and sound obtained by the Generalitat police (Mossos d'Esquadra) or by the local police forces of Catalonia using video cameras is governed by specific provisions and the special provisions, when applicable, in personal data protection legislation, as well as by that established herein.

4.3 That established in this Instruction is applicable without prejudice to the necessary compliance by entities responsible for the cameras with requirements stipulated in legislation on private security and by other applicable regulations.



## *Chapter II. Principles applicable to the processing of images*

### **Article 5** *Legitimacy of the processing*

5.1 The free, unambiguous and specific consent of the data subject or, failing this, any of the circumstances provided in article 6.2 of Organic Law 15/1999, of 13 December, on the Protection of Personal Data, is necessary for the use of cameras or video surveillance systems employed for any of the purposes provided in article 2.e) herein.
The use of cameras or video surveillance systems by the Generalitat police (Mossos d'Esquadra) or by the local police forces of Catalonia requires the corresponding authorisation in the circumstances provided in their specific legislation.

5.2 In cases where images area acquired that could reveal the ideology, trade union membership, religion or beliefs of data subjects, the processing shall only be considered legitimate when it has their express consent in writing. In the case of data that may refer to the racial origin, health or sex life of the data subjects it may be processed when, for reasons of general interest, a law so provides or the data subject gives his or her express consent.

The provisions of this section are not applicable to acquisition of the image of a person in which physical characteristics, appearance or even certain habits or conducts which could be considered especially protected data are processed in a purely incidental fashion.

The installation and use of video surveillance systems shall not be due to or give rise to constitutionally prohibited discriminatory practices.

5.3 Work on the installation of video surveillance equipment must be carried out by duly authorised private security companies. The Generalitat police (Mossos d'Esquadra) or corresponding local police force may install their own respective video surveillance systems.

5.4 The following do not comply with the legislation:

a) The installation of devices that enable the recording of other people's homes, except when carried out with their consent, or when any of the circumstances exist as provided in article 18.2 of the Spanish Constitution.
b) The acquisition of images of individuals in public spaces, except when carried out by the national security forces in accordance with their specific legislation. The incidental capturing of images of public spaces in the course of security surveillance of buildings or installations is only considered legitimate if it is inevitable in achieving the purpose of the surveillance of the building or installations in question.

5.5 The cession or communication of personal data consisting in images and when applicable, voices, obtained using video surveillance systems shall only be considered legitimate when it complies with that provided in articles 11, 21 and 22 of Organic Law 15/1999, of 13 December, on the Protection of Personal Data.
The cession or copying of images and sounds captured by the Generalitat police (Mossos d'Esquadra) or by the local police forces of Catalonia is governed by that provided in their specific legislation.

## **Article 6** *Purpose*

6.1 In accordance with the principle of quality of the data, images and when applicable, voices, may only be acquired and processed using video surveillance systems for particular, explicit and legitimate purposes.
The images and when applicable, voices, captured for a particular purpose may not be used for any different purpose, except with the consent of the data subject or when a law so authorises.



6.2 Images acquired for cultural or tourism purposes, or in order to provide meteorological or other similar information may not be used for video surveillance and, thus, must not enable the identification of specific individuals.

## **Article 7** *Proportionality*

7.1 Processing of the image and, especially, the voice of individuals for security purposes may only occur when it is appropriate to contribute clearly to the improvement of the service or activity, and the aforementioned purpose cannot be achieved with other mediums which, without requiring disproportionate effort, are less intrusive for the rights of persons.

This same principle of minimum intervention shall also apply to the choice of the technology employed, the recording duration and the decisions made regarding the conservation and access to the images.

7.2 Prior to installing video surveillance systems the persons responsible for their use should consider the different rights and legally protected interests in play, analysing:

a) The need to use these systems.
b) The suitability of installing video surveillance systems to achieve the purposes sought.
c) The inherent risk to persons' rights in view of the characteristics of the video surveillance system employed, circumstances of the acquisition of the images and the people affected.
d) The absence of alternative security measures that involve a lesser risk, in relation to possible interference with fundamental rights.

Such consideration shall be documented in the report provided for in article 10 herein.

7.3 The following may not satisfy the principle of proportionality:

a) The installation of cameras in spaces such as bathrooms, toilets, changing rooms, recreation or rest rooms with restricted access, or hotel rooms and other similar spaces where, by their very nature, the acquisition of images would be especially intrusive with respect to the right to privacy, personal dignity and the free development of personality. This also applies to rooms in care centres, except when necessary to protect a vital interest of the data subject. In the case of cells used for police detainees or in prisons or similar places of imprisonment, the installation shall not be considered proportionate except where there exists a higher legitimate interest which justifies same.
b) The use of video surveillance systems in work areas for the exclusive purpose of monitoring workers' performance.
c) The installation in educational areas of cameras in classrooms, gymnasiums or students' recreational areas for the monitoring of same.

7.4 The capturing and recording of an individual's voice along with the recording of his or her image using video surveillance systems may only be considered legitimate in exceptional cases when the conversation is not strictly private, when the purpose of the video surveillance cannot be achieved by recording solely the image, and providing the reasons justifying such voice recording are stated in the report provided for in article 10 herein.

Should conversations of a strictly private nature be recorded they shall be cancelled, except when consent is given by the data subject or when conservation or communication of the information is authorised by a regulation with the status of law.

## **Article 8** *Storage of images*



8.1 In those cases where the intended purpose cannot be achieved without storing the images, the storage period shall not exceed that which is necessary to fulfil the objective for which the data is acquired or recorded. As a general rule, it is recommended that cancellation of the processed images should be carried out within a maximum period of one month from their acquisition.

8.2 The cancellation shall be produced without prejudice to the blocking obligation, according to which the images may be stored to be available to the public administrations, courts and judges for possible liabilities arising from the processing of data during the statute-of-limitations periods of the corresponding responsibilities.

8.3 Blocking shall result in the images and when applicable, voices, remaining outside the usual circuits of use and their custody being established using a system that enables the monitoring and recording of any access to same that may take place for the purposes referred to in the preceding section.

In the case of images on digital medium, this shall also entail their encryption.

In the case of images recorded on mediums other than digital, blocking shall be guaranteed by means of labelling which indicates this circumstance, together with their storage in sealed boxes, containers or other recipients with restricted access. These mediums shall remain under the custody of the data Controller or security officer, where applicable, or the person delegated by same, but in no case may this person be the operator of the system.

8.4 When images or voices have been captured accidentally in circumstances which result in their being illicit they shall be eliminated immediately upon knowledge of their existence.

8.5 The storage of images and sounds acquired by the Generalitat police (Mossos d'Esquadra) or by the local police forces of Catalonia is governed by that provided in their specific legislation.

## Chapter III. Creation and registration of files

### Article 9 Creation of files

9.1 To be able to initiate the acquisition of images, the corresponding file shall previously have been created in accordance with that established in the legislation on the protection of data of a personal nature and in this Instruction, except when images are captured without being stored.

9.2 Without prejudice to those cases in which the request for a report is compulsory, prior to creation of the file or, where applicable, start-up of the system or of one or more cameras, the Catalan Data Protection Authority may be asked to draft a report on the processing's compliance with data protection legislation. The request for a report must be accompanied by the draft agreement or general provision for creation of the file and by the report referred to in the following section.

9.3 The file may include images referring to one or more cameras provided that, in the latter case, these images present sufficient homogeneity in relation to the purpose for which they were captured, the characteristics of their acquisition and the processing it is intended to carry out with them.

9.4 In data processing operations carried out by the Generalitat police (Mossos d'Esquadra) or by the local police forces of Catalonia and subject to recording in the register as provided for in these forces' specific legislation, creation of the file is not necessary.

### Article 10 Report

10.1 Prior to creation of the file or to start-up of a video surveillance system in those cases in which images are not recorded, a Report shall be drafted which shall refer to the following points:

a) The responsible body, organisation or entity: Identification of the person responsible for the file, of the persons operating the video surveillance system and, when applicable, the person responsible for the installation and its maintenance.
b) Justification of the legitimacy of the intended acquisition or of the subsequent processing, stating whether the data subjects have given their consent or, if this is not the case, which sections of article 6.2 of Organic Law 15/1999, of 13 December, on the Protection of Personal Data and, where necessary, other applicable legislation, apply in the case in question, for the purposes of legitimating the processing of the images and voices.
c) Justification of the purpose and proportionality of the system, in accordance with that established in articles 6 and 7 herein.
d) Personal data processed: The Report shall specify whether the voice will also be recorded and whether the purpose is expected to entail acquisition of images that reveal especially protected personal data or other information which would require a medium or high security level.
e) Location and field of vision of the cameras: Reference must be made to the location and orientation of the cameras. In particular, when the system includes exterior cameras it must be stated whether there are health centres, places of worship or religious assembly, political party headquarters or centres of education attended by minors within a radius of 50 metres. Mention shall also be made of the spaces that enter into the cameras' field of vision.
f) Definition of the system's characteristics. This section shall include specification of:
The total number of cameras that make up the system.
Technical conditions of the cameras and other elements.
Whether the cameras are fitted with slots or connections for external recording devices.
Whether the cameras capture still or moving images.
Whether the possibility is available to obtain close-ups at the time of acquisition of the images or once they have been recorded.
Whether the images will be visualised directly or only recorded, with access limited to certain circumstances provided in the Report.
Whether the acquisition and, where applicable recording, will be continuous or discontinuous.
Whether the images will be broadcast.

Provisions relating to the mechanisms of identification and disassociation available to respond to any request from the data subject to exercise his or her right to access, rectification, cancellation and objection.
When the voice is recorded, the distance at which it can be captured shall also be specified.

g) Duty to inform: Reference shall be included to the number and location of the information warning signs, as well as to other additional informative mediums employed, in order to demonstrate compliance with the duty to inform.
h) The period for which the system will be installed and the period of storage of the images.
i) Measures intended to evaluate the results of the system's operation and its need for maintenance.
j) Security measures: Specification of the security level required and description of the security measures applied.

10.2 The information referred to in sections e) and g) shall be accompanied by the corresponding graphic information.

10.3 In publicly-owned files this Report may form part of the report provided for in the procedure for development of the general provisions.

10.4 The Report shall also be drawn up when processing of the image and when applicable, the voice, is supplementary to another processing operation. In such cases this circumstance must be specified and justified.

10.5 The Report shall be made available to officials of the Catalan Data Protection Authority who carry out inspections.

### **Article 11** *Registration of video surveillance files*



11.1 Any processing of personal data that involves the recording of images of identified or identifiable individuals, captured using one or more cameras that form part of a video surveillance system, constitutes a file and must be notified to the Catalan Data Protection Register. Notification shall be made once the file has been created, in accordance with that provided in data protection legislation, using the form established by resolution of the director of the Catalan Data Protection Authority. Any modification or deletion of files must also be registered.

11.2 The acquisition of images that are not stored is exempt from the obligation to register.

11.3 If the acquisition of images constitutes a supplement to or complement of another processing operation it may be registered as a single file.

11.4 The Catalan Data Protection Authority forwards to the General Data Protection Register of the Spanish Data Protection Agency all registrations, modifications or deletions of video surveillance files that are made in the Catalan Register.

11.5 The provisions of this article do not apply to personal data processing operations using video surveillance systems carried out by the Generalitat police (Mossos d'Esquadra) or by the local police forces of Catalonia, which shall be recorded in the Register of Authorisations as provided for in these forces' specific legislation, notwithstanding which, cooperation agreements may be established between this Register and the Catalan Data Protection Register.

## *Chapter IV. Duty to inform*

### **Article 12** *Information*

12.1 Those responsible for the processing of images using permanent cameras shall provide clear and permanent information about the existence of such cameras by placing as many warning information signs as necessary to

ensure the data subjects are aware of their presence. This duty is equally applicable when the images captured are not recorded.

12.2 The information signs shall be placed prior to initiation of the acquisition of images and voices, even in the case of trials of the equipment, and may only be withdrawn once the system has been uninstalled.

12.3 The signs shall be placed where they can be clearly seen before entering the cameras' field of vision. Specific location of the signs will depend in each case on the nature and structure of the zones and spaces subject to video surveillance. Nonetheless, the following conditions shall be taken into consideration:

In the case of video surveillance cameras in buildings or installations, an information sign shall be placed in each of the entrances to the area under surveillance. Moreover, if the buildings or installations are divided into floors a further information sign shall be placed on each floor fitted with video cameras, in the main entrance to the area or zone subject to the video surveillance.

In the case of video surveillance on public transport, a minimum of one information sign shall be placed in each of the points of access to the area under surveillance, as well as at the entrance to vehicles subject to video surveillance, in a place where they are clearly visible to the data subjects entering same.

In the case of video surveillance cameras in open spaces, an information notice shall be placed at a sufficient distance for the data subjects to be clearly and permanently aware of the existence of such cameras in the area or zone they are entering. In any case, the location of the information sign shall be at a distance not exceeding 50 metres from the exterior limit of the area.

12.4 The content and design of the information sign shall conform to that established in the appendix to this Instruction, but under no circumstances is it required that said sign specify the location of the cameras.

The sign may be substituted by information provided by electronic panels when these offer a permanent image of the sign or when it may be read and appears with a frequency that ensures data subjects' awareness of the video surveillance cameras.



12.5 The data Controller is responsible for the conservation and maintenance of the information signs in order to ensure they enable data subjects to be aware at all times of the existence of the cameras.

12.6 The data Controller or the person designated in his or her place shall also provide data subjects with information about the remaining points provided in article 5.1 of Law 15/1999, on the Protection of Personal Data, in printed form or through the website, in which the specific purpose of the video surveillance shall be stated, together with the information established in sections a), d) and e) of article 5 of the aforementioned law.

12.7 Additionally and when applicable, further mediums such as the use of public address systems for example may be employed to comply with the duty to inform which ensure that all individuals are aware of the existence of the cameras.

12.8 In the case of permanent cameras employed on public roads for traffic control, monitoring and disciplinary purposes, the content of the sign may be limited to informing about the existence of the camera or speed monitoring device, without prejudice to that established in section 6 of this article.

12.9 Except when their presence is clearly perceptible, information about the existence of mobile cameras must be provided to the extent that this is possible during the same recording process or, if this is not possible, through other mediums.

12.10 Compliance with the duty to inform in processing operations subject to legislation on the use of video cameras by the Generalitat police (Mossos d'Esquadra) or by the local police forces of Catalonia is provided for in these forces' specific legislation.

## *Chapter V. Rights of access, rectification, cancellation and objection*

### **Article 13** *Right of access*

The right of access includes the entitlement of the data subject, owner of the image or voice, to be informed by the data Controller about whether his or her image has been captured by video surveillance systems, the purpose of such capturing, whether the image is recorded in a file, whether it is the object of any other type of processing, whether any communication of the data has been or is intended to be carried out and the period the images or voices will be stored.

When the data subject so requires, he or she also has the right to access the images or voices and obtain a copy thereof, as well as of any subsequent processing operations that may have been performed on said images and voices.

Should exercise of the right also affect images or voices pertaining to third parties, except when their consent has been secured, access shall require the prior disassociation of such images and voices using any means which impedes their identification. When such disassociation requires disproportionate effort due to the period of time recorded or the high number of third parties affected, the data Controller may request that the period of the recording to which access is requested be reduced.

### **Article 14** *Right of rectification*

14.1 The right of rectification of images or voice captured by video surveillance systems shall only apply when the image or voice in question has been distorted or altered subsequent to its acquisition.

14.2 In order to comply with that provided herein, when images or voices are altered or distorted a copy of the original recording shall be kept or a method of recovering the original data be available. The alteration or distortion shall be recorded in the Incident Register, with indication of the period in question and the reasons for such actions.



### **Article 15** *Right of cancellation*

The data subject may, by exercising the right to cancellation, demand the deletion, with prior blocking, of his or her images or voice whose processing has been inadequate, excessive or contrary to legal rules.

### **Article 16** *Right of objection*

16.1 By exercising the right of objection unless a law or a European Directive states otherwise, the data subject may demand exclusion of the processing of his or her image or voice in those cases in which consent is not necessary. The request to exercise this right must be based on justifiable and legitimate reasons relating to a specific personal situation.

16.2 The right of objection may also be exercised in the case of files whose purpose is that of advertising or commercial prospection, or when the purpose of the processing is that of adoption of a decision referring to the data subject based solely on automated processing of his or her personal data.

### **Article 17** *Procedure for exercising rights*

17.1 In order to exercise the rights of access, rectification, cancellation and objection, a request must be made to the data Controller or, when applicable, the person responsible for the processing, indicating the place, date and approximate time in slots not exceeding two hours in which the data subject's image was obtained. The request shall be accompanied by a photo of said data subject corresponding to the period in which his or her image was captured which enables his or her identification. Image recognition tools may be employed to check the coincidence between the image provided and those recorded.

17.2 In video surveillance systems that record the voice, the right of access may be exercised by providing a recording of the data subject's voice. For this purpose, the devices used by the person responsible for video surveillance systems that record sound shall be equipped with voice recognition tools that enable confirmation of the coincidence between the recording of the voice provided and one of the voices recorded.

17.3 If the photo or voice provided does not offer sufficient definition or elements that enable their identification, a period of amendment of 10 working days shall be granted for the data subject to provide another photo or voice recording.

17.4 The procedure for and resolution of the request is governed by that established in personal data protection legislation and by this Instruction. The duty to resolve persists irrespective of whether the images have been recorded or not or have already been cancelled when the right is exercised. In the latter case, such resolution may be limited to reference to this circumstance and notification of the material impossibility of fulfilling the right being exercised.

17.5 The request to exercise the rights of access, rectification, cancellation or objection may be denied when the required conditions are not met, or when the level of coincidence between the image or voice provided with the request and those which have been the object of the processing is insufficient to guarantee that the latter corresponds to the data subject.
The request may also be denied when they have not been recorded or have already been cancelled.

17.6 In the event of denial of rights or of the data subject not receiving a response before the established deadline, he or she may formulate an appeal to the Catalan Data Protection Authority.

### **Article 18** *Images and voice acquired by the national security forces*

18.1 Exercise of the rights of access and cancellation of images or voice processed by the Generalitat police (Mossos d'Esquadra) or by the local police forces of Catalonia is governed by these forces' specific legislation.



18.2 The rights of objection and rectification in relation to images captured by cameras for which the aforementioned police forces are responsible shall be exercised in accordance with that established in Spanish state or regional laws on the protection of personal data, as well as by that stipulated herein.

## *Chapter VI. Security measures*

### **Article 19** *Obligations of the data Controller*

19.1 The data Controller shall implement the technical and organisational measures required to ensure the authenticity, integrity and confidentiality of the images acquired by camera systems, as well as to prevent their alteration, loss and unauthorised processing or access.

19.2 The data Controller shall inform those persons who have access to the images in the performance of their functions that they must comply with the obligation to confidentiality and that this obligation persists even after termination of their labour relationship.

19.3 The provisions of this chapter are also applicable to files and processing operations carried out by video surveillance systems for which the Generalitat police (Mosses d'Esquadra) or the local police forces of Catalonia are responsible.

### **Article 20** *Security level*

20.1 The security level to be assigned to the file is that stipulated in the legislation regulating required security levels in the processing of personal data, in accordance with that established in the Report referred to in article 10 hereof.

20.2 As a general rule, the acquisition and processing of images of identified or identifiable individuals requires the basic level of security, without prejudice to the application, in certain circumstances, of the medium or high security levels specified in the aforementioned legislation.

Without prejudice to the other circumstances provided for in data protection legislation, the capturing and processing of certain images or voice which, in a predictable and significant manner and not merely by chance, offer information which enables the evaluation of aspects of the data subject's personality traits or conducts requires medium level security measures. The high security level is required when they provide information about especially protected data, when the images are acquired or processed for police purposes without the consent of the data subjects, or when they relate to acts of gender-based violence.

20.3 The acquisition of an image of an individual in which, in a purely incidental manner, it is possible to distinguish physical traits, the appearance, certain habits or conducts or other circumstances which could merit the attribution of a different security level does not alter the level of security which is to be applied if that circumstance is not taken into account in the processing performed.

20.4 The processing of images captured with video surveillance systems and which are supplementary to other main processing operations may be segregated from the latter and the level of security measures applied that corresponds to the processing of those images, providing the users who have access to same are recorded and this is stated in the security document.

## **Article 21** *Security measures*

21.1 The technical and organisational measures stipulated in personal data protection legislation for automated files or processing operations in accordance with the security level established in the preceding article shall be applied to the images and when applicable, voices, obtained or processed using digital video surveillance systems, including during the trials of same.



21.2 The technical and organisational measures stipulated for non-automated files or processing operations shall be applied to those images and when applicable, voices, which are obtained or processed with devices that do not employ digital technology or which, subsequent to their acquisition, are incorporated onto mediums which are not based on digital technology.

21.3 Likewise and in recognition of the inherent risks of video surveillance systems, the Controller may implement measures which are additional or complementary to those expressly required by legislation on the protection of data of a personal nature.

21.4 In order to adapt the measures provided for in data protection legislation to the security requirements deriving from the processing of images and voice, the following shall be taken into account:

a) The security document shall define the users or user profiles of those who may handle the cameras and those who may see the live or recorded images. Likewise, it shall define the persons who may perform blocking, deletion, destruction, storage, identification and distortion operations and any other manipulation of the images, as well as the staff who may authorise, modify or revoke access by third parties. When this is established on the basis of user profiles the number of such persons shall be limited in the same security document.
b) Viewing equipment shall be located in restricted areas inaccessible to the public or, failing this, zones where the images are not visible to unauthorised persons.
c) The person responsible for the file or processing shall implement such measures as may be necessary to ensure the training of system operators in the custody, reservation and security of the images, as well as in attending to the exercise of persons' rights through a flexible procedure.
d) Necessary measures shall be implemented to ensure the complete destruction of content in digital file deletion operations or in the re-use of mediums for analogue recordings.
e) The creation of backup copies of automated files must be carried out on a weekly basis, except when the image storage period is less than one week.
f) When it is necessary to apply high-level security measures to automated files or processing operations, the Access Register must record the identification of any user who attempts to access the system or file,

his or her user profile, the date and time of the attempt, the functions he or she attempts to carry out and whether they have been authorised or not. If authorised, record shall be kept of the images accessed and they shall be identified with the date and period of time during which they are visualised.
If the processing is not performed with a digital system, the Access Register shall be operational as from the day following the date on which the recording was made. This Register shall be maintained by the person responsible for the custody of the recordings, who may not be one of the system operators.

21.5 For the purposes of ensuring their integrity and at the same time facilitating the exercise of rights, the images shall incorporate a dating system which indicates the day and time they were captured.

21.6 In those circumstances in which images are not stored, security measures shall nonetheless be implemented insofar as they are applicable.

### **Article 22** *Security document*

22.1 The technical and organisational measures required for processing the images shall be stipulated in the security document. When the processing of the image is of a secondary nature, it shall be stipulated for in the security document corresponding to the main processing operation.

22.2 The security document shall include those aspects provided for in data protection legislation.

### Transitory provisions *Pre-existing files and processing*

1 The video surveillance files already existing on entry into force of this Instruction shall adapt to that established in article 12 herein within 3 months of its publication.

In the case of cameras that solely capture images, the information signs which were already in place on entry into force of this Instruction and which conformed to that established in Instruction 1/2006 of the Spanish Data Protection Agency shall remain valid. In such cases, the period stipulated in the preceding paragraph shall not apply until such time as these signs are replaced.



2 The storage and processing of images and voice, including those recorded prior to entry into force of this Instruction, shall be adapted to the new security measures, obligations and guarantees provided herein within a period of 3 months from its publication.

3 The provisions of article 10 herein are only applicable to video surveillance system files created as from the entry into force of this Instruction.

### Sole final provision *Entry into force*

This Instruction shall enter into force on the day after its publication in the Official Gazette of the Generalitat of Catalonia.

Barcelona, 10 February 2009

Esther Mitjans Perelló
*Director of the Catalan Data Protection Authority*

## Appendix

1 The sign referred to in article 12 herein shall clearly and visibly contain, from top to bottom, at least the following information:

Indication of the purpose for which the data is being processed ("Video surveillance area").
A pictogram which symbolises a video surveillance camera inside a white rectangle. When the voice is captured, the pictogram shall reflect this circumstance.
The informative text "data protection".
Express indication of the identification of the data Controller to whom requests for exercising the rights of access, rectification, cancellation and objection may be addressed.
Indication of the place or website where the information referred to in article 12.6 herein may be obtained.

2 The design of the information sign shall conform to the following requirements:

a) It shall be rectangular with the edges at right angles. The standard dimensions of the sign are, approximately, base 21 cm by height 29.7 cm.
These dimensions may be increased or reduced according to the area or zone subjected to video surveillance and to the distance from which the information must be visible to the affected parties.
b) The background is yellow, and the logo of the Catalan Data Protection Authority may be included in the top left-hand corner.
c) The pictogram referred to in section 1 of this appendix must be centred in a white rectangle whose dimensions are approximately 1/3 of the height of the sign and 4/5 of its width and which, in the standard sign, is situated approximately 6 cm from the upper edge of the sign.
In any case, these indications shall maintain the proportions indicated in any possible variations of the dimensions of the information sign.

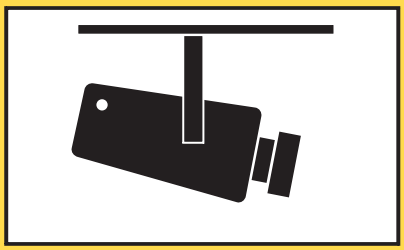


3 Examples of the sign conforming to the requirements established herein are available on the website of the Catalan Data Protection Authority, www.apd.cat, from which they may be downloaded.

(09.034.046)

apdcat

**ZONA VIDEOVIGILADA**



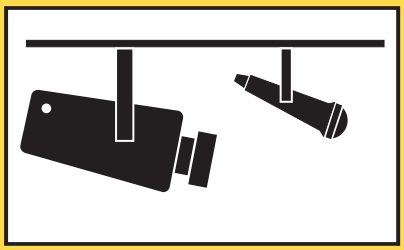
PROTECCIÓ DE DADES

POT EXERCIR ELS SEUS DRETS DAVANT:

PER A MÉS INFORMACIÓ:

apdcat

**ZONA VIDEOVIGILADA**



PROTECCIÓ DE DADES

POT EXERCIR ELS SEUS DRETS DAVANT:

PER A MÉS INFORMACIÓ:

apdcat

Agència Catalana de Protecció de Dades

www.apd.cat