Prime Minister's Office
Data Protection Office

GUIDELINES
to regulate
THE PROCESSING OF PERSONAL DATA BY VIDEO SURVEILLANCE SYSTEMS
(Volume 5)

GUIDELINES
to regulate
THE PROCESSING OF PERSONAL DATA BY VIDEO SURVEILLANCE SYSTEMS
(Volume 5)

CONTENT

FOREWORD BY THE COMMISSIONER

Video surveillance has infiltrated our daily life at a pace which requires some monitoring by the state. The systems available on the market are capable of recording both images and sounds which either identify or allow the identification of data subjects, directly or indirectly, in addition to monitoring their conduct. The implementation of closed circuit TV (CCTV) as a convenient means to achieve security purposes raises fundamental issues with regard to privacy and data protection.

A widespread and abusive use of surveillance may jeopardise the citizens' freedom of movement and behaviour. Therefore, the solution lies in striking the right balance between these two competing interests namely-the safeguard of both privacy and public interest/national security.

Video surveillance techniques have evolved from static and passive cameras documenting events to dynamic and preventive networks. Two trends have spearheaded this change: the shift towards wireless IP systems and the emergence of video analytics. The former allows for flexible networks, massive customisation whereas the latter comes to solve the problem of increased network complexity. This evolution has brought however new threats for individual freedoms, challenging in particular the application of data protection safeguards.

There is thus a pressing societal need to identify the parameters within which video surveillance should operate and the necessary safeguards to be implemented to protect the privacy of individuals and to counteract the psychological effect related to video surveillance, whereby it is sometimes regarded by public opinion, rightly or not, as an "invaluable tool" in the prevention and detection of offences.

Data subjects have the right to exercise their freedom of movement without undergoing excessive psychological conditioning as regards their conduct on account of disproportionate application of video surveillance by entities in a number of public and/or publicly accessible premises.

The objectives of these guidelines are to ensure that those who operate video surveillance systems including CCTV (Closed Circuit Television) and other systems such as satellite based GPS systems, adopt good practice standards. They are aimed primarily at businesses and organisations (both public and private) which regularly capture images of identified or identifiable individuals on their video surveillance equipment for viewing and /or recording the activities of individuals for specific purposes since the personal data captured may potentially be used for other incompatible purposes affecting the privacy of the individual.

Recognisable images captured by CCTV systems including satellite-based GPS systems are "personal data". They are therefore subject to the provisions of the Data Protection Act.

Since, the use of CCTV and other systems may also be suspiciously viewed as contributing to the make of a surveillance society, following the principles enunciated in these guidelines will help to foster public confidence and trust in the use of these systems.

INTRODUCTION

In deciding whether to use a video surveillance system, a data controller or processor should consider objectively the benefits to be gained from such an installation, whether there exist better alternative solutions which are not privacy intrusive and which can achieve the same objectives, commonly known as privacy-enhancing technologies (PETs).

Indeed, surveillance systems form part of a multifarious and continuously evolving sector ranging from surveillance related to:-

- road traffic,
- unlawful conduct in the surroundings of schools,
- the provision of medical facilities during surgery with a view to, for instance, providing distance care to or monitoring patients in intensive care units or the hospitalization of quarantined patients,
- the supervision of airports and on board of ships and near border areas in order to monitor alien smuggling as well as to facilitate the searching of minors and other missing persons,
- investigation by private detectives,
- the control within and near supermarkets and shops especially those dealing in luxury goods with a view to collecting evidence in case offences are committed as well as for the purpose of marketing goods and/or profiling consumers,
- to exercise control within and in areas adjacent to private condominiums both for security purposes and in order to make available evidence in case offences are committed,
- for journalistic and advertisement purposes that are pursued on line by means of either web cams or cameras on line used for example for advertising purposes, tourist promotion on beach resorts and dancing premises,
- to the filming of customers and visitors at regular intervals without any warning.

Where the system is operated by or on behalf of a public authority, it will have to consider whether :-

- the system is being operated in accordance with the law;
- it is addressing issues such as public safety, order, morality, crime prevention and detection, national security and whether it is reasonably justifiable in a democratic society;
- it is strictly proportionate, legitimate and necessary, i.e. do the ends justify the means?

Video surveillance, generally, may serve quite different purposes which can therefore be grouped, however, into a few main areas:

- protection of individuals,
- protection of property,
- public interest and national security,
- crime prevention and detection and apprehension and prosecution of offenders, collection of evidence,
- other legitimate interests, reasonably justifiable in a democratic society.

Clear documented procedures need to be put in place by the data controller to ensure an effective administration of these systems and the responsibility for ensuring that these procedures are followed should be delegated to appropriate staff who should also carry out regular checks to ensure these procedures are being followed.

A data controller must justify the obtaining and use of personal data by means of a CCTV system. Thus, a system used to control the perimeter of a building for security purposes will usually be easy to justify. The use of CCTV systems in other circumstances – for example, to constantly monitor employees, customers or students – may be more difficult to justify and could involve a breach of the Data Protection Act.

Identifiability within the meaning of the Data Protection Act may also result from matching the data with information held by third parties, or else from the application, in the individual case, of specific techniques and/or devices.

Hence, one of the first precautions to be taken by the data controller is to check whether the video surveillance entails the processing of personal data because it relates to identifiable persons.

This may be the case, for instance, with equipment located either at the entrance of or inside a bank, where the said equipment allows identification of customers; conversely, in certain circumstances the applicability of the Data Protection Act may be ruled out for example, air survey images that cannot be usefully magnified or else do not include information related to living individuals as for equipment providing sweeping images of motorway traffic.

Thus, image and sound data relating to identified or identifiable living individuals is personal data:

- when used within the framework of a closed circuit system;
- even if they are not associated with a person's particulars;
- even if they do not concern individuals whose faces have been filmed, but contain other information such as, for instance, car plate numbers or PIN numbers as acquired in connection with the surveillance of automatic cash dispensers;
- irrespective of the medium used for the processing – e.g., fixed and/or mobile video systems such as portable video receivers, colour and/or Black or White images ;
- irrespective of the technique used for the processing– cabled or fibre optic devices ;
- irrespective of the type of equipment used for the processing– stationary, rotating, mobile -, the features applying to image acquisition – i.e. continuous as opposed to discontinuous, which may be the case if image acquisition only occurs in case a speed limit is not respected and has nothing to do with video shootings performed in a wholly casual, piecemeal fashion; and
- irrespective of the communication tools used for the processing, e.g. the connection with a "centre" and/or the circulation of images to remote terminals, etc.

As regards obtaining the data subject's consent, the latter will have to be freely given, specific, informed, unambiguous and based on clear-cut information. Consent will thus have to be sought separately and specifically in connection with surveillance activities.

PROPORTIONALITY

The principle that data must be adequate and proportionate to the purposes sought means, in the first place, that CCTV and similar video surveillance equipment may only be deployed on a subsidiary basis, that is, for purposes that actually justify recourse to such systems.

Therefore, the proportionality principle entails that these systems may be deployed only if other prevention, protection and/or security measures, of physical and/or logical nature, requiring no image acquisition – e.g. the use of armoured doors to fight vandalism, installation of automatic gates and clearance devices, joint alarm systems, better and stronger lighting of streets at night etc. – prove clearly insufficient and/or are inapplicable to the legitimate purposes sought.

The same principle also applies to the selection of the appropriate technology, the criteria for using the equipment in concrete, and the specification of the data processing arrangements also related to access rules and retention period.

It should be avoided, for instance, that an administrative body may install Video Surveillance equipment in connection with minor offences – e.g. in order to reinforce the ban on smoking in schools and other public places or else the prohibition to leave cigarette stumps and litter about in public places.

In other words, it is necessary to apply, on a case by case basis, the *principle of adequacy* in respect of the purposes sought, which entails a *duty of minimisation of data collection* on the controller's part.

Whilst a proportionate video surveillance and alerting system may be considered lawful if several episodes of violence occur in an area close to a stadium, or if repeated assaults are committed on board buses in peripheral areas or near bus stops, this is not the case with a system aimed either at preventing insults against bus drivers and the dirtying of vehicles, identifying citizens liable for minor administrative offences such as the fact of leaving waste disposal bags outside litter bins and/or in areas where no litter is to be left about, or detecting the persons responsible for occasional thefts at swimming halls.

Proportionality should be assessed on the basis of even stricter criteria as regards non-publicly accessible premises.

The above considerations apply, in particular, to the increasingly frequent use of video surveillance for the purpose of self-defence and protection of property – above all near public buildings and offices including the surrounding areas. This type of implementation requires assessing, from a more general viewpoint, the indirect effects produced by the massive recourse to video surveillance – i.e., whether the installation of several devices is really an effective deterrent, or whether the offenders and/or vandals may simply move to other areas and activities.

WHAT IS THE PURPOSE FOR USING CCTV SYSTEMS?

Images must be processed fairly and lawfully as well as for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. The data controller should ensure that the purposes sought are neither unclear nor ambiguous, also in order to be provided with a precise criterion when assessing compatibility of the purposes aimed at by the processing.

The purpose and use of the CCTV system should be established before actual use:-

- Assess the reasons for using the equipment and how appropriate it is.
- Establish the person or organisation that is legally responsible for the scheme
- Establish the purpose of the scheme.
- Document the standards contained stated above.
- Effect registration under section 34 and notification under section 35 B of the DPA for changes in particulars with the Office of the Data Protection Commissioner to cover this additional purpose of use of personal data, if you are already registered and that purpose is not included in your registration form.
- Document and identify the person or organisation that will monitor compliance of the scheme.
- Establish and document security and disclosure policies.

It should be clearly ruled out that the images collected may be used for further purposes, for instance, with particular regard to technical reproduction opportunities –by expressly prohibiting copying of these images to unauthorized third parties or recipients. The relevant purposes should be referred to in a document where other important privacy policy features should also be summarised – in respect of such major issues as documenting the time when images are deleted, possible requests for access by data subjects and/or lawful consultation of the data.

Section 26 © of the Act provides that personal data should be *"adequate, relevant and not excessive in relation to the purpose for which such data has been collected and processed"*. Therefore, a data controller must be able to demonstrate that installing a system that collects personal data on a continuous basis is indeed justified. It must further be able to meet its obligations to provide data subjects, on request, with copies of images captured by the system.

This principle under which data must be adequate, relevant and not excessive also entails a careful assessment of the *proportionality of the arrangements* applying to the data processing once the lawfulness of the latter has been validated.

The *filming arrangements* will have to be taken into account in the first place, by having regard, in particular, to the following issues:

the visual angle as related to the purposes sought - for e.g :–

- if the surveillance is performed in a public place, the angle should be such as
- not to allow visualising details and/or somatic traits that are irrelevant to the purposes sought, or else the areas inside private places located nearby, especially if zooming functions are implemented;
- the type of equipment used for filming, i.e. whether fixed or mobile;
- actual installation arrangements, i.e. location of cameras, use of fixed view and/or movable cameras, etc.;
- possibility of magnifying and/or zooming in images either at the time the latter are filmed or thereafter, i.e. as regards stored images, and possibility to blur and delete individual images;
- image-freezing functions;
- connection with a "centre" to send sound and/or visual alerts and/or the circulation of images to remote terminals;
- the steps taken as a result of video surveillance, i.e. shutting down of entrances, calling up surveillance staff, etc.

Whilst in a few cases a system only enabling closed circuit visualisation of images, which are not recorded, may be sufficient – e.g., in the case of the tills at a supermarket –, in other cases - e.g. to protect private premises – it may be justified to record the images and automatically erase them, no later than at the end of the day and at least at the end of the week.

An exception to this rule will obviously be the case in which an alert has been issued or else a request has been made deserving specific attention; in such cases there are reasonable grounds to await, for a short time, the decision to be possibly taken by either police or judicial authorities.

To quote another instance, a system aimed at detecting unauthorised accesses of vehicles to city centres and restricted traffic areas should only record images in case a breach is committed.

The proportionality issue should also be taken into due account whenever longer retention periods are deemed to be necessary – e.g., as regards video surveillance images that may be used to identify the persons frequenting the premises of a bank prior to performing a robbery.

Thirdly, attention will have to be paid to the *cases in which identification of a person is facilitated* by associating the images of the person's face with other information concerning imaged conduct and/or activities – e.g., in the case of the association between images and activities performed by clients in a bank at an easily identifiable time.

In this regard, account will have to be taken of the clear-cut difference existing between temporary retention of video surveillance images obtained by means of equipment located at the entrance of a bank and the definitely more intrusive establishment of data banks including photographs and fingerprints provided by bank clients with the latter's consent.

Finally, consideration will have to be given to the decisions to be made in respect of both the *possible communication of the data to third parties* – which in principle should not involve entities unrelated to the video surveillance activities – and their total or partial disclosure possibly abroad or even online.

Obviously, the requirement that images should be relevant and not excessive also applies to the matching of information held by different controllers of video surveillance systems.

The above safeguards are meant to implement, also operationally, the *principle of moderation in the use of personal data* – which is aimed at preventing or reducing, to the greatest possible degree, the processing of personal data.

This principle should be implemented in all sectors by also having regard to the fact that many purposes can be actually achieved without making recourse to personal data, or by using really anonymous data, even though they may initially seem to require the use of personal information.

The above considerations also apply in the presence of the justified need to streamline business resources or else improve the services delivered to users.

This may be the case, for instance, with the need to calculate the number of tills to be kept simultaneously open in a supermarket depending on the number of incoming customers, or else with the requirement of building optimised shopping routes for customers in a supermarket.

To facilitate access to a working place and/or a specific transportation means requiring identity controls, personal cards with photographs may be enough, possibly on computerised media, without the need for implementing a facial recognition system.

It is advised that processing operations by means of video surveillance carried out by public bodies should always be grounded on express legal provisions.

It is also necessary to consider the *decision to be taken as to retention of images and retention period* – the latter having to be quite short and in line with the specific features of the individual case.

QUALITY OF DATA

Images produced by the system must be as clear as possible to ensure that they are effective for the purposes for which they are intended. When installed, the equipment should be checked to ensure it performs correctly:-

- The medium on which the images are recorded should be cleaned to prevent recording on top of previous images;
- The medium on which the images are recorded should no longer be used if there is a deterioration in the quality of the images;
- If the system records location of camera, date, time etc. these should be accurate;
- There should be a documented procedure;
- Cameras should be sited only where they will capture relevant images;

- If automatic facial recognition systems are utilised, the database of images should be clear;
- A human operator should assess and determine the action to be taken to verify matches made by automatic facial recognition systems;
- The assessment above should be documented regardless of a match on the database;
- Consideration must be given to the physical conditions in which the cameras are located;
- Operators should assess whether real time or specific timed recordings are required;
- Cameras should be properly maintained and serviced;
- Cameras should be protected from vandalism where the risk for such a situation may arise;
- A maintenance log should be kept;
- If a camera is damaged, there are clear procedures for:
    - Defining the person responsible for making arrangements for ensuring the camera is fixed;
    - Ensuring the camera is fixed within a specific time period;
    - Monitoring the quality of the maintenance work.

SHOULD THE PROCEDURES FOR CAPTURE OF IMAGES BE MADE TRANSPARENT TO TARGETTED DATA SUBJECTS?

- Signs, which are clearly visible and legible, should be displayed so that the public are aware they are entering an area covered by CCTV.
- Specific information should be included on the sign:-
- The identity of the person responsible for the scheme;
- The purpose of the scheme;
- Details of who to contact regarding the scheme; (only applies if the location does not make this obvious).
- If signs are not appropriate and monitoring is for a specific criminal activity:
    - Fully document the following steps;
    - Identify the specific criminal activity;

- Identify whether there is a need to use surveillance to obtain evidence of that activity and whether the use of signs would prejudice success in obtaining such evidence;
- To ensure covert monitoring is not carried out for longer than is necessary, assess how long such monitoring should take place.

Section 22 (2) of the Act requires that at the time any personal data are recorded, the data controller is placed under the obligation to supply some essential information to the data subject which includes:

- the identity of the data controller;
- the purposes for which personal data are processed;
- any third parties or recipients to whom the personal data may be disclosed.

If the identity of the data controller and the usual purpose for processing is obvious, i.e, security, all that need be placed on the sign is a statement that CCTV is in operation as well as a contact (such as a phone number) for persons wishing to discuss this processing. This contact can be for either the security company operating the cameras or the owner of the premises.

If the purpose or purposes is not obvious, there is a duty on the data controller to make this clear. A CCTV camera in premises is often assumed to be used for security purposes. Use for monitoring staff performance or conduct is not an obvious purpose and staff must be informed **before** any data are recorded for this purpose. Similarly, if the purpose of CCTV is also for health and safety reasons, this should be clearly stated and made known.

CCTV must not be used to record conversations between members of the public as this is highly intrusive and unlikely to be justified. If your system is equipped with sound recording facility, you should disable it.

In the limited circumstances where audio recording is justified, clear signs must be displayed that audio recording is being or may be carried out.

Use of CCTV to monitor areas where individuals would have a reasonable expectation of privacy would be difficult to justify. Surveillance should not include premises that either are reserved for employees' private use or are not intended for the discharge of employment tasks – such as toilets, shower rooms, lockers and recreation areas; that the images collected exclusively to safeguard property and/or detect, prevent and control serious offences should not be used to charge an employee with minor disciplinary breaches; and employees should always be allowed to lodge their counterclaims by using the contents of the images collected.

To justify use in such an area, a data controller would have to demonstrate that a pattern of security breaches had occurred in the area prior to the installation of the system which would warrant constant electronic surveillance.

Openness and appropriateness in the use of video surveillance equipment entails the provision of adequate information to data subjects. They should be aware of the fact that video surveillance is in operation, even where the latter is related to public events and shows or else to advertising activities (web cams); they should be informed in a detailed manner as to the places monitored. It is not necessary to specify the precise location of the surveillance equipment, however the context of surveillance is to be clarified unambiguously.

The information should be positioned at a reasonable distance from the places monitored taking into consideration the filming arrangements.

The information should be visible and may be provided in a summary fashion, on condition that it is effective; it may include symbols that have already been proved useful in connection with video surveillance and no-smoking information– which may differ depending on whether the images are recorded or not. The purposes of the video surveillance and the relevant data controller will have to be specified in all cases. The format of the information should be adjusted to the individual location.

Information must be given to employees and every other person working on the premises. This should include the identity of the controller and the purpose of the surveillance and other information necessary to guarantee fair processing in respect of the data subject, for instance in which cases the recordings would be examined by the management of the organisation, the recording period and when the recording would be disclosed to the law enforcement authorities.

Finally, specific attention should be given to the appropriate way to furnish blind persons with the information.

STORAGE AND RETENTION

Section 26(d) of the Data Protection Act states that personal data shall *"not be kept for longer than is necessary for the purposes for which such data has been collected and processed"*. A data controller is required to justify the retention period. For a normal security system, it would be difficult to justify retention beyond for instance, two months, except where the images identify an issue – such as a break-in or theft - and is retained specifically in the context of an investigation of that issue.

Recorded images should be stored in such a way that the integrity of the image is secured as it may be needed for evidence in a court, for instance. Thus, appropriate technology affording the data controller the possibility to take copies of a recording without interrupting the operation of the system should be used.

The viewing of recorded images should be effected in a secure area restricted to authorised personnel only.

The Data Protection Act does not prescribe any minimum or maximum retention periods which apply to all systems. Each organisation should adopt a retention policy which reflects the needs and requirements of the organization. Images should not be retained longer than is strictly necessary to fulfill the purposes for which they were meant to be recorded. A data controller should be able to decide, based on the needs of its organisation, as to what would be the shortest period it would require to retain those images. The retention policy should also be explained to those responsible for operating the system. Measures should be put in place to ensure the permanent deletion of images through secure methods at the end of the specified period and regular checks are to be carried out.

The storage medium should be stored in a secure environment with a log of access kept. Access should be restricted to authorised personnel. Images should not be retained for longer than is necessary. Once a retention period has expired, images must be erased.

While retained, the integrity of the images must be maintained to ensure their evidential value and/or to protect the rights of the people whose images have been recorded. If images are to be held for evidential purposes, they should be kept in a secure place with controlled access away from other routine data.

Documented procedures should be put in place for removing the medium on which the images have been recorded as follows:-

- The date and time of removal
- The names of the person removing the images and the outcome, if any, of the viewing
- The name(s) of the person(s) viewing the images and the organisation(s) they represent
- The reason/s why they were removed
- Any crime incident number to which the images are relevant
- The date and time that images were returned to the system (or secure place if they have been retained for evidential purposes)
- The location of the images
- The signature of the collecting officer;

All operators to be trained in their responsibilities so they are aware of the user's security and disclosure policies and the rights of individuals.

DISCLOSURE OF CCTV IMAGES TO THIRD PARTIES

Access to, and the disclosure of, CCTV images and the disclosure of images to third parties should be restricted and carefully controlled to ensure the rights of individuals are protected. The chain of evidence must remain intact if the images are required for evidential purposes. Reasons for the disclosure of the images must be compatible with the purpose for which the images were originally recorded.

- Access to the images should be restricted only to those who need access to fulfill the purpose of the system
- All access should be documented;
- Disclosure should be made in limited and prescribed purposes;

ACCESS REQUESTS BY DATA SUBJECTS

Under section 41 of the DPA, individuals whose images are recorded have a right to view the images of themselves and be provided with a copy of them. The data controller must in place internal procedures to be able to handle these requests.

If images of third parties are contained in that document, the data controller must obscure, disguise and blur the images of third parties where appropriate to avoid an unfair intrusion into the privacy of these people where it may occur. In giving a person a copy of his/her data, the data controller may provide a still/series of still pictures, a tape or a disk with relevant images.

A data controller may refuse any request for information where the request falls under section 43 of the DPA and where he is unable to comply to the request as provided in section 42 of the DPA. Clear guidance should be put in place to determine the appropriateness of making a disclosure, which should in any case be restricted to genuine requests as a wide disclosure may be unfair to the individuals concerned in the images and a record of when the disclosure has been effected and the reasons for such disclosure.

Any person whose image has been recorded has a right to be given a copy of the information recorded. To exercise that right, a person must make an application in writing named the "request for access to personal data form". A data controller should charge Rs 75 for responding to such a request and must respond within 28 days, subject to certain exceptions provided in section 42 of the DPA.

Practically, a person should provide necessary information to a data controller, such as the date, time and location of the recording. If the image is of such poor quality as not to clearly identify an individual, that image may be considered not to be personal data.

The procedures put in place should ensure the following:-

1 When data subjects make a request for accessing their information, those operating the system must be able to recognise such a request.

2 Written information should be given to individuals of the types of images retained, their purpose and the policy concerning disclosure in relation to those images.

3 A designated person should deal with all subject access.

4 The images requested should be located by the designated person.

5 The designated person should make the decision whether disclosure also entails disclosure to a third party.

6 The designated person should determine the decision as to whether the images of third parties are held under a duty of confidentiality.

7 The designated person must ensure that third party images are disguised if third party images are not to be disclosed.

8 An editing company may be used if the system does not have the capability to comply with standard 7 above.

9 All requests for access should be recorded and reasons for any denials;

10 There are procedures for allowing access or disclosure:-

11 When access to or disclosure of the images is allowed then the following should be documented:

- The date and time of access or disclosure;
- Identification of third party to whom access or disclosure is allowed;
- The reason for allowing access or disclosure;
- The extent of information to which access or disclosure is allowed.

12 Recorded images should not be made widely available e.g. on an intranet site;

13 If the images are made widely available, the decision should be made by a designated person and the reasons documented;

14 If the images are disclosed to the media for instance, the images of individuals will need to be disguised to avoid identification;

15 If the system does not have the capability to comply with standard 8 above, a data processor, i.e. an editing company may be hired:-

The procedures to be followed when an editing company is hired are as follows:-

- There must be a contractual relationship between the data controller and the editing company;
- The editing company must provide the appropriate guarantees regarding the security measures taken in relation to the images;
- The designated person must carry out checks to ensure the guarantees are met
- The written contract must make it explicit that the editing company should only use the images in accordance with the instructions of the designated person;
- The written contract must make the security guarantees provided by the editing company explicit.

If the Police require the CCTV images for a specific investigation, it is up to the data controller to satisfy himself that there is a genuine investigation underway.

16 If it is decided by a designated person that an access is not to be complied with, the following should be documented:

- The date of the request;
- The identity of the person making the request;
- Why the request to supply the images was refused;
- The name and signature of the designated person making the decision.

17 All staff should be trained as to what are the individuals' rights under section 41.

18 If disclosure is made, it should be in private with only authorised staff present

19 The Data Subject is entitled to a copy of his data in intelligible format.

20 Where there is a request from an individual to prevent processing likely to cause unwarranted and substantial damage to him, all operators must be able to recognise such a request:-

- When such requests are made, all staff must be aware of the designated person who should respond to them.
- The response from the designated person must indicate whether they will comply with such requests.
- There must be a response in writing within 28 days of the designated person receiving the request.
- The designated person must give written reasons if the request cannot be complied with as provided in section 41.
- A copy of the request and response must be kept.
- The designated person must notify the individual if an automated decision is made.
- If the individual makes a request in writing within 28 days the designated person must reconsider an automated decision.
- The designated person must document the original decision, the request from the individual and their response to the request.
- Data Subjects can take court action to prevent unlawful processing.
- Data Subjects can claim compensation for "damage" suffered as a result of breaches of this Act.

Action Surrounding Subject Access Requests, Complaints and Audits

- The contact point indicated on the sign should be available to members of the public during office hours. Employees staffing the contact point should be aware of the appropriate policies and procedures.
- Specific documentation should be provided to each enquiry.
- A complaints procedure should be clearly documented.
- A record of the number and nature of complaints or enquiries received should be kept together with an outline of the action taken.
- A designated person should undertake regular reviews of the documented procedures and make a report.
- An internal annual assessment should be undertaken.

COVERT SURVEILLANCE

The use of recording mechanisms to obtain data without an individual's knowledge is generally unlawful. Covert surveillance is normally only permitted on a case by case basis where the data are kept for the purposes of preventing, detecting or investigating offences, or apprehending or prosecuting offenders.

Where it is allowed, covert surveillance must be focused and of short duration. Only specific (and relevant) individuals/locations should be recorded. If no evidence is obtained within a reasonable period, the surveillance should cease.

If the surveillance is intended to prevent crime, overt cameras may be considered to be a more appropriate measure, and less invasive of individual privacy.

SECURITY MEASURES

Appropriate security and organisational measures would include:-

- Sufficient safeguards to protect wireless transmission systems from interruption.
- The ability to make copies of images to be restricted to appropriate and authorised staff.
- Copies should be safely delivered to the intended recipients.
- To Secure Control Rooms and the area where images are stored.

Whenever video surveillance is only aimed at preventing, detecting and controlling offences, the solution consisting in the use of two access keys – of which one would be held by the controller and the other one by the police – may prove useful in many cases to ensure that images are only viewed by police staff rather than by unauthorised staff – without prejudice to the data subject's legitimate exercise of his right of access by means of a request made during the short image retention period.

Appropriate security measures should be implemented, including dissemination of information that may be helpful to protect a right of the data subject, a third party or the data controller himself – also with a view to preventing manipulation, alteration or destruction of data and related items of evidence.

Finally, it is fundamental for the operators concretely involved in video surveillance activities to be adequately trained in and made aware of the steps to be taken to fully comply with the relevant requirements. Training of controllers and operators, also related to the relevant risks and the mechanisms correctly identifying the imaged individuals, can be considered to be a useful measure as well.

Security companies that place and operate cameras on behalf of clients are considered to be "Data Processors". As data processors, they operate under the instruction of data controllers (their clients). Sections 27(3), (4) & (5), 28 and 29 of the Data Protection Act place a number of obligations on data processors.

These include having appropriate security and organisational measures in place to prevent unauthorised access to, or alteration of, disclosure of, accidental loss, and destruction of, the data in his control, in particular where the processing involves the transmission of data over a network. This obligation can be met by having appropriate access controls to image storage or having robust encryption where remote access to live recording is permitted.

Staff of the security company must be made aware of their obligations relating to the security of data. Staff using the CCTV system should be trained to ensure that they know:

- What are the organisation's policies for recording and retaining images?
- How to handle the images securely?
- What to do when they receive a request for viewing images from data subjects?

Clients of the security company should have a contract in place which details what the security company may do with the data; what security standards should be in place and what verification procedures may apply.

Furthermore, section 33 of the Data Protection Act requires that data processors must have an entry in the public register maintained by the Data Protection Commissioner. For further information, please refer to our Guidance Notes on Registration on our website http://dataprotection.gov.mu. Those who are required to be registered and process data whilst not being registered are committing a criminal offence and may face prosecution by this office. (This provision will only apply where the data controller can identify the persons whose images are captured.)

DOMESTIC USE OF CCTV SYSTEMS

The processing of personal data kept by an individual and concerned solely with the management of his/her personal, family or household affairs or kept by an individual for recreational purposes is exempt from the data protection principles and Parts V and VI of the Act. This exemption would generally apply to the use of CCTVs in a domestic environment. However, the exemption may not apply if the individual works from home. Where the exemption does apply, a person who objects to the use of a CCTV system – for example, a neighbour who objects to images of her/his property being recorded – may be able to take a civil legal action based on the constitutional right to privacy.

NATIONAL SECURITY

According to section 45 (1) of the DPA, where in the opinion of the Prime Minister, personal data would be required for the purpose of safeguarding national security , they are exempt from the application of the DPA. This exemption will also apply to video surveillance systems being used for the purpose of safeguarding national security.

CONCLUSION

CCTV is a seductive technology which has also become an icon for security. The clarity of the pictures is often excellent, with many systems being able to recognize a cigarette packet at a hundred metres. The systems can often work in pitch blackness, bringing images up to daylight level.

However, surveillance by the public or private sector, as illustrated in George Orwell's novel *Nineteen-Eighty-Four* by the impressive figure of 'Big Brother' should not result in the infringement of privacy rights of individuals.

GOVERNMENT PRINTING DEPARTMENT
MARCH 2010