VIDEO SURVEILLANCE GUIDELINES BY THE ITALIAN DPA

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

VIDEO SURVEILLANCE GUIDELINES BY THE ITALIAN DPA

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Table of Contents

THE ITALIAN DATA PROTECTION AUTHORITY

Having convened today in the presence of its President, Mr. Francesco Pizzetti, its Vice-President, Mr. Giuseppe Chiaravalloti, its members Mr. Mauro Paissan and Mr. Giuseppe Fortunato, and its interim Secretary-General, Mr. Daniele De Paoli;

Having regard to the draft provision on video surveillance as approved by the Italian DPA on 22 December 2009 and forwarded to the Ministry for Home Affairs, the Union of Italian Provinces (UPI), and the National Association of Italian Municipalities (ANCI) in order to gather their specific comments as for the respective areas of competence;

Taking account of the remarks made by ANCI via letters dated 25 February 2010 and 29 March 2010, respectively;

Taking account of the remarks submitted by the Ministry for Home Affairs via a letter dated 26 February 2010;

Having regard to the Personal Data Protection Code (legislative decree no. 196 dated 30 June 2003);

Having regard to the remarks submitted by the Office via the Secretary General pursuant to Article 15 of the Rules of Procedure no. 1/2000;

Acting on the report submitted by Prof. Francesco Pizzetti

1. FOREWORD

The processing of personal data by means of video surveillance is not regulated by specific legislation; accordingly, the general provisions on personal data protection are applicable in this context.

The Italian data protection authority considers it necessary to address this issue again by way of this general scope decision that replaces the one issued on 29 April 2004.

This is due both to the many regulatory instruments introduced with regard to video surveillance and to the considerable amount of questions, reports, complaints and prior checking applications lodged with the Italian DPA.

It should be recalled that over the past five years some pieces of legislation empowered mayors and municipalities to discharge specific tasks related to public safety and urban security, whilst other regional and State laws envisaged economic benefits for public bodies and private organizations in order to foster the use of video surveillance as a method for passive defence against, control of and deterrence against crime and vandalism.

2. PROCESSING OF PERSONAL DATA AND VIDEO SURVEILLANCE: GENERAL PRINCIPLES

Collecting, recording, storing and - generally speaking - using images entail the processing of personal data (see section 4(1)b. of the DP Code). Personal data means any information related to a natural person that is or can be identified, whether directly or not, by reference to any other type of information.

A non-exhaustive analysis of the main applications can show that video surveillance is employed for the most diverse purposes, some of which can be grouped into the following categories:

1. Protection and integrity of individuals - including urban security; ordre public; public bodies' prevention, detection and/or suppression of offences; streamlining and improving publicly available services also in order to enhance user safety pursuant to the competences vested in the said bodies under the law;

2. Protection of property;

3. Detecting, preventing and controlling breaches of the law as performed by public bodies pursuant to the competences vested in them under the law;

4. Taking of evidence.

The need to ensure, in particular, a high level of protection of fundamental rights and freedoms when processing personal data allows resorting to video surveillance on condition this does not interfere to an unjustified extent with data subjects' rights and fundamental freedoms.

There is little doubt that the installation of image-collecting systems should be carried out in accordance not only with data protection legislation, but also with the requirements set forth in other pieces of legislation where applicable - such as for instance the civil and criminal law provisions in force concerning unlawful interference with private life; the legislation protecting employees from monitoring in the workplace; the regulatory instruments on security in sports facilities and stadiums, museums, public libraries and State archives; the regulations concerning installation of audiovisual equipment on passenger ships travelling on domestic routes; and the regulations concerning harbours, railway stations, metropolitan railway stations, and urban transportation facilities.

Given the above context, it is accordingly necessary:

a. For the processing of data via video surveillance to be grounded in any of the lawfulness preconditions expressly referred to in the DP code as for public bodies - discharge of institutional functions, see sections 18-22 of the DP Code - and private bodies/profit-seeking public bodies, respectively - e.g. fulfilment of legal obligations, compliance with a so-called "balancing of interest" decision by the Italian DPA as per point 6.2 below, free and explicit consent by the data subject, see sections 23-27 of the DP Code. These preconditions are applicable to different sectors, which is why they are referred to separately in the paragraphs below as for the public and the private sector, respectively;

b. For every IT system including the respective software to be designed from the start in such a way as to not use data related to identifiable individuals if the purposes of the processing can be achieved by only relying on anonymous data - e.g. by configuring the software to only enable bird's-eye views in monitoring road traffic without zooming in images and making individuals identifiable. This is a requirement arising out of the data minimization principle, whereby IT systems and software should be configured in order to minimize the use of personal data (see section 3 of the DP Code);

c. For video surveillance to be carried out in compliance with the so-called proportionality principle when selecting filming arrangements and location (e.g. the use of fixed or pan-tilt cameras with or without zooming) as well as in the course of the processing of data, which must be in any case relevant and not excessive in connection with the purposes to be achieved (see section 11(1)d. of the DP Code).

3. OBLIGATIONS APPLYING TO PUBLIC AND PRIVATE BODIES

3.1. Information Notice

Data subjects should always be informed that they are about to enter an area under video surveillance; this also applies to events and/or public shows (e.g. concerts, sports events, etc.).

To that end, the DPA considers that the same simplified model of "minimal" information notice - where the data controller and the purpose of the processing are specified - can be used as described in the 2004 video surveillance decision by this DPA pursuant to section 13(3) of the DP Code; a facsimile model notice is shown in Annex 1 to this decision.

The above model notice can obviously be adjusted to the specific requirements. If several cameras are deployed and/or the area under surveillance is especially large, and by having regard to the filming arrangements, several notices may have to be posted.

The said information notice:

- should be posted outside the area covered by the surveillance cameras, but it can be as close as possible to them and need not be posted on the devices themselves;

- should be formatted and posted in such a way as to be clearly visible regardless of lighting conditions, including during night operation of the video surveillance system;

- may include a symbol and/or graphical parts that should be immediately and easily understandable and may also be different to specify whether the images are only viewed or are also recorded.

In this DPA's view, it is desirable for the simplified information notice mentioned above to refer to the availability of a detailed notice that should contain all the items referred to in section 13(1) of the DP Code. This detailed information notice should be available easily and without any charges to data subjects, and it should be easily accessible also via IT tools - in particular via the Internet and/or Internet websites, by means of its posting on billboards and indoor areas, via notices and warnings placed close to teller windows, via pre-recorded messages that can be played by dialling a toll-free number, etc. .

Nevertheless, it should be recalled that data controllers have to provide adequate information where requested to do so, also by way of a person in charge and in verbal form; such information should contain the items mentioned in section 13 of the DP Code.

3.1.1. Information Notice and Security

Some provisions in the DP Code including the obligation to inform data subjects beforehand do not apply to the processing of personal data - including sound and image data - that is performed by "either the Data Processing Centre at the Public Security Department or by the police with regard to the data that are intended to be transferred to said centre under the law, or by other public bodies or public security entities for the purpose of protecting public order and security, the prevention, detection or suppression of offences as expressly provided for by laws that specifically refer to such processing."

(see section 53 of the DP Code).

Under the above provision, the aforementioned data controllers should comply with the following:

a. They may fail to provide an information notice if personal data is processed for the purposes of protecting ordre public and/or preventing, detecting or suppressing criminal offences;

b. They may only process personal data if this is expressly provided for by laws that specifically refer to such processing.

3.1.2. Additional Specifications: Non-Mandatory Information Notices When Video Surveillance Is Aimed at Protecting Ordre Public or Preventing, Detecting or Suppressing Criminal Offences

To enhance the protection of data subjects' rights and fundamental freedoms, this DPA considers that it is strongly advisable to provide an information notice whenever video surveillance is carried out under the terms of Section 53 of the DP Code - even though this is not mandatory - if there are no specific grounds that prevent this from being done as related to ordre public and/or the prevention, detection or suppression of criminal offences.

Obviously, this will only be possible following careful assessment to establish that the provision of an information notice would not hamper, indeed would enhance, the discharge of the specific tasks; account should also be taken that disclosing the presence and use of video surveillance systems often works as an effective deterrent.

To that end, data controllers may inform on the collection of images by means of video surveillance also through simplified notices, which should highlight that video surveillance systems are deployed for protecting ordre public and security and/or preventing, detecting and suppressing criminal offences - e.g. via graphics, symbols, specific labels, etc. to be posted as appropriate.

Those data controllers that decide to provide information notices are obviously empowered further to not apply the provisions of the DP Code referred to exhaustively in section 53(1), letters a. and b., thereof.

Finally, it should be pointed out that a suitable information notice must be provided whenever the processing of personal data by means of video surveillance as performed by law enforcement bodies and/or other public bodies does not fall within the scope of section 53 of the DP Code - e.g. if video surveillance is used to detect and fine road traffic violations.

3.1.3. Information Notices Provided by Private Entities That Are Connected to the Police

The processing of personal data by private entities relying on video surveillance systems that are linked directly to the police falls outside the scope of section 53 of the DP Code. Accordingly, the implementation of the said links must be disclosed to data subjects. This DPA considers that the aforementioned simplified model of "minimal" information notice may be used for this purpose - specifying who the data controller is, what purposes underlie the processing, and that the surveillance system is connected to the police; this simplified model notice pursuant to section 13(3) of the DP code is shown in Attachment 2 to this decision.

The detailed notice to be made available to data subjects should also mention the existence of the linkage in question.

The above processing operations fall within the scope of application of point 4.6. hereof.

Failure to comply with the provisions concerning information notices as per section 13 of the DP code, e.g. if no notice is provided or the notice is inadequate because it does not specify who the data controller is, what purposes are pursued, and that the system is connected with the local police, is punished by the administrative sanction set forth in section 161 of the DP Code.

The issues related to the competences allocated to municipalities with regard to urban security will be addressed in point 5.1. below.

3.2. Specific Requirements

3.2.1. Prior Checking

The processing of personal data in connection with video surveillance should be performed by complying with the measures and arrangements specified by the DPA as a result of a prior checking exercise, which may be initiated ex officio or else following the application lodged by the data controller (section 17 of the DP Code) if there are specific risks to data subjects' rights and fundamental freedoms and/or to their dignity; account is taken in this connection of the nature of the data, the processing arrangements and/or the effects produced by the processing.

The above requirements apply unquestionably to video surveillance systems coupled with the use of biometrics. The blanket, unrestrained use of biometrics information may factually entail the risk of substantially prejudicial effects for data subjects because of the peculiarities of that information; accordingly, it is necessary to prevent the inappropriate use and/or the misuse of biometrics data.

For instance, prior checking by this DPA will be required in respect of video surveillance systems equipped with software that enables recognition of individuals by matching and/or comparing the images captured (e.g. faces) with other specific personal data (in particular biometrics data), or else by comparing a given image with a sample created prior to capturing of the image in question.

Similar obligations apply to the so-called smart systems, which do not simply film and record images as they can also automatically detect "deviant" behaviour and/or unusual events, send out alerts and record the relevant images. In principle, these systems should be considered to go beyond the standard remit of video surveillance, since they can result into considerable interference with the data subject's self-determination sphere - and accordingly impact on his/her conduct. Their deployment can only be justified in specific cases, by taking account of the purposes and context underlying the data processing - which should be assessed on a case-by-case basis in terms of its compliance with data minimization, proportionality, purpose limitation and fairness principles (see sections 3 and 11 of the DP Code).

The use of integrated video surveillance systems should undergo prior checking if the processing arrangements do not fall into line with those mentioned under points 4.6. and 5.4. hereof.

Prior checking shall also be necessary whenever the retention period of the recorded images is to be extended beyond the maximum 7-day term on account of special requirements - unless such extension results from specific requests made by judicial authorities and/or the judicial police with regard to ongoing investigations (see point 3.4.).

Regardless of whether any of the above conditions is fulfilled, a data controller shall be required to apply for prior checking by this DPA whenever the nature and features of the processing to be performed by means of video surveillance are such as to prevent the full-fledged application of the measures and arrangements laid down in this decision because of the nature of the data and/or the mechanisms of the processing and/or the effects the latter may produce.

3.2.2. Cases Where No Prior Checking Is Required

No prior checking application shall have to be lodged by the controller of processing operations performed via video surveillance if all the conditions below are fulfilled:

a. The Italian DPA has already issued a prior checking decision in respect of specific categories of processing and/or data controller;

b. The factual circumstances, the purposes of the processing, the type and implementing arrangements of the system to be deployed, and the categories of data controller are in line with those approved via the said prior checking decision;

c. The measures and arrangements set forth in the decision mentioned under point a. above are complied with in full.

It shall be understood that the standard operation of a video surveillance system that does not fall under any of the cases mentioned in point 3.2.1. does not require prior checking by the DPA - on condition the processing in question is performed in line with the guidance provided herein.

It shall also be understood that mere fact of sending the Italian DPA documents relating to planned video surveillance applications - which are often vaguely worded and cannot be assessed remotely - may not be construed as tacit approval if no reply is explicitly provided by the DPA, since the silent assent principle is not applicable.

3.2.3. Notification

As a general rule, a processing operation is only to be notified to the Italian DPA in the cases specifically referred to in Section 37 of the DP Code. Under Section 37(1)f. thereof, this DPA has already provided that processing operations performed exclusively for purposes of security and/or the protection of individuals or property do not have to be notified, even though they relate to unlawful and/or fraudulent conduct, where the sound/or image data collected are only stored temporarily. For the remainder, any processing operation that is performed by means of video surveillance systems and falls within the

scope of the provisions contained in Section 37 of the DP Code must be notified beforehand to the Italian DPA.

Failure to submit a notification or the provision of an incomplete notification as per Sections 37 and 38 of the DP Code are punished by the administrative sanction referred to in Section 163.

3.3. Security Measures Applying to Personal Data That Is Processed by Means of Video Surveillance and Entities in Charge of Their Application

3.3.1. Security Measures

Any data that is collected via video surveillance must be protected through suitable security measures that should minimize the risk of their destruction or loss - whether by accident or not -, unauthorized access to the data or of processing operations that are either unlawful or inconsistent with the purposes for which the data have been collected also with regard to transmission of the images (see section 31 et seq. of the DP Code).

Accordingly, specific technical and organisational measures should be implemented to enable the data controller to check the tasks discharged by those accessing the images and/or controlling the surveillance systems - where the latter individuals are other than the data controller and the data controller is a natural person.

Minimum security measures are bound to vary, also to a significant extent, by having regard to the wide-ranging gamut of use of video surveillance as well as to the different entities relying on this type of surveillance for the most diverse purposes and by means of widely diverging technological systems.

However, the said security measures must comply at least with the following principles:

a. If different competences are allocated specifically to the individual operators, a tiered system of image visibility and processing should be deployed (see point 3.3.2.). Where this is technically feasible by having regard to the features of the individual systems, the said operators - who must be appointed as persons in charge of the processing or else as data processors, where applicable - must be equipped with authentication credentials enabling them to only discharge the tasks allocated to them based on the respective competences;

b. If the video surveillance system is configured to record and then store the filmed images, appropriate limitations should be introduced on the operators' capability to view the recorded images not only at the time they are filmed, but also thereafter and to cancel and/or duplicate those images;

c. As for the retention period of the images, technical or organizational measures should be envisaged to erase the recorded images, also automatically, upon expiry of the relevant period (see point 3.4.);

d. If maintenance actions have to be undertaken, specific precautions are necessary; in particular, the entities in charge of the said maintenance may only access the images if this proves indispensable to perform technical checks and in the presence of operators with authentication credentials that enable them to view those images;

e. If digital cameras are used and connected with an IT network, such cameras must be protected against unauthorised access as per section 615-ter of the Criminal Code;

f. The transmission of video surveillance images via a public communications network may only occur if the said images are encrypted so as to ensure their confidentiality; this also applies to the transmission of images from surveillance points using wireless technology (wi-fi, wi-max, Gprs).

3.3.2. Data Processors, Persons in Charge of the Processing

The data controller or - if appropriate - the data processor should appoint, in writing, all the natural persons in charge for the processing, whether they are authorised to access the premises where surveillance equipment is deployed, to use such equipment or else - if this is indispensable for the specific purposes - to view the images (see Section 30 of the DP Code). A finite number of persons should be appointed, especially if external collaborators are relied upon. Additionally, different access levels should be introduced depending on the tasks specifically allocated to the individual operators; a distinction should be drawn between those only enabled to view the images and those empowered to perform additional operations under specific conditions - such as recording, copying, erasing the images, changing the visual angle and/or zooming settings, etc. (see point 3.3.1.).

The standard rules should be complied with as also related to the appointment of data processors, if any (see section 29 of the DP Code).

Failure to comply with the requirements set forth in letters a. to f. of point 3.3.1. entails imposition of the administrative sanctions referred to in section 162(2-ter) of the DP Code.

Failure to implement the minimum security measures entails imposition of the administrative sanctions referred to in section 162(2-bis) of the DP Code as well as representing a criminal offence under section 169 thereof.

3.4. Retention Period

Where the system in use also stores the images collected, the proportionality principle set forth in section 11(1) of the DP Code requires the provisional retention of this data to be commensurate with the time that is required - as determined beforehand - to achieve the specific purpose(s).

The images should not be retained for longer than a few hours up to a maximum of 24 hours - subject to special requirements whereby the images are to be retained for longer because of festivities and/or the closing of offices and/or shops or else following specific requests by investigating judicial (police) authorities. Only in some cases may one allow for a longer retention period because of specific technical requirements (e.g. transportation means) or else due to the high-risk activities performed by the data controller (e.g. in the case of banks, where one may justifiably need to identify the individuals who have reconnoitred the premises a few days in advance of a bank robbery); however, the period in question should never be longer than one week, by having also regard to the maximum retention period set forth by law in respect of other processing operations.

As regards municipalities, the images may not be retained for longer than "the seven days following collection of the information and images via video surveillance, subject to specific requirements". This is based on recent regulatory provisions, and only applies to the use of video surveillance for protecting urban security.

Whenever the retention period is to be extended to over one week, a request to that effect will have to be lodged with the Italian DPA for a prior checking decision (see 3.2.1.); at all events, such extension should be assumed by the data controller to be exceptional and must comply with the proportionality principle. The appropriateness of a longer retention period must be accounted for adequately by referring to the specific security requirements to be met and by having regard to factual risk circumstances that have to do with impending events and only relate to the time span in which such exceptional requirements obtain. The appropriateness in the given case might also depend on the need to comply with a specific request to keep and/or deliver a copy as made specifically by judicial/police authorities in respect of ongoing investigations.

The system deployed should be configured in such a way as to automatically erase all the information from all media upon expiry of the pre-determined deadline; the relevant arrangements should be such as to prevent re-use of the erased information and may also consist in overdubbing. If non-digital technologies are used and/or if the data processing capability of the system in question does not allow implementing automatic expiring mechanisms for the recorded data, the images will have to be erased as quickly as possible following expiry of the retention period set by the data controller.

Failure to comply with the retention periods applying to the images collected as well as with the related obligation to erase such images entails imposition of the administrative sanction set forth in Section 162(2-ter) of the DP Code.

3.5. Data Subjects' Rights

Any identifiable data subject must be enabled to actually exercise their own rights in pursuance of the DP Code, in particular the right to access the data concerning them, check the purposes of the processing as well as the relevant arrangements and the underlying logic (see Section 7 of the DP Code).

In replying to a request for access to the stored data, one should cover all the data related to the identifiable petitioner and may include data related to third parties only under the terms set forth in the DP Code - i.e. exclusively if separating the relevant data and/or eliminating certain items from the processed data makes the personal information related to the data subject no longer understandable (see Section 10(5) of the DP Code).

As regards the recorded images, it is factually impossible to exercise the right to have data updated, rectified and/or supplemented on account of the very nature of the data in question - which are real-time images of factual occurrences (see Section 7(3)a. of the DP Code). Conversely, any data subject has the right to have the data blocked if such data is processed in breach of the law (see Section 7(3)b. of the DP Code).

4. SPECIFIC SECTORS

4.1. Employment Relationships

The prohibition against monitoring of employees' activities at the workplace should be complied with; accordingly, it is forbidden to deploy equipment that is specifically intended for the above purposes. No surveillance should take place in order to check compliance with the duties applying to working hours and appropriate discharge of workplace tasks - e.g. by tilting cameras to film employees' badges. Additionally, occupational safeguards should be abided by if video surveillance proves necessary because of organizational and/or production requirements or else for occupational safety purposes; under section 4 of Act no. 300/1970, any devices and equipment "that may give rise to the mere possibility of remotely monitoring employees' activities may only be installed in agreement with the trade union representatives in the given business or, failing these, with the internal labour committee. Failing such agreement, the Labour Inspectorate shall step in at the employer's request and lay down, where necessary, the arrangements applying to use of the said devices and equipment." (see also sections 113 and 114 of the DP Code; section 8 of Act no. 300/1970; section 2 of legislative decree no. 165/2001).

The above safeguards should be respected both indoors and in any other workplace environment - e.g. in building yards, or as regards the cameras installed onboard passenger vehicles (see sections 82 and 85-87 of legislative decree no. 285 dated 30 April 1992 - "New Road Traffic Act") or taxi cabs. Those cameras should not film the drivers continuously, and any images collected to ensure security and counter criminal offences may not be used to check - albeit indirectly - the relevant employees' activities (see point 4.4. above).

Failure to comply with the above requirements results into imposition of the administrative sanction set forth in section 162(2-ter) of the DP Code.

Using video surveillance systems to purposely monitor employees remotely and/or investigate employees' opinions is a criminal offence under the terms of section 171 of the DP Code.

On a different note, the case of TV cameras filming workplaces and employees to document activities and/or operations exclusively in order to provide information to the general public and/or in connection with institutional and/or corporate communication initiatives may be equated to a transitional processing operation for the purpose of the occasional publication of articles, papers and other intellectual works. Accordingly, the provisions on journalistic activities contained in the DP Code (under section 136 et seq.) are applicable - without prejudice to the limitations placed on press freedom to ensure confidentiality, the need for complying with the code of conduct related to journalistic activities, and employees' right to protect their own images by objecting, on legitimate grounds, to dissemination of such images (see section 7(4)a. of the DP Code).

4.2. Hospitals and Treatment Centres

Surveillance in health care premises as well as the monitoring of patients that have been admitted to specific departments and/or areas (e.g. resuscitation units, medical isolation divisions) should only be implemented if it proves indispensable on account of specific treatment and health care requirements applying to the data subjects - taking account of the sensitive nature of many items of information that may be collected in this manner.

Furthermore, all the additional precautions should be taken that are necessary to ensure a high level of protection of patients' privacy and dignity - partly in pursuance of the requirements laid down in the DPA's decision dated 9 November 2005 under the terms of section 83 of the DP Code.

The data controller should make sure that only specifically authorised staff may access the images recorded for the above purposes - e.g. medical and/or nursing staff. Special attention should be paid to the arrangements whereby authorised third parties may access the video records; this applies to relatives, family members, and acquaintances/friends of patients hospitalised in divisions the said third parties are not allowed to access in person (e.g. resuscitation units). In that case, they should be enabled to only view the respective relatives/friends by means of the appropriate technical arrangements.

Images suitable for disclosing health may not be disseminated (as per section 22(8) of the DP Code); on no account should images of patients be displayed on monitors located in publicly accessible premises.

Failure to comply with the above requirements results into imposition of the administrative sanction set forth in section 162(2-ter) of the DP Code.

Dissemination of images in breach of section 22(8) of the DP Code is a criminal offence under the terms of 167(2) thereof as well as resulting into imposition of the administrative sanction referred to in section 162(2-bis).

4.3. Schools

The deployment of video surveillance systems in schools should ensure "the student's right to privacy" as per section 2(2) of Presidential decree no. 249/1998; the appropriate precautions should be taken to ensure the balanced development of a child's personality by having regard to their lives, growth and right to education.

4.3.1. In this connection, it may be admissible to use video surveillance systems if they prove absolutely indispensable to protect premises and property against vandalism; the cameras should only film the areas concerned and operate when the school is closed. Furthermore, it is forbidden to operate video cameras on the occasion of extracurricular activities performed within school premises.

4.3.2. Where the images also include neighbouring areas, the visual angle of the cameras should only capture the areas concerned without extending the surveillance to premises that do not pertain closely to the school building(s).

4.3.3. Failure to comply with the above requirements results into imposition of the administrative sanction referred to in section 162(2-ter) of the DP Code.

4.4. Public Transportation Safety

4.4.1. In the presence of especially risky situations, the installation of video surveillance systems may be found lawful both on board public transport vehicles and at/close to the respective stops.

4.4.2. The cameras should be located and the filming arranged in such a way as to comply with the aforementioned principles of data minimization, proportionality and purpose specification; accordingly, no detailed filming will be permitted if this is not indispensable for the specific purposes.

4.4.3. Data controllers will have to provide the necessary information notices to the users of public transportation facilities. Coaches, trolleys, cabs and

leased cars with and without drivers will have to bear specific notices and/or signs, if equipped with video cameras, to quickly alert to the presence of video surveillance devices. To that end, the facsimile notice in Attachment 1 hereto may also be used, whereby the data controller's name and the purposes of the processing have to always be included.

4.4.4. Specific precautions should be taken if video surveillance systems are deployed close to stops, where passers-by may happen to be filmed. In particular, the visual angle of the filming devices must be limited to the waiting area of the given stop so that only the stop shelter and any other appurtenances that are functional to the public transportation service - such as timetables, poles, bus flags etc. - are filmed; the neighbouring area and anyhow any area that is not directly related to the security requirements applying to the public transportation system should not be included in the visual angle of surveillance. Again, uselessly detailed shots and/or excessively detailed filming of the individuals waiting at the given stop should be avoided. Presence of the cameras must be notified appropriately at each stop.

4.4.5. Whilst any violation of the provisions concerning information notices as per Section 13 of the DP Code carries the administrative sanction referred to in section 161 of the DP Code, and the use of video surveillance systems that are intended to monitor employees remotely is a criminal offence as per Section 171 thereof, failure to comply with the requirements laid down in paragraph 4.4.4. results into imposition of the administrative sanction set forth in section 162(2-ter) of the DP Code.

4.5. Use of Web Cams and/or Online Cameras for Promotional, Tourism and/or Advertising Purposes

The filming of activities for promotional, tourism and/or advertising purposes based on the use of web cams should only be carried out in such a way as not to allow the filmed individuals to be identifiable. This is related to the peculiar processing mechanisms, which entail the tangible risk of causing substantial harm to data subjects: indeed, the images collected via these systems are posted directly on the Internet, which enables any surfer to view them in real time and use them also for purposes that have nothing to do with the promotional, tourism and/or advertising objectives pursued by the data controller.

4.6. Integrated Video Surveillance

Pursuant to the cost-effectiveness principle as for the use of the available resources and tools, integrated video surveillance systems have been increasingly deployed via public-private partnerships whilst centralised remote video surveillance systems have become increasingly available via surveillance companies, Internet service providers, professional video service providers, etc. . Furthermore, the images collected in this manner are sometimes made available to law enforcement authorities (police) by means of different technologies and/or arrangements.

The following categories of integrated video surveillance can be distinguished in this context:

a. Co-ordinated management of functions and services via partial/total sharing of the images collected by separate data controllers, who use the same technological facilities. In this case, the individual data controllers may only process the images to the extent this is necessary to discharge their

own institutional tasks and achieve the purposes specified unambiguously in the relevant information notices - if they are public bodies; as for private bodies, the processing should only serve the purposes specified in the information notices;

b. Establishment of electronic connections between various data controllers and a single "central" unit managed by a third party: the latter third party must be appointed as data processor by each data controller in pursuance of section 29 of the DP Code and should work as a co-ordination and management unit of the video surveillance without allowing for any matching of the images collected on behalf of the individual data controllers;

c. Both in the above cases and whenever video surveillance is performed by a single data controller, the video surveillance system may be connected with operation rooms and/or stations of law enforcement authorities (police). Implementation of the connection at issue must be disclosed to data subjects; to that end, this DPA considers that the simplified "minimal" information notice may be used as per section 13(3) of the DP Code (see Annex 2 to this decision), referring to the data controller, the relevant purpose(s) and the existence of a link with the police. Existence of the connection should also be notified within the framework of the detailed information notice that is made available to data subjects (see 3.1.3.).

The above processing arrangements require specific security measures to be in place in addition to those referred to under point 3.3.1. - such as the following:

1. Implementation of systems to log accesses of the persons in charge and the operations performed with regard to the recorded images, including the respective time stamps; the logs will have to be kept for as long as is appropriate in order to enable the data controller to fulfil the obligation of regularly checking the data processor's performance, and in any case they should be kept for at least six months;

2. Logical separation of the images recorded by the individual data controllers.

Failure to comply with the measures mentioned under points 1. and 2. above entails imposition of the administrative sanction set forth in section 162(2-ter) of the DP Code.

Except for the above cases, if the processing performed by means of integrated video surveillance systems is such as to prevent the full-fledged application of the aforementioned measures and precautions because of the nature of the data and/or the arrangements applying to the processing and/or the effects produced by the latter, the data controller is required to lodge a prior checking application with the Italian DPA (see point 3.2.1.).

5. PUBLIC BODIES

Public bodies acting in their capacity as data controllers (section 4(1)f. of the DP code) may process personal data in compliance with the purpose specification principle to pursue specific, explicit and legitimate purposes (see section 11(1)b. of the DP Code) insofar the processing is aimed at the discharge of their own institutional tasks. This also applies to the collection of images by means of video surveillance (see section 18(2) of the DP Code).

Public bodies are required to respect the principles laid down in this decision just like any other controller of processing operations performed by means of video surveillance.

Public bodies are required to inform data subjects beforehand (under section 13 of the DP Code), subject to the conditions referred to in paragraph 3.1.1. . Accordingly, whoever enters or happens to pass by premises where video surveillance is operating must be informed beforehand about the processing of their personal data. To that end, public bodies may use the simplified "minimal" information notice shown as a fac-simile in Annex 1 hereto (see point 3.1.).

5.1. Urban Security

Recent legislation on security has empowered mayors to carry out surveillance activities and take the measures they are competent for in accordance with the law and regulations on ordre public and public security as well as to discharge the tasks they have been entrusted with by the law on security and judicial police. In order to prevent and counter certain dangers affecting public safety and urban security, the mayor may also take urgent, extraordinary measures in compliance with the general principles of our legal system. Finally, mayors contribute to ensuring co-operation of the local police with the State police in their capacity as governmental officials, within the framework of the co-ordination guidelines issued by the Ministry for Home Affairs.

Based on the above premises, it appears that specific competences have been allocated both to mayors in their capacity as governmental officials and to municipalities; from this standpoint, the said entities may deploy video surveillance systems in premises that are public or open to the public with a view to protecting urban security.

It is not up to this DPA to define "urban security" and set the operational scope of this type of security vis-à-vis ordre public; however, it shall be understood that section 53 of the DP Code applies if the video surveillance activities can be equated to protecting public security and/or preventing, detecting or suppressing criminal offences (see paragraph 3.1.1.).

At all events, it would be highly desirable - as already pointed out - that an information notice be provided in all the cases mentioned above even though it is not mandatory; this is especially appropriate if the municipalities plan to inform their citizens on the adoption of measures and arrangements such as the deployment of video surveillance systems that are aimed at keeping the local area under control and ensuring the protection of individuals.

5.2. Waste Disposal

Pursuant to the aforementioned principles of lawfulness, purpose specification, and proportionality, video surveillance may be lawfully used to check on the unauthorised use/misuse of dumping sites for hazardous waste and materials only if the use of alternative control systems and mechanisms proves impossible or ineffective.

By the same token, video surveillance systems may be lawfully used if other measures prove ineffective and/or unfeasible to monitor compliance with the regulations on mechanisms, type and time schedule of waste disposal; administrative sanctions are applicable in case such regulations are violated (see section 13 of Act no. 689 dated 24 November 1981).

5.3. Use of Electronic Devices to Detect Traffic Violations

Electronic systems automatically detecting traffic violations are used to provide proof of such violations; like video surveillance, they entail the processing of personal data.

5.3.1. Accordingly, these systems may be used lawfully if only such data as is relevant and non-excessive is collected to pursue the data controller's institutional purposes; to that end, the location and filming angle of the cameras will have to be such as not to collect irrelevant and/or excessively detailed images. Pursuant to existing practices and the sector-specific legislation in respect of certain traffic violations, the following requirements should be met:

a. The alphanumerical data contained in licence plates will have to be retained exclusively in the presence of a traffic violation;

b. Pictures and/or video shots may only show the items referred to in the specific regulations with a view to drafting the relevant violation notice (e.g., pursuant to section 383 of Presidential decree no. 495/1992, type of vehicle, day, time and place of the violation); the vehicle should be shown in such a way as not to include - or to blank, if this is feasible - any items that have to do with individuals who are not concerned by the administrative proceeding (e.g. passers-by, other drivers);

c. Pictures and/or video shots may only be used to establish traffic violations including the notification thereof, subject to their being made available to any entity entitled thereto;

d. Images should be kept for no longer than necessary with a view to the notification of the traffic violation, the possible imposition of sanctions, and the settlement of any disputes arising therefrom pursuant to the applicable legislation; this is without prejudice to the need for retaining the images longer because of specific investigation-related requests made by judicial authorities and/or the judicial police;

e. Any pictures and/or images to be used as evidence of the notified violation(s) should not be sent to the vehicle owner's home address jointly with the violation notice(s), subject to their being made available to any entity entitled thereto;

f. In the light of the vehicle owner's legitimate interest in checking who committed the relevant traffic violation and accordingly obtaining all the information useful for this purpose from the competent authority, inspection of the video and photographic records should be permitted at the owner's request; when the records are accessed, any passengers on board the vehicle will have to be blanked and/or blurred as appropriate.

Failure to comply with the above requirements (letters a. to f.) entails imposition of the administrative sanction set forth in section 162(2-ter) of the DP Code.

5.3.2. All the drivers and individuals that access and/or pass by areas where electronic systems operate to automatically detect traffic violations should also be informed beforehand as for the processing of their personal data (see section 13 of the DP Code).

Specific regulatory provisions in force already refer to cases in which public bodies are required to provide specific information to users regarding the use of electronic devices - e.g. in case speed limit violations are detected remotely.

The ultimate objective consists in ensuring that data subjects are informed effectively, and this can be achieved in different ways by the entities in charge of collecting the images.

To provide information appropriately, one should first and foremost rely on the appropriate tools to clearly signify that image collection devices are present in the relevant area. To that end, one can effectively make use of awareness-raising tools and initiatives, also on a regular basis, such as web sites and press releases; to this one might add other measures such as the handing out of information leaflets, the deployment of electronic message boards, announcements broadcast on radio and TVs, dissemination of information via community networks and other institutional communication networks, etc. .

Additionally, one might also rely in this context on ad-hoc posters and signs. To that end, the simplified model of "minimal" information notice can be used that is shown in the Annex hereto, whenever road traffic legislation does not explicitly require that users be informed of the presence of electronic devices that can automatically detect traffic violations.

As already pointed out, the sector-specific legislation provides explicitly in some cases - e.g. remote surveillance of compliance with speed limits or no-overtake signs - that users be notified of the deployment of electronic devices that can automatically detect traffic violations. Therefore, in such cases one can dispense with providing an additional, separate data processing information notice that contains information already known to data subjects because of the signposting obligation laid down in the relevant road traffic legislation (see section 13(2) of the DP Code). The deployment of such ad-hoc signs and notices pursuant to the Road Traffic Act already enables data subjects to become apprised of various essential items in respect of the processing of their personal data. Accordingly, the signs that draw attention adequately to the operation of electronic devices that can automatically detect traffic violations can be considered to suitably fulfil the information obligation referred to in section 13 of the DP Code.

Finally, the obligation to provide the above information can be considered to be also fulfilled if the data controller signifies the automated detection of traffic violations by means of notices and signs similar to those provided for under the Road Traffic Act - even in the absence of a specific legal obligation to do so.

Any breach of the provisions on information notices as per Section 13 of the DP Code carries the administrative sanction referred to in Section 161 of the DP Code.

5.3.3. If access surveillance systems are deployed by municipalities to monitor access to town centres and restricted traffic areas, the provisions laid down in Presidential decree no. 250 dated 22 June 1999 will have to be complied with. The latter decree requires the processed data to be retained for no longer than necessary in order to challenge the fine and settle the relevant dispute, whilst the data in question may be made available to the judicial police and/or criminal investigators (see section 3 of decree no. 250/1999).

5.4. Additional Precautions Applying to Video Surveillance Systems Deployed by Public Bodies, in particular by Local Authorities

Local authorities and, generally speaking, public bodies operating at local level also rely on integrated video surveillance by joining a shared surveillance system in order to reduce the expenditure and resources required to discharge diverse institutional tasks.

In paragraph 4.6. above, several specific safeguards have already been referred to in order to ensure that the processing is performed appropriately; they should be taken into account in this context as well with particular regard to the surveillance performed by local municipalities as also related to the provisions regulating video surveillance by municipalities.

More specifically,

a. The shared use, in whole or in part, of video surveillance systems via the same technological facilities should be configured in such a way as to enable the individual bodies - if appropriate, the individual organisational departments within each body - to only access the images to the extent this is absolutely necessary to discharge the respective institutional tasks. Data subjects should not be tracked and their routes should not be pieced together as for the areas that fall outside the individual body's/organisation's geographical competence;

b. Where a single "centre" handles video surveillance activities on behalf of various public bodies, any personal data that is collected will have to be processed by having regard to the institutional functions vested in the individual public administrative bodies.

The data controller is required to lodge a request for prior checking with this DPA if neither of the above conditions is applicable as well as whenever the processing performed by way of integrated video surveillance systems is such - on account of its nature and features - as to prevent full application of the aforementioned measures and precautions; account will be taken in this regard of the nature of the data and/or the processing arrangements, the effects possibly produced by the processing, and - in particular - of the circumstance that prior checking is mandatory in respect of the given system as per paragraph 3.2.1. above - e.g. in the case of image collection associated with biometrics information, or if so-called smart systems are used, i.e. systems that can automatically detect deviant/abnormal conduct and/or events, report them and, if appropriate, record the data.

6. PRIVATE BODIES AND PROFIT-SEEKING PUBLIC BODIES

6.1. Personal Data Processed for Exclusively Personal Purposes

Based on the considerable number of applications lodged with this DPA, it appears that video surveillance systems are often deployed by natural persons for exclusively personal purposes. In these cases one should clarify that the DP Code does not apply if the data are not communicated to third parties on a regular basis and/or are not disseminated; still, it is necessary to take measures to protect third parties' personal data pursuant to section 5(3) of the DP Code, which leaves third party liability and data security requirements unprejudiced. Such cases include, for instance, the deployment of video surveillance devices capable to identify any individual that is about to enter privately-owned premises (e.g. video door entry systems and any device collecting images and/or sound data also by way of their recording) as well as video surveillance systems installed close to private premises and within jointly-owned properties (condos) including the respective appurtenances (e.g. parking areas).

Even though the DP Code does not apply, the cameras should be angled in such a way as to only display the areas owned directly by the individual person in order not to commit the offence of unlawful interference with private life (under section 615-bis of the Criminal Code); this means that the area close to the entrance to one's flat/home may be filmed, whilst no surveillance is admissible - whether with or without recording - of areas such as courtyards, landings, staircases, jointly owned parking places or the areas close to the entrance to other tenants' flats/homes.

6.2. Personal Data Processed for Non-Exclusively Personal Purposes

6.2.1. Consent

If the DP Code is applicable, the data may only be processed lawfully by private bodies and profit-seeking public bodies with the data subject's prior consent; alternatively, any of the other preconditions for lawful data processing must be fulfilled (see sections 23 and 24 of the DP Code).

Obtaining the data subjects' consent when video surveillance is involved can actually prove difficult because of the features of these systems, which accordingly makes it necessary to select a suitable alternative to consent out of the equivalent preconditions mentioned in section 24(1) of the DP Code.

6.2.2. Balancing of Interests

The said alternative can be found in the balancing of interests mechanism (see section 24(1)g. of the DP Code). This decision implements the latter mechanism by setting forth the cases in which images may be collected without the data subjects' consent providing this is aimed at pursuing legitimate interests vested either in the data controller or in a third party by obtaining items of evidence - in accordance with the arrangements laid down in this decision - or else with a view to protecting individuals and property against possible attacks, theft, robberies, damage, or vandalism, or else for the purpose of fire prevention and/or occupational safety.

To that end, the following cases can be referred to as those in which the processing may be performed lawfully in the absence of the data subjects' consent by complying with the requirements below.

6.2.2.1. Video Surveillance (with or without recording of the images)

This type of processing is only permitted in the presence of specific situations justifying installation of video surveillance to protect individuals, property and/or corporate assets.

As for the use of any equipment intended for filming, with or without recording of the images, areas outside buildings such as parking places, loading/unloading areas, accesses, emergency exits, etc., it should be recalled that the processing must be such as to limit the visual angle to the area(s) to be protected; this means that the neighbouring areas and any irrelevant items (streets, buildings, shops, institutions) may not be filmed.

6.2.2.2. Video Surveillance in Condos

If the processing in question is performed by a condo - also by the agency of the respective manager - one should recall that the Italian DPA recently drew Parliament's and the Government's attention to this issue, in particular because of the lack of specific regulations that can shed light on a few implementing problems surfaced over the past few years. Indeed, it is unclear whether video surveillance systems may be installed at the request of the joint owners or whether the tenants' views are also to be taken into account. Nor is it clear how many votes are required for the condo to take the relevant decisions - i.e. whether unanimity is necessary or a specific majority vote is sufficient.

7. REQUIREMENTS TO BE MET AND SANCTIONS

All the controllers of personal data processing operations performed by means of video surveillance systems are hereby called upon to comply with the requirements laid down herein.

The necessary measures set forth herein must be complied with by all data controllers. If this were not the case, the processing may prove unlawful or unfair - depending on the specific circumstances. The consequences can be the following:

- The personal data processed in breach of the applicable provisions may not be used (section 11(2) of the DP Code);
- The DPA may order the processing to be blocked or ban the processing as such (section 143(1)c. of the DP Code), and similar decisions may be issued by civil and/or criminal judicial authorities;
- The applicable administrative and criminal sanctions may be imposed (section 161 et seq. of the DP Code).

NOW, THEREFORE, BASED ON THE ABOVE PREMISES,
THE ITALIAN DATA PROTECTION AUTHORITY

1. Under section 154(1)c. of the DP Code, orders the controllers of personal data processing operations performed by means of video surveillance to take the measures and precautions referred to in the premises hereof as shortly as possible, anyhow by no later than the deadlines specifically mentioned in the individual cases as calculated from the date on which this decision is published in Italy's Official Journal. The said measures and precautions are recalled hereinafter:

a. Visible information notices must be displayed within twelve months, irrespective of whether the video surveillance system operates at night time (paragraph 3.1.);

b. A prior checking application must be lodged within six months in respect of any processing operation that entails specific risks to data subjects' rights and fundamental freedoms as per section 17 of the DP Code (paragraph 3.2.1.):

c. Security measures must be implemented within twelve months to protect the data recorded via video surveillance systems (paragraph 3.3.);

d. The measures required to ensure compliance with the provisions set forth in paragraphs 4.6. and 5.4. as for integrated video surveillance systems must be implemented within six months;

2. Under section 24(1)g. of the DP Code, specifies the cases in which personal data may be processed via video surveillance by private bodies and profit-seeking public bodies according to the terms and conditions referred to in order to pursue legitimate interests and without the data subjects' consent (paragraph 6.2.2.);

3. Determines that a simplified model information notice to be used under the terms set forth in the premises is the one contained in Annex 1 hereto, pursuant to section 13(3) of the DP Code (paragraph 3.1.);

4. Determines that a simplified model information notice to be used under the terms set forth in the premises for informing data subjects that a video surveillance system is connected with law enforcement authorities is the one contained in Annex 2 hereto, pursuant to section 13(3) of the DP Code (paragraphs 3.1.3. and 4.6. letter c.);

5. Recalls that it is advisable to provide an information notice when discharging the tasks mentioned in section 53 of the DP Code even though such notice is not mandatory, providing this is not factually in conflict with specific requirements related to ordre public and/or the prevention, detection or suppression of criminal offences (paragraph 5.1.);

6. Orders that a copy of this decision be sent to the Ministry of Justice - Ufficio pubblicazione leggi e decreti in pursuance of section 143(2) of the DP Code in order for it to be published in Italy's Official Journal.

Done in Rome, this 8th day of the month of April 2010

ANNEX 1

Instructions on use can be found in paragraph 3.1.

If the images are not recorded, replace "recording" [registrazione] by "collection" [rilevazione]

ANNEX 2

Instructions on use can be found in paragraphs 3.1.3. and 4.6. letter c.

If the images are not recorded, replace "recording" [registrazione] by "collection" [rilevazione]

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Garante per la protezione dei dati personali
Piazza di Monte Citorio, 121
00186 Roma
Phone: +39-06 696771 - fax: +39-06 696773785
www.garanteprivacy.it

Contact:
Ufficio per le relazioni
con il pubblico (Front Desk)
Mon-Fri 10-13
Email: urp@garanteprivacy.it

**Edited by Servizio relazioni
con i mezzi di informazione
(Media and Communications Service)
at the Garante per la protezione
dei dati personali**

October 2010

Designed by: Vertigo Design