



AGENCIA
ESPAÑOLA DE
PROTECCIÓN
DE DATOS



Video surveillance GUIDE ON

© AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS
(SPANISH DATA PROTECTION AGENCY)
Official Publications Identification Number: 052-08-007-8

Graphic Design: 

Printed by: NILO Industria Gráfica, S.A.



Video surveillance

GUIDE ON

Guide on Video surveillance

contents

4	INTRODUCTION
6	WHEN SHOULD DATA PROTECTION RULES BE APPLIED TO IMAGE PROCESSING?
8	HOW THE IMAGES SHOULD BE PROCESSED
10	IMAGE CAPTURING AND PROCESSING FOR SECURITY PURPOSES
10	OBLIGATIONS
10	FILE REGISTRATION
11	DUTY TO INFORM
13	THIRD PARTY DATA ACCESS CONTRACT
16	SECURITY MEASURES
17	DUTY TO CANCEL IMAGES
17	SECURITY FIRMS
19	SPECIFIC CIRCUMSTANCES
19	ACCESS TO BUILDINGS AND GAMES ROOMS
21	FINANCE INSTITUTIONS
22	CAMERAS WITH ACCESS TO THE PUBLIC THOROUGHFARE
24	CAMERAS CONNECTED TO THE INTERNET
25	SCHOOLS AND ENVIRONMENTS WITH MINORS
27	PUBLIC SPACES OF PRIVATE USE
28	TAXIS
28	OTHER SECURITY-RELATED USES
28	VIDEO CAMERAS OF THE NATIONAL SECURITY FORCES
31	VIDEO CAMERAS FOR TRAFFIC CONTROL PURPOSES
33	SPORTING EVENTS
34	USE OF VIDEO CAMERAS WITH BUSINESS CONTROL PURPOSES
37	OTHER PROCESSING ARRANGEMENTS
37	PROCESSING IN SCHOOL ENVIRONMENTS FOR NON-SECURITY PURPOSES
38	VIDEO INTERCOM SERVICES
39	SCIENTIFIC RESEARCH AND RELATED USES
39	TOURISM PROMOTION AND RELATED PURPOSES
39	GENERAL RULES
41	PERSONAL RIGHTS
42	GUIDELINES
44	FAQS

INTRODUCTION

Image capturing and/or processing for surveillance purposes is a very widespread practice in our society. Video surveillance generally seeks to safeguard the security of property and persons or is used in business settings to check on worker compliance with their occupational duties and obligations. Both purposes are valuable pursuits worth legal protection but subject to compliance with certain conditions. The use of technical resources for surveillance purposes impinges on the rights of persons, and this means that some guarantees need to be set beforehand.

Video surveillance enables personal information to be captured and sometimes recorded in the form of images. When its use affects identified or identifiable persons, this information is then deemed to be personal data for enforcement purposes of the Spanish Personal Data Protection Act dated 13th of December 1999 (Ley Orgánica de protección de los datos de carácter personal: LOPD for short).

Application of the LOPD to these systems poses a certain degree of difficulty in all aspects. First of all, the controller must be able to identify whether or not the use of the video cameras is subject to the legislation in force. Secondly, it is a complex matter to inform the data subject and do so with understandable, uniform and easily identifiable criteria.

Nonetheless, unlike the video surveillance carried out by the National Security Forces, which is regulated by special legislation, the only existing regulation in the private sector, the Private Security Act 23/1992 of the 30th of July lays down no precise data-protection indications. Therefore, it stands to reason, as reflected by various judgements of the Constitutional Court, that video surveillance is a particularly invasive measure and, hence, it is necessary to concurrently satisfy certain eligibility conditions in order to legally justify its processing. In addition, it is also necessary to define the principles and safeguards that must be applied.

For all these reasons, and to bring this processing into line with the LOPD, the Spanish Data Protection Agency passed Instruction 1/2006 of the 8th of November on the processing of personal data for surveillance purposes using video systems or video cameras

However, together with video surveillance for security or workforce monitoring purposes, other new uses and services have also cropped up based on capturing and processing images recorded by video cameras or webcams. In the cases where these images belong to identified or identifiable persons, the LOPD is applicable.

The Guide will try to provide practical criteria and directions to ensure appropriate compliance with the current legislation in all cases.

WHEN SHOULD DATA PROTECTION RULES BE APPLIED TO IMAGE PROCESSING

The concept of personal data includes images when they refer to identified or identifiable persons. Therefore, personal data protection principles in force should be applied to the use of cameras, video cameras and any other analogous technical resource for capturing and/or recording images, whether for surveillance purposes or for other purposes, under the following circumstances:

- There is recording, capturing, transmission, preservation or storage of the images, including their reproduction or broadcasting in real time or the processing of the personal data derived from these images.
- These activities refer to the data of identified or identifiable persons.

In order to be able to use a system of this nature it is not enough for it to meet the technical requirements that allow it to work. Its use must be legally justifiable. This legitimacy will be attained under the following circumstances:

- The consent of the data subject has been obtained.

E.g. These are still infrequent circumstances. Nonetheless the question has arisen in the case of parental access to crèche images or access to images taken in scientific research.

- A rule with the status of law discharges this consent obligation, as in the cases laid down by the Private Security Act or in Article 20 of the Statute of Workers' Rights.

E.g. Consent for the use of video cameras will not be required for ensuring security of goods and persons, providing they are fitted and maintained by an authorised security firm.

- When any of the circumstances laid down in Article 6.2 LOPD or Article 11.2 LOPD occur, as applicable to resources of this type:

Furthermore, if the current legislation imposes any additional requirement, it will also have to be complied with.

There are also cases in which the LOPD is not applicable:

- It is not applicable to image processing in the personal and domestic sphere, understanding this to be image processing performed by an individual in the context of an exclusively private or family-based activity.

E.g. Data protection principles do not apply to recordings made on a tourism trip or during a family celebration.

- To image processing by the media in exercising their legitimate rights as laid down in Article 20 of the Spanish Constitution.

E.g. The broadcasting of television news or publishing of a newspaper.

Without prejudice to the specific provisions of Act 4/1997 of 4th of August regulating the use of video cameras by National Security Forces in public places, the LOPD is applicable to this processing on a supplementary basis in issues such as the creation of files by a provision of a general nature published in an official journal. This will be looked at later.

HOW THE IMAGES SHOULD BE CAPTURED AND PROCESSED

The use of camera and video camera facilities has to abide by certain rules governing the whole process from the capturing, storage and reproduction up to cancellation of the images. The controller has to take the following principles into account:

- There must be a due proportionality between the end in view and the way the data is processed.

E.g. It would be clearly disproportionate to set up a video camera for watching a garage access and then use its technical characteristics – mobility, orientation, zoom etc. – for the purpose of obtaining images from inside vehicles driving down the public thoroughfare or from local residences.

- The controller must inform data subjects on the image capturing and/or recording.

E.g. Even in cases in which the video cameras are used for legal and legitimate ends, the duty to inform data subjects still exists.

- The use of camera or video camera facilities is admissible only when there is no less invasive alternative.

E.g. It is not necessary to record class students to monitor attendance if a traditional roll call will do.

- Cameras and video cameras set up in private areas shall not obtain images from public areas.

E.g. A video camera used for private security purposes in a building should not capture images from the whole street where it is set up.

- Partial and limited images of public thoroughfares may be taken when this is essential for the surveillance purpose in view or it is impossible to avoid doing so because of the location of the cameras.

E.g. If a camera must necessarily be sited in a bank entrance door or on the corner of a building, it should be angled so that the part of the public thoroughfare it captures is limited to the entrance under surveillance, without recording more of the public thoroughfare than is absolutely necessary. Images may not be taken from the rest of the sidewalk or the street.

- In any case the use of video surveillance system shall always respect personal rights and abide by the rest of the legal system.

E.g. It would not be permissible to capture images in spaces protected by the right to privacy, such as the interiors of nearby dwellings, in bathrooms or dressing rooms or physical spaces outside the sphere specifically protected by the surveillance system.

- The images will be preserved only for the time required for fulfilling the purpose for which they were captured.

E.g. As will be pointed out later in this Guide, Instruction 1/2006 on the preservation of images for surveillance purposes lays down a maximum time of one month. In those instances in which the images are captured for other purposes, the procedure will be subject to specific applicable legislation.

IMAGE CAPTURING AND PROCESSING FOR SECURITY PURPOSES

In this field the principles that have to be abided by and applied are those laid down by the legislation in force, in particular in the LOPD, the Regulation developing the Data Protection Act 15/1999 of 13th of December (Reglamento de Desarrollo de la Ley Orgánica de Protección de Datos de Carácter Personal: RDLOPD for short), approved by Royal Decree (Real Decreto) 1720/2007 of 21st of December and Instruction 1/2006 of 8th of November of the Spanish Data Protection Agency on the processing of personal data for surveillance purposes by means of camera or video camera systems.

This compliance will be dealt with in terms of the various aspects concerned.

■ OBLIGATIONS

FILE REGISTRATION

The use of video camera surveillance systems might give rise to the creation of files. The RDLOPD establishes in which cases a file will be deemed to exist:

File: Any structured set of personal data which are accessible according to specific criteria, depending on its means or method of creation, storage, organisation and access.

E.g. If a system is used connected up to a computer that stores the images on a hard disk or in any other computer support and it enables these images to be located in terms of criteria such as day and/or time of recording, cross-image correlation, the physical site recorded, etc.

If the video surveillance system generates a file, the controller must notify the Spanish Data Protection Agency beforehand, and register the said system with the

Agency's General Register. This shall take place whenever there is any type of recording.

In the case of government files, these have first to be created by means of a provision of a general nature published in the corresponding official journal as laid down in Article 20 LOPD, and, subsequently, they have to be registered.

It should be borne in mind here that the Spanish Data Protection Agency makes the registration procedure easier by means of a predefined form for use with the Online Notification system-

NOTE.

<https://www.agpd.es/portalweb/canalresponsable/index-ides-idphp.php>

There are systems that do not record images and, therefore, Instruction 1/2006 indicates that any processing arrangement consisting exclusively in the real-time reproduction or broadcasting of images will not be considered as a file.

E.g. Closed circuit television controlled by screen display.

It is therefore not necessary to register them. This does not, however, release these systems from complying with the rest of the duties laid down by the LOPD and Instruction 1/2006 as detailed in this Guide.

DUTY TO INFORM

Providing the proper information on any data collection procedure is a key element in the right to data protection and compliance with this requirement is therefore obligatory. However, the special characteristics involved in video surveillance call for the design of specific procedures to inform persons whose images are being captured. Instruction 1/2006 includes an informative sign whose use and display is

mandatory. The sign will be placed at least in the entrances leading onto the areas under surveillance, whether these be indoor or outdoors. If the site under surveillance has many entrances, the sign must be fitted in all of them so that the information may be seen regardless of the entrance used.

The model sign can be obtained from:

https://www.agpd.es/portalweb/canaldocumentacion/legislacion/normativa_estatal/index-ides-idphp.php#video

The file controller must also make available a printed handout with all the information laid down in Article 5 LOPD. This handout will, hence, include information at least on the following:

- The existence of a personal data file or processing arrangement, the purpose behind collecting the data and the recipients of the said the information.
- The possibility of exercising the rights to data access, rectification, cancellation and objection.
- The identity and address of the data processing controller or, as the case may be, the representative.

The handout will have to be available, or at least there must be the possibility of printing it, upon request from the data subject. The information on the handout may also be included on the informative sign, and this sign may replace the handout only in those cases in which its content and location make the information legible and intelligible.

E.g. If the sign is fixed on doors or entrances and is set within the natural field of vision of the data subject, i.e., at eye level.

The use of the sign and information handout does not preclude the existence of additional methods for providing information that may be added to the two former ones such as the publication of a privacy policy on the website, information given to trade union representatives, notifications to local residents, etc.

THIRD PARTY DATA ACCESS CONTRACT

Implementation of video surveillance systems can give rise to the rendering of different types of services. The following services might be outsourced:

- Technical installation and/or maintenance of video surveillance system and equipment without access to the images. In this case the security firm is not considered to be the processor, and the responsibility of adapting the system to the legal requirements falls upon the controller who contracted the said firm. Nonetheless, the firm might also be held liable for any untoward circumstances if it breaches its duties of giving advice as laid down in Article 5 of the Private Security Act (LSP in Spanish initials).

E.g. The mere technical installation of recording equipment and cameras by a security firm acting as authorised installer hired by a residents' association, its tasks being limited to purely technical matters with no image access.

- Installation and/or maintenance of the video surveillance systems and equipment with use of equipment and access to the images. Only in this second case will the security firm be considered to be in charge of processing and hence liable to comply with the obligations laid down in Article 12 LOPD.

E.g. Security firms providing combined services of alarm centre and video surveillance so that, when the alarm is set off, the security firm's personnel directly check the images.

In general, the installation of video surveillance systems for private security purposes necessarily entails hiring the services of a security firm duly authorised by the

Ministry of Home Affairs, which, under article 5 of the Private Security Act 23/1992 of 30 July (Ley de Seguridad Privada), is entitled, inter alia, to provide the following services:

- Surveillance and protection of goods, establishments, shows, exhibitions or conventions.
- Installation and maintenance of security-system devices and appliances.
- Running central offices for receiving, checking and sending alarm signals and communicating them to the National Security Forces, as well as providing response services that are not included within the competencies of the aforementioned National Security Forces.
- Planning and providing advice regarding security activities contemplated by the law.

Hence, whenever images are captured and/or recorded for private security purposes and the hired security firm uses the video cameras and/or its personnel has access to the images, then it is obligatory to enter into a third party data access.

This contract, as regulated by the RDLOPD, has the following main features:

- It is a contract whose content is determined in view of the specific circumstances pertaining to the service arrangement. It is not enough to reproduce the clauses of Article 12 LOPD; the actual services rendered must be reflected, and decisions to ensure compliance with the legislation must be adopted.
- There is a due-diligence duty in terms of checking the processor's eligibility conditions. In terms of video surveillance for private security purposes this means that the controller must check compliance of LOPD terms by the security firm and whether it meets all legal requirements authorising it to provide these services.

- There is no possibility of subcontracting to third parties unless:
 - The processor is empowered to enter into contracts of this type on behalf of the controller.
 - The contract authorises subcontracting with a specific firm or a generic authorisation is given with the proviso of seeking subsequent authorisation by the controller.
 - As well as the capacity of subcontracting in either of the previous two cases, a third party data access contract is entered into by the processor and the subcontractor.
 - Compliance with the controller's Instructions must be guaranteed at all times.
- It is worth recalling that Article 6 of the Private Security Act lays down an additional obligation and the contracts for providing the various security services must, in any case, be set down in writing and communicated to the Ministry of Home Affairs at least three days before the services are rendered for the first time.
- Lastly, we should keep in mind that in cases where the security firm providing the service has no image access rights, due application should be made of the provisions laid down in Article 83 of RDLOPD, whereby the service contract governing the rendering of the service without data access rights shall expressly state the prohibition of accessing personal data and the obligation to observe secrecy with respect to the data that might come to the personnel's knowledge under the service contract.

SECURITY MEASURES

The facility controller shall take all the technical and organisational measures as may be necessary to ensure security of the images and avoid their unauthorised use, therefore, whether it be a company, a residents' association, etc, must comply with the duty of guaranteeing the security of the images in the terms laid down by the LOPD and its development Regulation.

In general, video surveillance files usually have a basic security level. Nonetheless the file controller must assess the security level at all times, bearing in mind provisions of Article 81 of the Regulation in relation to the contents and purpose of the file.

E.g. it might happen that the capturing of images strays beyond the surveillance field and they are used for personnel selection or to verify the response to certain stimuli, in psychology or medicine, and then the security level would be medium or high.

Furthermore, any images made available to a court authority or to the National Security Forces in relation to an offence automatically become data related to police investigations, and these authorities will apply a high security level to the said files.

The controller shall inform people allowed to access the data about their security obligations and secrecy duty under the terms of Article 8 of Instruction 1/2006.

Furthermore, any person who has access to the data in the performance of his or her duties, will have to maintain due secrecy and confidentiality in relation to the aforementioned data. The controller shall inform the people accessing the data of the secrecy duty referred to in the above section

It is advisable to check the Data Security Guide available in the Documentation Channel of the Agency's website.

<https://www.agpd.es/portalweb/canaldocumentacion/publicaciones/index-ides-idphp.php>

DUTY TO CANCEL IMAGES

Article 6 of Instruction 1/2006 lays down a one month deadline for cancelling images, running from the date when they were captured. This deadline follows the same criterion as that laid down in Article 8 of Act 4/1997 of 4th of August regulating the use of video cameras by National Security Forces in public places.

Once this deadline has been reached, therefore, the images must be cancelled. This means that they must be blocked as laid down in Organic Law 15/1999 and the RDLOPD, whereupon they are kept available only for Public Authorities, Judges and Courts for dealing with any processing liabilities that may arise until the liability time bar lapses. Once the time bar has run its course the data must then be erased.

Should the controller ascertain the recording of an administrative infringement or offence that has to be reported to the corresponding authorities and then duly report it, then the images must be kept available for said authority to check them.

SECURITY FIRMS

As previously pointed out, the use of systems for image capturing and/or processing for video surveillance and security purposes is subject to conditions deriving from the Private Security Act 23/1992 of 30th of July and its Development Regulation, the LOPD and Instruction 1/2006. These are services that may be performed only by companies specifically authorised by virtue of their conditions and qualification. This calls for special diligence in advising the controller who hires their services with respect to compliance with the LOPD and Instruction 1/2006. This qualified diligence duty translates into some specific requirements. First and foremost, and in general:

- Article 20 of the Private Security Regulation (RSP in Spanish initials) lays down the obligation to formalize a contract when a security service is to be provided and notify the appropriate authority. In the video surveillance field the failure to comply with said obligation makes the security firm ineligible for processing purposes.
- The private security firm carrying out operations of camera-based surveillance service installation and maintenance must guarantee that these systems meet the requirements of the LOPD and Instruction 1/2006. Their technical expertise will be particularly important in the following aspects:
 - Entering of the file in the General Data Protection Register (Registro General de Protección de Datos).
 - Siting of the information signs.
 - Definition of the space under surveillance and orientation of the video cameras.
 - Adoption of security measures.
- Absence of the contract will nullify the facilities' legitimacy.

Moreover, as already pointed out above, it should be remembered that whenever the security firm accesses the images, regardless of what the controller might do, the firm will be considered to be the processor and will be held accountable as such pursuant to the provisions laid down in the contract and in Article 12 LOPD.

Security firms, however, whether or not they are considered as processors, must advise private individuals on how to bring the video surveillance facilities into line with data protection legislation. The Spanish Data Protection Agency, in performance of its activity, will notify the government authority ex officio of any incidents

that might come to light, so that the authority becomes aware of the said incidents and may act accordingly in application of the Private Security Act.

■ SPECIFIC CIRCUMSTANCES

In some cases image capturing techniques, even in connection with private security, may have specific characteristics.

ACCESS TO BUILDINGS AND GAMES ROOMS

Controlling access to buildings might involve the capturing of images. They generally involve checkpoints where the data subjects identify themselves, their image is taken and they are issued with a pass or identification card. In these cases, personal data is collected by the security services both in public and private buildings and also in establishments, showrooms, exhibitions and conventions.

Such cases will be governed by the provisions laid down in Instruction 1/1996 of 1st of March, from the Spanish Data Protection Agency, which regulates the automated data files established for the purpose of controlling access to such buildings. All the following will therefore apply:

- The file controller will be responsible for compliance with all the obligations laid down in the LOPD:
 - The file controller will be the natural or legal person, of a public or private nature, or administrative body on whose behalf the security service is being performed.

- Instruction 1/1996 also allows the security firm to be considered as the file controller.
- The data collection procedure will be restricted to the purposes of access control.
- Information on the procedure has to be provided as laid down in Article 5 of the LOPD.
- Personal data may not be used for other purposes or transferred to third parties outside the cases expressly allowed for by law, unless the data subject has given express consent.
- The data will be cancelled when a one-month period has lapsed, this time to run from the moment when the data was collected.
- The file controller will guarantee adoption of appropriate security measures.

Instruction 2/1996 also regulates filing systems set up for the purposes of controlling access to casinos and bingo halls. In this case:

- The file controller will be considered to be the company running the games casino or the tenure holding firm of the bingo hall.
- The file controller must comply with its duty to inform of the data collection procedure.
- Personal data may not be used for other purposes or transferred to third parties outside the cases expressly allowed for by law, unless the data subject has given express consent.

- Personal data shall be destroyed when a six month deadline has passed, this time to run from the date of last access.
- The file controller will guarantee adoption of appropriate security measures.

FINANCIAL INSTITUTIONS

Video surveillance facilities used in banks, saving and loans and other credit institutions are subject by specific rules. The Public Security Act 1/1992 of the 21st of February allows certain measures to be taken for public security purposes. Subsequent development of this law by the Private Security Regulation (Reglamento de Seguridad Privada) has required the installation of cameras and video cameras in this type of institutions. Thus, the provisions of Royal Decree 2364/1994 approving the Private Security Regulation has to be interpreted in connection with the LOPD.

These facilities are privately owned and it is these companies that are responsible for them. Article 120 of the Private Security Regulation defines the peculiarities of the legal system that governs them:

- The images will be made available solely to judicial authorities and National Security Forces, who will immediately be furnished with any images referring to the perpetration of illegal acts.
- The content will be strictly reserved and the recorded images may be used only as a means of identifying the perpetrators of the illegal acts against natural persons and property.

- In general, the images may be seen only by the National Security Forces, judges and courts of law, the inspectorate of the Spanish Data Protection Agency in exercising its rightful duties and by persons entitled to such access by virtue of the Private Security Act.
- Due to the above restrictions the data subjects are not entitled to access these files, unless such right can be invoked by the Spanish Data Protection Agency.
- The cancellation must take place fifteen days after the recording, unless otherwise stipulated by the competent National Security Forces or judicial authorities.
- Matters not explicitly provided for in the Private Security Regulation will be governed by the LOPD and Instruction 1/2006.

This special system calls for abidance by two additional requisites:

- The presence of specific information available to the public which may eventually replace the one laid down in Instruction 1/2006.
- That the employees or managers of the bank have no access to the images, in which case Instruction 1/2006 is fully applicable. Exception is made of cases in which the bank has its own security manager as provided by the Private Security Act and the Regulation on Private Security.

CAMERAS WITH ACCESS TO THE PUBLIC THOROUGHFARE

Video surveillance facilities may be legitimately used only for protection of private environments. Crime prevention and the guarantee of law and order on public thoroughfares is exclusively the responsibility of the National Security Forces. As a general rule, therefore, it is forbidden to take images of the street from private facilities.

On some occasions, however, the protection of private spaces is possible only by setting up the cameras in such spots as building facades. Sometimes it is also necessary to capture images from doors or entrances. Even though the actual camera may be inside the building, it might be impossible not to record at least part of what is happening in the part of the public thoroughfare that is also inadvertently filmed. For this reason article 4.3 of Instruction 1/2006 lays down the following:

3. Cameras and video cameras installed in private places shall not record images of public spaces unless this is essential for the surveillance purpose in view or it is impossible to avoid such recording due to the location of the said cameras. In any case, any data processing other than for the purpose sought shall be avoided.

For this exception to be applicable, there must be no alternative siting possible. It should be borne in mind here that:

- The use of video surveillance facilities in the public thoroughfare is reserved to National Security Forces under Act 4/1997 of the 4th of August which regulates the use of video cameras by National Security Forces in public places.
- Article 4.3 of Instruction 1/2006 does not constitute authority for capturing images in public spaces.
- The file controller will arrange facility use in such a way as to ensure minimum possible impact on the rights of passers by.
- In no case will use of surveillance practices beyond the facility's target area be allowed, especially in regard to surrounding public spaces, adjacent buildings and vehicles other than those entering the space under surveillance.

- Signage will guarantee, in all cases, the rights of the data subjects.
- The security and use indications given to personnel will include express instructions to ensure a proper and commensurate use of the resource.

CAMERAS CONNECTED TO INTERNET

There is an increasingly widespread use nowadays of IP video cameras and webcams capable of transmitting data in digital form on the Internet. The new technology of direct recording in digital format has cut costs and spawned new video surveillance services. These are affordable, widely advertised products whose installation calls for no expert technical knowledge. Certain usage risks need to be analysed, however.

- The use of these cameras involves additional risks when the use of the programme and/or the communications environment is improperly configured.
- The default software configuration may not meet security guarantees, allowing anyone to access the images. A due check needs to be made of whether the identification and authentication functions are activated, to avoid third party access to the images and ensure that only authorised users can access them.
- Digital recording also allows very easy use of the images.

For this reason the following factors should not be forgotten:

- The technical resource used is irrelevant. The installation of any video surveillance system for security purposes calls for the participation of a security firm duly authorised by the Ministry of Home Affairs.

- The system has to meet the security level stipulated in the RDLOPD and in particular:
 - System user identification and authentication procedures have to be set up without allowing access to unauthorised third parties.
 - Access security will be guaranteed by means of public communication networks.
 - Personnel obligations will be defined in due accordance with the nature of the facility concerned.

SCHOOLS AND ENVIRONMENTS WITH MINORS

The capturing of images in school environments is not forbidden but does call for certain precautions to be taken. The installation of video surveillance cameras in a school for controlling behaviour that might affect security has to bear due proportion with the infraction to be avoided; in no case may it be the initial surveillance measure taken. The use of these systems has to be commensurate with the end in sight, which must in all cases be legitimate. The installation of video surveillance cameras would be a commensurate and justified measure if the following requisites are met:

- That it is a measure likely to achieve the end in view.
- That there is no other more moderate measure for achieving this end with the same efficiency.
- That the pros and cons of the measure are duly weighed up, ensuring that the benefits or advantages for the general interests outweigh than harm or damage to other assets or values in conflict.

Minors are data subjects worthy of a special protection and, therefore, the proportionality principle must be applied rigorously. In environments such as schools, crèches, amusement arcades whose target public is minors and similar sites, the installation of video cameras will be legitimate only when it derives from an unavoidable need, when the measure is the most appropriate one to take and providing that there is no alternative method less injurious to the rights of the minor. In particular:

- The area under video surveillance will be the minimum that is essential for the purposes in view, taking in public areas such as entrances or corridors.
- In no case may these resources be installed in spaces protected by the right to privacy, such as bathrooms, dressing rooms or those in which the activities carried out, if recorder, might affect the image or private life, such as gyms.
- Except in extraordinary circumstances, the recording of images for the purpose of checking school attendance will not be allowed.
- The use of video cameras for security purposes in games rooms, classrooms and other areas in which the minors' personality is being developed can be recorded only under exceptional circumstances, duly accounted for by the presence of an objective and likely risk to the security of the minors.

Lastly, video cameras may also be used in school environments for providing other services, which will be examined at a later section.

PUBLIC SPACES OF PRIVATE USE

A great part of people's private life takes place in public spaces of private use, like shopping centres, restaurants, leisure sites, etc. The guarantee of data protection rights extends also to these areas. For that reason, whenever video surveillance systems need to be installed in these places, due consideration has to be given to the rights involved, with strict observance of the proportionality principle.

Thus, by way of example:

- In no case is it permissible to set up cameras in bathrooms or dressing rooms.
- Although use of video surveillance techniques in leisure sites is justifiable, due respect has to be paid to the rights of persons:
 - By not recording conversations.
 - By not using the images for commercial or promotional purposes without authorisation of the subject data, especially for broadcasting on Internet.
- In spaces like gyms or spas, etc, captured images may violate the right to privacy, to the image of the person involved and to data protection. These circumstances have to be taken into account, respecting these rights by not capturing images of identified or identifiable persons in places where they are playing sports or receiving these types of services.

TAXIS

Video surveillance devices in taxis have to be fitted by a private security firm, which has to obtain permission to do so from the Ministry of Home Affairs and, if it is a recording camera, this must be notified previously to the Spanish Data Protection Agency, for entry into the Agency's General Register, as well as fulfilling the other stipulations laid down by Instruction 1/2006.

■ OTHER SECURITY-RELATED USES

Current legislation authorises the use of video cameras in the following contexts: public security, law and order enforcement, crime prevention, traffic control, road safety and security in sporting events.

VIDEO CAMERAS OF THE NATIONAL SECURITY FORCES

Act 4/1997 of 4th of August, which regulates the use of video cameras by National Security Forces in public places, deals with its use by police entities for the purpose of ensuring a civic coexistence, the eradication of violence and peaceful use of public spaces and thoroughfares, as well as preventing the perpetration of offences, crimes and infractions related to public security.

It follows from the provisions laid down in Article 2.2 of the said Act and Article 2.3.e) of the LOPD that the processing of personal data from images obtained from cameras and video cameras used by the National Security Forces will be governed by their specific provisions and by any special provisions laid down in the LOPD. For that reason the specific provisions will be applied to:

- Powers and responsibilities of the Video Surveillance Guarantees Committees (Comisiones de Garantías de la Videovigilancia) with respect to the pre-authorisation report and other powers and responsibilities attributed by the Act and its development regulation.
- Authorisation of fixed facilities and the use of mobile video cameras.
- Registration of authorised facilities.
- Proportionality principle in the use of video cameras in the twofold aspect of suitability and minimum intervention.
 - The suitability principle determines that the video camera can be used only when it turns out to be suitable in a specific situation for law and order purposes and in due accordance with the law.
 - The minimum intervention principle calls for commensurate weighting, in each case, between the end sought and possible effects of the use of the video camera on the right of dignity, image rights and the right to privacy.
 - The use of video cameras will require the existence of a reasonable risk to law and order, in the case of fixed facilities, and a specific hazard, in the case of mobile facilities.
 - Video cameras may not be used for taking images or sounds from inside homes or from dressing rooms, unless the data subject has given his/her consent or there exists a judicial authorisation, nor from sites in public places, open or closed, when this involves a direct and serious effect on the privacy of persons. Neither is it admissible to use them for recording conversations of a strictly private nature.

- Making captured images available to the administrative authority or competent judicial authority.
- Period for preserving the images and its subsequent destruction.
- Signage of the zones under surveillance.
- Exercising rights of access and cancellation.
- Infractions and penalties related to the carrying out of the police activity.

It should be borne in mind here that Act 4/1997 grants the Spanish Regions powers and responsibilities for the protection of persons and property and for the maintenance of public order, to authorize and regulate the use of video cameras by their own regional police forces and by the police forces dependent on local corporations established in their territory, the safe keeping of the recordings obtained, responsibility for their final destination and requests for access and cancellation of these images.

In any case the LOPD is fully applicable and in particular in relation to:

- The creation of files by means of a provision of a general nature published in the corresponding official journal.
- Entry in the General Data Protection Registry of the Spanish Data Protection Agency.
- Adoption of security measures and their corresponding documentation.

- Communication of data to assignees other than the administrative authorities or competent judicial authorities, in relation to any infractions or offences recorded.
- Third party data access contracts.
- Infractions and penalties related to the provisions laid down by Act 15/1999.

Lastly, it should be pointed out that the regulation developing Act 4/1997 excludes its application to:

- Fixed video camera facilities run by the armed forces and the National Security Forces in their buildings, as long as these are dedicated exclusively to guaranteeing security and protection in their interior or exterior.
- When judicial police units regulated by the legislation of National Security Forces capture images and sounds by means of video cameras, while performing functions of judicial police in a strict sense, they will be governed by the Criminal Procedures Act (Ley de Enjuiciamiento Criminal) and its specific legislation.

In these cases, therefore, the provisions of the LOPD and Instruction 1/2006P are fully applicable.

VIDEO CAMERAS FOR TRAFFIC CONTROL PURPOSES

Act 4/1997 and its development regulation lays down specific provisions for these facilities. Specifically, its eighth additional provision runs as follows:

The installation and use of video cameras and of any other means of capturing and reproducing images for traffic control, regulation, surveillance and discipline will be carried out by the authority in charge of traffic regulation for the purposes laid down in the Road Safety and Motor Vehicle Traffic Act (Ley sobre Tráfico, Circulación de Vehículos a Motor y Seguridad Vial) approved by Royal Legislative Decree (Real Decreto Legislativo) 339/1990 of the 2nd of March and other specific legislation on the matter, and will be governed by the Personal Data Computerised Processing Regulation Act 5/1992 of the 29th of October (Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal) and Civil Protection Act 1/1982 of the 5th of May (Ley Orgánica de Protección Civil del Derecho al Honor, a la Intimidación Personal y Familiar y a la Propia Imagen) on the Right to Dignity, the Right to Personal and Family Privacy and to one's Own Image.

This entails application of some specific provisions of said Act and of the single additional provision of Royal Decree 596/1999 of the 16th of April, approving the regulation for development and enforcement of Act 4/1997 of the 4th of August regulating the use of video cameras by National Security Forces in public places:

- The cameras shall be used with due respect for the principle of proportionality in its twofold aspect of suitability and minimum intervention.
- It will be the responsibility of the public authority in charge of traffic regulation to authorise the installation and use of these devices.
- The resolution authorising the installation and use of fixed image capturing and reproducing devices:
 - Will give a general identification of the public thoroughfares or sections whose image is likely to be captured.
 - The measures to be taken to guarantee availability, confidentiality and integrity of the recordings or registrations obtained.

- The body in charge of its safeguarding and dealing with requests for access and cancellation.

It should be borne in mind here that these cameras can also be used under the framework of Act 4/1997, with all the authorisations laid down in this Act being duly processed and obtained.

In any case these video cameras are also governed by the Spanish Data Protection Act 15/1999 of the 13th of December, especially in terms of the following aspects:

- Creation of files by means of a provision of a general nature published in the corresponding official journal.
- Entry in the General Data Protection Registry of the Spanish Data Protection Agency.
- Adoption and documentation of security measures.
- Satisfaction of the rights of persons.
- Signage of the area under surveillance.

SPORTING EVENTS

Article 61 of Royal Decree 769/1993 of the 21st of May, approving the Regulation for the Prevention of Violence at Sporting Events provides for the installation and use of closed circuit television. These circuits will be fixed with fixed and mobile cameras.

- Fixed cameras will monitor the inside and outside of the venue, covering the entrance areas and the stands and giving a total view of the whole venue.
- Mobile cameras will be set up in such areas as the security coordinator deems necessary for monitoring each particular sporting event.
- Closed circuit television will also have the necessary recording devices to film the attitudes of the crowd and the behaviour of violent groups.

The board of directors or steering board of the professional football clubs will be responsible for designating a Security Service Chief. This will also be done in such cases as are established by regulations. The Security Service Chief will work under the instructions of the Security Coordinator in each club, public limited company or sporting event.

In this context the following should therefore be taken into account:

- The tenure holder of the facility will be the file controller.
- All provisions of Instruction 1/2006 have to be met.

USE OF VIDEO CAMERAS FOR BUSINESS CONTROL PURPOSES

Article 20.3 of the Statute of Workers' Rights entitles employers to adopt such surveillance and control measures as they deem fitting to check on worker compliance with their occupational duties and obligations, making sure that due heed is paid to human dignity in the adoption and implementation of these

measures and bearing in mind the actual capacity of any disabled workers. These measures might include the capturing and/or processing of images without previous consent.

Such practices, however, are fully governed by the LOPD and Instruction 1/2006 and shall meet the following requisites:

- The processing will be limited to the purposes laid down by the Statute of Worker's Rights, and/or the legitimate purposes recognised by legislation. In the latter case, such additional provisions as may be applicable must also be met.
- They will strictly abide by the principle of proportionality:
 - This measure will be taken only when there is no other more suitable alternative.
 - The facilities, if used, will be limited to the strictly necessary uses for capturing images in essential areas for fulfilling the workforce monitoring purposes.
 - These resources may not be used for purposes other than those of workforce monitoring unless it is a question of legitimate purposes and all due measures are taken to ensure compliance with such legislation as may be applicable.
- Due heed will be paid to the specific rights of the workers, respecting:
 - The right to privacy and the fundamental data protection right in relation to areas where resources of this type are vetoed, such as bathrooms, locker rooms and rest zones.
 - The right to the workers' own image.

- The private life within the working environment, in particular avoiding any recording of private conversations.
- The right to receive information on the image collection procedure will be guaranteed:
 - With specific information to trade union representation.
 - By means of an informative poster and the informative handout established by Instruction 1/2006.
 - By means of personalised information.
- The corresponding file will be created and/or registered as need be.
- Cancellation of the images within 30 days will be guaranteed. Only those recording an infraction or breach of occupational duties may preserved further.
- Rights of access and cancellation will be guaranteed.
- Any third-party data access contracts will be drawn up as necessary.
- The corresponding security measures will be taken.

OTHER PROCESSING ARRANGEMENTS

The use of video cameras and the capturing of images is also provided for in other fields to which data protection legislation applies.

■ PROCESSING IN SCHOOL ENVIRONMENTS FOR NON-SECURITY PURPOSES

There are value added services based on image capturing. An increasingly frequent use involves giving parents access to images of classes and play areas in crèches or children's education centres. In this case, due heed must be paid to the following:

- The general principles of the LOPD are applied.
- Consent for the processing of data of minors is regulated in article 13 RDLOPD and calls for authorisation from the father, mother or legal guardian in the case of minors.
- A precise definition must be made of the purpose for which said images are being captured. In all cases this procedure must abide by the principle of proportionality and suitability and, in particular, any additional uses with promotional or marketing purposes, school activity reports or public websites of the centre concerned.

- Due information must be given on the procedure and due respect must be shown for the rights of workers affected by the use of video cameras, such as monitors, teachers, cleaning personnel, etc.
- Security and secrecy must be guaranteed, in particular with online access to the images.
- In cases where group access is allowed, such as all the parents of the children in a classroom:
 - Access profiles must be defined, for example, limiting access only to the classrooms where the particular parents' children are, and no others.
 - Parents must be informed of the data access liabilities incumbent upon them.

■ VIDEO INTERCOM SYSTEMS

Instruction 1/2006 expressly excludes its application to images taken in personal and domestic environments, understanding these to be those taken by an individual in the context of an exclusively private or family-based activity.

In those cases, therefore, in which the use of video intercom systems is limited to their function of identifying the person calling at the door and letting them in, the data protection legislation will not be applicable. Nonetheless, if the service involves constant reproduction and/or recording of images which are then made available to neighbours, either through the Internet or TV broadcasts, and in particular when the images include the neighbouring courtyard and/or public thoroughfare, Instruction 1/2006 will then be fully applicable.

■ SCIENTIFIC RESEARCH AND RELATED USES

One of the possible purposes for capturing or recording images of identified or identifiable persons is research, whether this be scientific research, consumer studies or even in personnel selection processes.

Such cases would be fully governed by the Personal Data Protection Act 15/1999 of the 13th of December. A crucially important factor here is compliance with the principles of purpose and proportionality in data processing.

■ TOURISM PROMOTION AND RELATED PURPOSES

Internet broadcasting of images for promotional purposes is an increasingly frequent practice. These images might be broadcast a specific corporate sphere such as building facades or one-off spaces in firms and institutions – or they might portray places of interest for tourists. Only when the capturing and broadcasting of these images does not affect any identified or identifiable persons will the activities concerned be exempt from the provisions of the LOPD.

■ GENERAL RULES

In any of the former cases, when the images refer to identified or identifiable persons, the general data protection principles currently in force shall be applied:

- Legal authorisation must have been obtained or the consent of the data subjects must have been applied for.
- If the environments concerned include areas in which worker images might be captured, due heed must be paid to occupational legislation containing criteria and guarantees with regard to their rights and duties.
- Due information will be given about the existence of the image capturing facilities and their tourism or promotional purpose and they shall not be used for any other purpose.
- The appropriate security measures will be adopted.
- The images will be preserved only for the essential time for fulfilling the purpose for which they were collected.
- In cases in which the images are freely accessible on the Internet, it is advisable to set up privacy policies establishing, particularly, conditions of use for third parties.

Data protection rules will not be applicable to images captured and/or reproduced in this way when they do not allow persons to be identified or provide any other information conducive to their personal identification, such as vehicle licence plate numbers.

PERSONAL RIGHTS

Exercising of personal rights has idiosyncratic features in terms of video surveillance.

Firstly, the right of rectification is unenforceable due to the very nature of the data in question. i.e., images of the real world reflecting an objective fact. Enforcing a rectification right within this context would prove impossible.

Secondly, exercising the right of objection also poses huge problems. If this is interpreted as the impossibility of taking images of a given subject in the context of private security video surveillance facilities, this would once more be an unenforceable right since the purpose of security protection would prevail.

Exercising the right of access also has idiosyncratic features:

- It would call for complementary documentation to be furnished with an up-to-date image of the data subject, to allow the controller to check and verify his or her presence in the recordings.
- It is practically impossible to access images of one person without compromising the image of another. Access could therefore be granted by means of a written document specifying as precisely as possible, and without affecting third party rights, the data that has been processed.

E.g. "Your image was recorded in our systems on ___ (day) _____ (month) _____ (year) between _ (time) and _ (time). Specifically, the system records you entering and leaving the building.

- If the right to access is requested to the controller of a system that only reproduces images without recording them, said controller will, in any case, have to reply to the request indicating the absence of any recorded images.
- The cancellation requested by the data subject will be governed by the provisions laid down in LOPD without any special feature whatsoever.
- It should not be forgotten that, pursuant to RDLOPD, when a right is turned down, an express indication should be made of the possibility of appealing to the manager of the Spanish Data Protection Agency.

It is advisable to check out the file controller's guide available on the Documentation Channel of the agency's website.

<https://www.agpd.es/portalweb/canaldocumentacion/publicaciones/index-ides-idphp.php>

GUIDELINES

The use of video surveillance facilities for capturing, recording or reproducing images of identified or identifiable persons is a practice that might impinge on fundamental rights and, in particular, on the fundamental right to data protection. It is therefore worthwhile bearing in mind some recommendations that can be drawn from the contents of this guide:

- The choice of this type of resource should always be made in due accordance with the principle of proportionality, ruling out video surveillance where there are alternative measures less injurious to fundamental rights.

- Analysis of the proportionality of the measure will be particularly thoroughgoing in sensitive environments, whether due to the nature of the subjects under surveillance, such as minors in a school environment, or whether because they comprise aspects of private life, as in leisure facilities or gymnasia.
- If video surveillance is used for private security purposes, security firms must always be resorted to.
- The controller, company, institution, residents' association, etc. must always be diligent in election of the security firm to render the service. The chosen firm shall always meet all legal requisites for performing this service.
- The security firm should diligently and faithfully advise whoever requires its services. This advice includes data protection legislation.
- In the working environment, due respect should be paid to workers' rights.
- In any case, the controller and processor shall ensure compliance with personal data protection laws and any other applicable legislation.

FREQUENTLY ASKED QUESTIONS

Why are the LOPD and Instruction 1/2006 applied to video surveillance?

A person's image constitutes data of a personal nature. Personal data shall mean any information relating to an identified or identifiable natural person. Video surveillance systems will normally capture images of workers, customers or persons bearing some degree of relationship that makes them identifiable.

What does Instruction 1/2006 on video surveillance regulate?

It regulates the capturing of images for security-related video surveillance purposes. It deals with cases where the controller is entitled to capture and record images for the purpose of guaranteeing the security of buildings, facilities, etc. under the provisions of the Private Security Act, or for exercising the workforce surveillance powers attributed to employers by the Statute of Workers' Rights.

Nonetheless, the principles of the Instruction are valid and useful for any other image processing by means of video cameras.

Is the use of a video camera for recording images of family life subject to Instruction 1/2006?

No, the Spanish Personal Data Protection Act 15/1999 of the 13th of December (Ley Orgánica de protección de los datos de carácter personal) and, in turn, the provisions of the Instruction, are not applicable to image processing by individuals pur-

suing exclusively personal or domestic activities, including social acts like school or group celebrations.

That said, if the video cameras are set up to safeguard the security of a dwelling, it must then comply with the provisions laid down in Instruction 1/2006, especially when it involves common areas in condominiums, private housing estates or when it affects personnel working inside the home.

What should be done when the cameras are installed by a residents' association or property owners in a housing estate?

First and foremost, systems of this type can be installed only with the help of a private security firm duly authorised for performing services of this type, pursuant to the Private Security Act. Furthermore, the residents' association will be responsible for the corresponding file or processing arrangement and will have to comply with all obligations laid down by law.

A file will be deemed to exist if the images captured by the camera are recorded by any means – VHS tape, DVD, CD-ROM, hard disk of a computer – which hence allows retrieval of information relating, for example, to a recording made on a particular day in a particular place. The LOPD makes it compulsory for the file to be entered into the General Data Protection Registry of the Spanish Data Protection Agency.

Persons also have to be informed that they might be recorded. This information is to be provided by means of an informative sign set up as established in Instruction 1/2006. This sign must identify the existence of an area under surveillance and the file controller from whom to invoke rights of access and cancellation. In these access points, or in a suitable place, a printed informative handout will be made available giving detailed information on the circumstances of the image processing under the terms laid down in article 5 LOPD.

It is necessary to formalise a contract with the security firm, bearing in mind that if this firm has access to the images or uses the equipment and facilities it will be considered to be the official processor. There are also obligations such as guaranteeing the rights of the image subjects and security of the systems.

What if the images are not recorded but only broadcast in closed circuit under the control of a security employee?

In this case there will be no file or registration obligation but the rest of the processing obligations do have to be complied with. In particular there is a duty of displaying information by means of an informative poster.

Where should the sign be fitted? Below each camera?

No, the sign has to identify the area under surveillance so that everybody subject to the video surveillance has the opportunity of becoming aware of the existence of the video cameras when entering the premises. This does not mean that the specific siting of each camera needs to be pinpointed.

Premises with several entrances have to have an informative poster fitted in each access, thereby ensuring that anyone entering the premises by any entrance always sees the information.

Should the informative poster of Instruction 1/2006 only be used in the context of private security?

The objective of the instruction is that it be used whenever there is a video surveillance facility for security purposes. Nonetheless, there is no reason why the infor-

mation procedure laid down in Instruction 1/2006 could not be equally effective in other contexts.

Should printed informative handouts always be on hand for the affected parties?

The controller could prepare pre-printed handouts and make them available on site or print them at the request of the data subject.

Should the informative poster identify the controller in a precise way?

As a general rule it is essential for the controller to be identified. In certain environments, such as a shop or small-business entrance, where the controller is the owner of the establishment, the simple fixing of the poster enables the controller to be easily identified. But where these circumstances do not occur, or if the space lends itself to confusion, such as in a shopping centre where it might be very difficult to identify the processing controller, the mere mention of the existence of a video surveillance system will not suffice and express identification of the controller must be made, as laid down in Article 3 of Instruction 1/2006.

Can images of the public thoroughfare be taken?

The capturing of images on the public thoroughfare for security purposes is regulated by Act 4/1997 of the 4th of August regulating the use of video cameras by National Security Forces in public places, where its use is reserved for the said National Security Forces. On certain occasions, however, the installation of a private video surveillance system can partially capture images of the public thoroughfare. These cases have to be exceptional and must abide by the principle of due proportionality in the processing. Firstly, there should be no possibility of an alternative facility. Secondly, the video cameras have to be orientated so that the main object

of surveillance is the private environment, and the capturing of images of the public thoroughfare is kept down to an absolute minimum, as may be essential for the purposes in view. It might prove to be the case, for example, that the recording of images in a garage entrance also captures images of people passing precisely in front of the garage but it should never capture the street as a whole or the pavement or, of course, the adjacent buildings.

How long should the images be kept? Is there an obligatory one-month deadline?

Instruction 1/2006 lays down a maximum period of one month. So there is no reason why they could not be kept for a shorter period.

What happens if the images capture the perpetration of an offence or infraction?

The incidents and images should be, of course, reported to the appropriate authority, since this is one of the purposes sought by the Private Security Act. Moreover, Article 11.2.d) of the LOPD empowers the Public Prosecutor's Office and the judges and courts of law to summon personal data included in any information system and, thus, any images taken by a video surveillance system.

What rights do citizens have?

Citizens can exercise their right to access images and cancel them. On many occasions this access could affect the rights of third persons who also appear in the images, so the access might be authorised with written indication of the existence of images of the person exercising his or her right.

Is the capturing of images in a school environment subject to Instruction 1/2006?

A distinction has to be made between the rightful security purposes and other purposes. In the first case the installation of video cameras in entrances, playgrounds or public areas of a school not designed for teaching purposes is governed by Instruction 1/2006. This does not apply to facilities designed for teaching purposes, such as the classrooms, where security is unlikely to be a legitimising factor. In the latter case, therefore, the consent of the data subjects, or their parents or legal guardians if they are over fourteen years of age, will be required, without detriment to the additional duty of respecting the rights of classroom personnel.

Can recordings be made anywhere?

No, some areas are protected by the right to privacy such as bathrooms and changing rooms, where facilities of this type cannot be used.

Who is entitled to see the images? Only the security firm or the file controller, i.e., the tenure holder of the premises under surveillance?

Any of them is entitled to see the images. The processing controller shall designate the specific people who will be able to see the images, who will be registered as authorised users in the security document and shall be informed of their respective obligations.

Thus, for example, when the processing controller is a residents' association or the like, it shall designate the specific person(s) (for example concierge and association president) who is or are entitled to view the images. Closed circuit television seen by all homeowners would be disproportionate and could constitute an offense.

What rights do workers have in a working environment? Can they be recorded unbeknown to them?

This environment is fully governed by the personal data protection principles. Thus, although the recording might be made without their consent pursuant to the Statute of Workers Rights, due observance must always be made of the duty to inform and the other obligations laid down in the LOPD.

Is a video intercom system subject to Instruction 1/2006?

No, a video intercom system is considered to be for domestic or family-based use and, thus, it is excluded from application of the personal data protection legislation.

Nonetheless this exclusion will be made only when the use of these appliances is restricted to their rightful purpose.

Is the home installation of a camera to watch over those carrying out cleaning or child-care tasks understood to be private and/or domestic use?

Article 20.3 of the Statute of Workers' Rights authorises employers to process images of their workers. It is essential that the workers, at least, be informed of this fact. In general, therefore, providing that the workers are informed of the fact, cameras to monitor their activity can be installed within the home. It should be borne in mind here that there must be due proportionality between the purpose and the processing.

AGENCIA
ESPAÑOLA DE
PROTECCIÓN
DE DATOS





AGENCIA
ESPAÑOLA DE
PROTECCIÓN
DE DATOS



www.agpd.es