THE OFFICE OF THE
Data Protection Commissioner

DATA PROTECTION (JERSEY) LAW 2005

CODES OF PRACTICE & GUIDANCE ON THE USE OF CCTV EQUIPMENT

GD6

DATA PROTECTION (JERSEY) LAW 2005:

CODES OF PRACTICE & GUIDANCE ON THE USE OF CCTV EQUIPMENT

PART 1: CODES OF PRACTICE

PART 2: GUIDANCE & INTERPRETATION

Part I: CODES OF PRACTICE

INTRODUCTION

Closed circuit television (CCTV) surveillance is an increasing feature of our daily lives. There is an ongoing debate over how effective CCTV is in reducing and preventing crime, but one thing is certain, its deployment is commonplace in a variety of areas to which members of the public have free access. We might be caught on camera while walking down the high street, visiting a shop or bank or travelling through an airport.

These Codes of Practice & Guidance on the use of CCTV equipment are based on the recommendations of the House of Lords Select Committee on Science and Technology, who expressed their view that if public confidence in CCTV systems was to be maintained there needed to be some tighter control over their deployment and use (5th Report - Digital Images as Evidence).

This document is split into two parts, the first detailing the Codes of Practice for CCTV use. Part 2 gives guidance and interpretative notes which may assist when reading the Codes of Practice.

Regulation of CCTV

There was no statutory basis for systematic legal control of CCTV surveillance over public areas until the Data Protection (Jersey) Law 2005 came into force. The definitions in this new Law are broader than those of the Data Protection (Jersey) Law 1987 and so more readily cover the processing of images of individuals caught by CCTV cameras than did the previous data protection legislation. The same legally enforceable information handling standards as have previously applied to those processing personal data on computer now cover CCTV. An important new feature of the recent legislation is a power to issue a Commissioner's Code of Practice (Article 51(3)(b) Data Protection (Jersey) Law 2005) setting out guidance for the following of good practice.

This code deals with surveillance in areas to which the public have largely free and unrestricted access because, as the House of Lords Committee highlighted, there is particular concern about a lack of regulation and central guidance in this area. Although the Data Protection (Jersey) Law 2005 covers other uses of CCTV this Code addresses the area of widest concern. Many of its provisions will be relevant to other uses of CCTV and will be referred to as appropriate when we develop other guidance.

The Need for Codes of Practice

There are some existing standards that have been developed by representatives of CCTV system operators and, more particularly, the British Standards Institute. While such standards are helpful, they are not legally enforceable. The changes in data protection legislation mean that for the first time legally enforceable standards will apply to the collection and processing of images relating to individuals.

The Code of Practice has the dual purpose of assisting operators of CCTV systems to understand their legal obligations while also reassuring the public about the safeguards that should be in place. It sets out the measures which must be adopted to comply with the Data Protection (Jersey) Law 2005, and goes on to set out guidance for the following of good data protection practice. The Code makes clear the standards which must be followed to ensure compliance with the Data Protection (Jersey) Law 2005 and then indicates those which are not a strict legal requirement but do represent the following of good practice.

Areas not covered by the Codes of Practice

It is not intended that the contents of this Code should apply to:

- Targeted and intrusive surveillance activities, which are covered by the provisions of the forthcoming Regulation of Investigatory Powers Law.
- Use of surveillance techniques by employers to monitor their employees' compliance with their contracts of employment.
- Security equipment (including cameras) installed in homes by individuals for home security purposes.
- Use of cameras and similar equipment by the broadcast media for the purposes of journalism, or for artistic or literary purposes.

Uses for CCTV

Before installing and using CCTV and similar surveillance equipment, users will need to establish the purpose or purposes for which they intend to use the equipment.

This equipment may be used for a number of different purposes – for example, prevention, investigation and detection of crime, apprehension and prosecution of offenders (including use of images as evidence in criminal proceedings), public and employee safety, monitoring security of premises etc.

Business requirements and considerations for the use of CCTV

Establish who is the person(s) or organisation(s) legally responsible for the proposed scheme.

Assess the appropriateness of, and reasons for, using CCTV or similar surveillance equipment (First Data Protection Principle).

Document this assessment process and the reasons for the installation of the scheme.

Establish the purpose of the Scheme (First and Second Data Protection Principle).

Document the purpose of the scheme.

Ensure that the notification lodged with the Office of the Data Protection Commissioner covers the purposes for which this equipment is used

Establish and document the person(s) or organisation(s) who are responsible for ensuring the day-to-day compliance with the requirements of the Code of Practice (if different from above)

Establish and document security and disclosure policies. It is essential that the location of the equipment is carefully considered, because the way in which images are captured will need to comply with the First Data Protection Principle. Detailed guidance on the interpretation of the First Data Protection Principle is provided in Part II, but the standards to be met under the Code of Practice are set out below.

Camera location limitations

The equipment should be sited in such a way that it only monitors those spaces which are intended to be covered by the equipment (First and Third Data Protection Principles).

If domestic areas such as gardens or areas not intended to be covered by the scheme border those spaces which are intended to be covered by the equipment, then the user should consult with the owners of such spaces if images from those spaces might be recorded. In the case of back gardens, this would be the resident of the property overlooked (First and Third Data Protection Principles).

Operators must be aware of the purpose(s) for which the scheme has been established (Second and Seventh Data Protection Principles).

Operators must be aware that they are only able to use the equipment in order to achieve the purpose(s) for which it has been installed (First and Second Data Protection Principles).

If cameras are adjustable by the operators, this should be restricted so that operators cannot adjust or manipulate them to overlook spaces which are not intended to be covered by the scheme (First and Third Data Protection Principles).

If it is not possible physically to restrict the equipment to avoid recording images from those spaces not intended to be covered by the scheme, then operators should be trained in recognising the privacy implications of such spaces being covered (First and Third Data Protection Principles).

For example – individuals sunbathing in their back gardens may have a greater expectation of privacy than individuals mowing the lawn of their front garden.

For example – it may be appropriate for the equipment to be used to protect the safety of individuals when using ATMs, but images of PIN numbers, balance enquiries etc should not be captured.

Fair and lawful use of CCTV equipment

Signs should be placed so that the public are aware that they are entering a zone which is covered by surveillance equipment (First Data Protection Principle).

The signs should be clearly visible and legible to members of the public (First Data Protection Principle)

The size of signs will vary according to circumstances:

For example – a sign on the entrance door to a building society office may only need to be A4 size because it is at eye level of those entering the premises.

For example - signs at the entrances of car parks alerting drivers to the fact that the car park is covered by such equipment will usually need to be large, for example, probably A3 size as they are likely to be viewed from further away, for example by a driver sitting in a car.

Use of CCTV equipment to detect criminal activity

In exceptional and limited cases, if it is assessed that the use of signs would not be appropriate, the user of the scheme must ensure that they have:

a) Identified specific criminal activity.
b) Identified the need to use surveillance to obtain evidence of that criminal activity.
c) Assessed whether the use of signs would prejudice success in obtaining such evidence.
d) Assessed how long the covert monitoring should take place to ensure that it is not carried out for longer than is necessary.
e) Documented (a) to (d) above.

Information so obtained must only be obtained for prevention or detection of criminal activity, or the apprehension and prosecution of offenders. It should not be retained and used for any other purpose.

Audio recording

If the equipment used has a sound recording facility, this should not be used to record conversations between members of the public (First and Third Data Protection Principles).

Quality of the images recorded

It is important that the images produced by the equipment are as clear as possible in order that they are effective for the purpose(s) for which they are intended. This is why it is essential that the purpose of the scheme is clearly identified. For example if a system has been installed to prevent and detect crime, then it is essential that the images are adequate for that purpose. The Third, Fourth and Fifth Data Protection Principles are concerned with the quality of personal data.

If tapes are used, it should be ensured that they are good quality tapes (Third and Fourth Data Protection Principles).

The following guidelines should be observed:

1. Upon installation an initial check should be undertaken to ensure that the equipment performs properly.

2. The medium on which the images are captured should be cleaned so that images are not recorded on top of images recorded previously (Third and Fourth Data Protection Principles).

3. The medium on which the images have been recorded should not be used when it has become apparent that the quality of images has deteriorated. (Third Data Protection Principle).

4. If the system records features such as the location of the camera and/or date and time reference, these should be accurate (Third and Fourth Data Protection Principles).

5. If their system includes such features, users should ensure that they have a documented procedure for ensuring their accuracy.

6. Cameras should be situated so that they will capture images relevant to the purpose for which the scheme has been established (Third Data Protection Principle)

   For example, if the purpose of the scheme is the prevention and detection of crime and/or apprehension and prosecution of offenders, the cameras should be sited so that images enabling identification of perpetrators are captured.

   For example, if the scheme has been established with a view to monitoring traffic flow, the cameras should be situated so that they do not capture the details of the vehicles or drivers.

7. If an automatic facial recognition system is used to match images captured against a database of images, then both sets of images should be clear enough to ensure an accurate match (Third and Fourth Data Protection Principles).

8. If an automatic facial recognition system is used, procedures should be set up to ensure that the match is also verified by a human operator, who will assess the match and determine what action, if any, should be taken (First and Seventh Data Protection Principles).

9. The result of the assessment by the human operator should be recorded whether or not they determine there is a match.

10. When installing cameras, consideration must be given to the physical conditions in which the cameras are located (Third and Fourth Data Protection Principles).

    For example – infrared equipment may need to be installed in poorly lit areas.

11. Users should assess whether it is necessary to carry out constant real time recording, or whether the activity or activities about which they are concerned occur at specific times (First and Third Data Protection Principles)

For example – it may be that criminal activity only occurs at night, in which case constant recording of images might only be carried out for a limited period e.g. 10.00 pm to 7.00 am

12. Cameras should be properly maintained and serviced to ensure that clear images are recorded (Third and Fourth Data Protection Principles)

13. Cameras should be protected from vandalism in order to ensure that they remain in working order (Seventh Data Protection Principle)

14. A maintenance log should be kept.

15. If a camera is damaged, there should be clear procedures for:

    a) Defining the person responsible for making arrangements for ensuring that the camera is fixed.
    b) Ensuring that the camera is fixed within a specific time period (Third and Fourth Data Protection Principle).
    c) Monitoring the quality of the maintenance work.

16. Images, which are not required for the purpose(s) for which the equipment is being used, should not be retained for longer than is necessary. While images are retained, it is essential that their integrity be maintained, to ensure their evidential value and to protect the rights of people whose images may have been recorded. Access to and security of the images must be controlled in accordance with the requirements of the 2005 Law.

Retention of CCTV tapes

Images should not be retained for longer than is necessary (Fifth Data Protection Principle)

For example – publicans may need to keep recorded images for no longer than seven days because they will soon be aware of any incident such as a fight occurring on their premises.

For example – images recorded by equipment covering town centres and streets may not need to be retained for longer than 3l days unless they are required for evidential purposes in legal proceedings.

For example – images recorded from equipment protecting individuals' safety at ATMs might need to be retained for a period of three months in order to resolve customer disputes about cash withdrawals. The retention period of three months is based on the interval at which individuals receive their account statements.

Once the retention period has expired, the images should be removed or erased (Fifth Data Protection Principle).

If the images are retained for evidential purposes, they should be retained in a secure place to which access is controlled (Fifth and Seventh Data Protection Principles).

On removing the medium on which the images have been recorded for the use in legal proceedings, the operator should ensure that they have documented:

a) The date on which the images were removed from the general system for use in legal proceedings.
b) The reason why they were removed from the system.
c) Any crime incident number to which the images may be relevant.
d) The location of the images. For example- if the images were handed to a police officer for retention, the name and station of that police officer. The signature of the collecting police officer, where appropriate (see below) (Third and Seventh Data Protection Principles).

Viewing of CCTV images

Monitors displaying images from areas in which individuals would have an expectation of privacy should not be viewed by anyone other than authorised employees of the user of the equipment (Seventh Data Protection Principle).

Access to the recorded images should be restricted to a manager or designated member of staff who will decide whether to allow requests for access by third parties in accordance with the user's documented disclosure policies (Seventh Data Protection Principle).

Viewing of the recorded images should take place in a restricted area, for example, in a manager's or designated member of staff's office. Other employees should not be allowed to have access to that area when a viewing is taking place (Seventh Data Protection Principle).

Removal of the medium on which images are recorded, for viewing purposes, should be documented as follows:

a) The date and time of removal
b) The name of the person removing the images
c) The name(s) of the person(s) viewing the images. If this should include third
d) parties, this include the organisation of that third party
e) The reason for the viewing
f) The outcome, if any, of the viewing

g) The date and time the images were returned to the system or secure place, if they have been retained for evidential purposes

Staff training in the correct use of CCTV equipment

All operators and employees with access to images should be aware of the procedures which need to be followed when accessing the recorded images (Seventh Data Protection Principle).

All operators should be trained in their responsibilities under this Code of Practice i.e. they should be aware of:

a) The user's security policy e.g. procedures to have access to recorded images.
b) The user's disclosure policy.
c) Rights of individuals in relation to their recorded images. (Seventh Data Protection Principle)

It is important that access to, and disclosure of, the images recorded by CCTV and similar surveillance equipment is restricted and carefully controlled, not only to ensure that the rights of individuals are preserved, but also to ensure that the chain of evidence remains intact should the images be required for evidential purposes. Users of CCTV will also need to ensure that the reason(s) for which they may disclose copies of the images are compatible with the reason(s) or purpose(s) for which they originally obtained those images. These aspects of this Code are to be found in the Second and Seventh Data Protection Principles. However, the standards required by this Code are set out below:

1. All employees should be aware of the restrictions set out in this code of practice in relation to access to, and disclosure of, recorded images.

2. Access to recorded images should be restricted to those staff who need to have access in order to achieve the purpose(s) of using the equipment (Seventh Data Protection Principle).

3. All access to the medium on which the images are recorded should be documented (Seventh Data Protection Principle).

4. Disclosure of the recorded images to third parties should only made in limited and prescribed circumstances (Second and Seventh Data Protection Principles). For example - if the purpose of the system is the prevention and detection of crime, then disclosure to third parties should be limited to the following:

- Law enforcement agencies where the images recorded would assist in a specific criminal enquiry
- Prosecution agencies
- Relevant legal representatives
- The media, where it is decided that the public's assistance is needed in order to assist in the identification of victim, witness or perpetrator in relation to a criminal incident. As part of that decision, the wishes of the victim of an incident should be taken into account
- People whose images have been recorded and retained (unless disclosure to the individual would prejudice criminal enquiries or criminal proceedings)

5. All requests for access or for disclosure should be recorded. If access or disclosure is denied, the reason should be documented (Seventh Data Protection Principle)

6. If access to or disclosure of the images is allowed, then the following should be documented:

   a) The date and time at which access was allowed or the date on which disclosure was made
   b) The identification of any third party who was allowed access or to whom disclosure was made
   c) The reason for allowing access or disclosure
   d) The extent of the information to which access was allowed or which was disclosed

7. Recorded images should not be made more widely available – for example they should not be routinely made available to the media or placed on the Internet (Second, Seventh and Eighth Data Protection Principles).

8. If it is intended that images will be made more widely available, that decision should be made by the manager or designated member of staff. The reason for that decision should be documented (Seventh Data Protection Principle).

9. If it is decided that images will be disclosed to the media (other than in the circumstances outlined above), the images of individuals will need to be disguised or blurred so that they are not readily identifiable (First, Second and Seventh Data Protection Principles).

10. If the system does not have the facilities to carry out that type of editing, an editing company may need to be hired to carry it out.

11. If an editing company is hired, then the manager or designated member of staff needs to ensure that:

a) There is a contractual relationship between the data controller and the editing company.
b) That the editing company has given appropriate guarantees regarding the security measures they take in relation to the images.
c) The manager has checked to ensure that those guarantees are met
d) The written contract makes it explicit that the editing company can only use the images in accordance with the instructions of the manager or designated member of staff.
e) The written contract makes the security guarantees provided by the editing company explicit. (Seventh Data Protection Principle)

12. If the media organisation receiving the images undertakes to carry out the editing, then (a) to (e) will still apply (Seventh Data Protection Principle)

Subject Access to CCTV recordings

All staff involved in operating the equipment must be able to recognise a request for access to recorded images by data subjects (Sixth and Seventh Data Protection Principles).

An individual may have to provide dates and times of when they visited the premises of the user of the equipment.

Data subjects should be provided with a standard subject access request form which:

a) Indicates the information required in order to locate the images requested.
b) Indicates the information required in order to identify the person making the request. For example – if the individual making the request is unknown to the user of the equipment, a photograph of the individual may be requested in order to locate the correct image.
c) Indicates the fee that will be charged for carrying out the search for the images requested. A maximum of £10.00 may be charged for the search.
d) Asks whether the individual would be satisfied with merely viewing the images recorded.
e) Indicates that the response will be provided promptly and in any event within 40 days of receiving the required fee and information.
f) Explains the rights provided by the 2005 Law.

Individuals should also be provided with a leaflet which describes the types images which are recorded and retained, the purposes for which those images are recorded and retained, and information about the

disclosure policy in relation to those images (Sixth Data Protection Principle).

This should be provided at the time that the standard subject access request form is provided to an individual (Sixth Data Protection Principle).

All subject access requests should be dealt with by a manager or designated member of staff. The manager or designated member of staff should locate the images requested

The manager or designated member of staff should determine whether disclosure to the individual would entail disclosing images of third parties (Sixth Data Protection Principle).

The manager or designated member of staff will need to determine whether the images of third parties are held under a duty of confidence (First and Sixth Data Protection Principle). For example - it may be that members of the public whose images have been recorded when they were in town centres or streets have less expectation that their images are held under a duty of confidence than individuals whose images have been recorded in more private space such as the waiting room of a doctor's surgery.

If third party images are not to be disclosed, the manager or designated member of staff shall arrange for the third party images to be disguised or blurred (Sixth Data Protection Principle).

If the system does not have the facilities to carry out that type of editing, a third party or company may be hired to carry it out.

If a third party or company is hired, then the manager or designated member of staff needs to ensure that:

On receipt of a request to reconsider the automated decision, the manager or designated member of staff shall respond within 21 days setting out the steps that they intend to take to comply with the individual's request.

The manager or designated member of staff shall document:

a) The original decision.
b) The request from the individual.
c) Their response to the request from the individual.

On-going compliance with the code of practice

Businesses should take note of the following advice:

- The contact point indicated on the sign should be available to members of the public during office hours. Employees staffing that contact point should be aware of the policies and procedures governing the use of this equipment.

- Enquiries should be provided on request with one or more of the following:

  a) The leaflet which individuals receive when they make a subject access request as general information
  b) A copy of this code of practice
  c) A subject access request form if required or requested
  d) The complaints procedure to be followed if they have concerns about the use of the system
  e) The complaints procedure to be followed if they have concerns about non-compliance with the provisions of this Code of Practice

- A complaints procedure should be clearly documented.

- A record of the number and nature of complaints or enquiries received should be maintained together with an outline of the action taken.

- A report on those numbers should be collected by the manager or designated member of staff in order to assess public reaction to and opinion of the use of the system.

- A manager or designated member of staff should undertake regular reviews of the documented procedures to ensure that the provisions of this Code are being complied with (Seventh Data Protection Principle).

- A report on those reviews should be provided to the data controller(s) in order that compliance with legal obligations and provisions with this Code of Practice can be monitored.

- An internal annual assessment should be undertaken which evaluates the effectiveness of the system.

- The results of the report should be assessed against the stated purpose of the scheme. If the scheme is not achieving its purpose, it should be discontinued or modified.

- The result of those reports should be made publicly available.

Part II: GUIDANCE & INTERPRETATION

Glossary

There are several definitions in Articles 1 and 2 of the 2005 Law which users of CCTV systems or similar surveillance equipment must consider in order to determine whether they need to comply with the requirements of the 2005 Law, and if so, to what extent the 2005 Law applies to them:

Definitions:

a) Data Controller

"A person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed".

For example: if a police force and local authority enter into a partnership to install CCTV in a town centre with a view to: -

- Preventing and detecting crime.
- Apprehending and prosecuting offenders.
- Protecting public safety.

They will both be data controllers for the purpose of the scheme.

For example- if a police force, local authority and local retailers decide to install a CCTV scheme in a town centre or shopping centre, for the purposes of:

- Prevention or detection crime.
- Apprehending or prosecuting offenders.
- Protecting public safety.

All will be data controllers for the purposes of the scheme. It is the data controllers who should set out the purposes of the scheme (as outlined above) and who should set out the policies on the use of the images.

The data controller(s) may devolve day-to-day running of the scheme to a manager, but that manager is not the data controller - he or she can only manage the scheme according to the instructions of the data controller(s), and according to the policies set out by the data controller(s).

If the manager of the scheme is an employee of one or more of the data controllers, then the manager will not have any personal data protection responsibilities as a data controller. However, the manager should be aware that if he or she acts outside the instructions of the data

controller(s) in relation to obtaining or disclosing the images, they may commit a criminal offence contrary to Article 55 of the 2005 Law, as well as breach their contract of employment.

If the manager is a third party such as a security company employed by the data controller to run the scheme, then the manager may be deemed a data processor.

This is "any person (other than an employee of the data controller) who processes the personal data on behalf of the data controller". If the data controller(s) are considering using a data processor, they will need to consider their compliance with the Seventh Data Protection Principle in terms of this relationship.

b) Personal Data

"Data which relate to a living individual who can be identified:

a) from those data, or
b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller".

The provisions of the 2005 Law are based on the requirements of a European Directive, which at, Article 2, defines, personal data as follows:

"Personal data" shall mean any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

The definition of personal data is not therefore limited to circumstances where a data controller can attribute a name to a particular image. If images of distinguishable individuals' features are processed and an individual can be identified from these images, they will amount to personal data.

c) Sensitive Personal Data

Article 2 of the 2005 Law separates out distinct categories of personal data, which are deemed sensitive. The most significant of these categories for the purposes of this code of practice are information about:

- the data subject's commission or alleged commission of any offences
- any proceedings for any offence committed, or alleged to have been committed, by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.

This latter bullet point will be particularly significant for those CCTV schemes which are established by retailers in conjunction with the local police force, which use other information to identify known and convicted shoplifters from images, with a view to reducing the amount of organised shoplifting.

It is essential that data controllers determine whether they are processing sensitive personal data because it has particular implications for their compliance with the First Data Protection Principle.

d) Processing

Article l of the 2005 Law sets out the type of operations that can constitute processing:

"In relation to information or data, means obtaining, processing, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:

a) organisation, adaptation or alteration of the information or data,
b) retrieval, consultation or use of the information or data,
c) disclosure of the information or data by transmission, dissemination or otherwise making available, or
d) alignment, combination, blocking, erasure or destruction of the information or data."

The definition is wide enough to cover the simple recording and holding of images for a limited period of time, even if no further reference is made to those images. It is also wide enough to cover real-time transmission of the images. Thus if the images of individuals passing in front of a camera are shown in real time on a monitor, this constitutes “transmission, dissemination or otherwise making available.

Thus even the least sophisticated capturing and use of images falls within the definition of processing in the 2005 Law.

Purposes for which personal data/images are processed

Before considering compliance with the Data Protection Principles, a user of CCTV or similar surveillance equipment, will need to determine two issues:

- What type of personal data are being processed i.e. are there any personal data which fall within the definition of sensitive personal data as defined by Article 2 of the 2005 Law.
- For what purpose(s) are both personal data and sensitive personal data being processed?

Users of surveillance equipment should be clear about the purposes for which they intend to use the information/images captured by their equipment. The equipment may be used for a number of purposes:

- Prevention, investigation and/or detection of crime.
- Apprehension and/or prosecution of offenders (including images being entered as evidence in criminal proceedings).
- Public and employee safety.
- Staff discipline.
- Traffic flow monitoring.

Using information captured by a surveillance system will not always require the processing of personal data or the processing of sensitive personal data. For example, use of the system to monitor traffic flow in order to provide the public with up to date information about traffic jams, will not necessarily require the processing of personal data.

Data protection principles

The First Data Protection Principle

This requires that "Personal data shall be processed fairly and lawfully, and, in particular, shall not be processed unless:

a) at least one of the conditions in Schedule 2 is met, and
b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met".

The definition of sensitive personal data has been discussed above and it is essential that the data controller has determined whether they are processing information/images which fall into that category in order to assess which criteria to consider when deciding whether there is a legitimate basis for the processing.

To assess compliance with this Principle, it is recommended that the data controller address the following questions:

a) Are personal data and/or sensitive personal data processed?
b) Has a condition for processing been met?

The First Data Protection Principle requires that the data controller have a legitimate basis for processing. It is for the data controller to be clear about which grounds to rely on in this respect. These are set out in Schedules 2 and 3 to the Law.

Users of schemes which monitor spaces to which the public have access, such as town centres, may be able to rely on Paragraph 5 (d) of Schedule 2 because the processing is for the exercise of any other function of a public nature exercised in the public interest by any person. This could

include purposes such as prevention and detection of crime, apprehension and prosecution of offenders or public/employee safety.

Users of schemes which monitor spaces in shops or retail centres to which the public have access may be able to rely on Paragraph 6(l) of Schedule 2 because the processing is necessary for the purposes of legitimate interests pursued by the data controller or the third party or third parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.

It should be noted that while this criterion may provide a general ground for processing, in an individual case, the interests of the data controller, i.e. the user of the surveillance equipment, might not outweigh the rights of an individual.

If the data controller has determined that he or she is processing sensitive personal data, then the data controller will also need to determine whether he or she has a legitimate basis for doing so under Schedule 3. It should be noted that Schedule 3 does not contain the grounds cited above in relation to Schedule 2.

Users of surveillance equipment in town centre, particularly where the Parish or police force (or a partnership of the two) are the data controllers may be able to rely on Paragraph 7(b) of Schedule 3 because the processing is necessary for the exercise of any functions conferred on any person by or under an enactment.

Users of information/images recorded in a shop or retail centre may also be able to rely on one of the grounds contained in the Regulations made under Schedule 3(10) of the 2005 Law.

For example:

“The processing:

a) is in the substantial public interest;
b) is necessary for the purposes of the prevention and detection of any unlawful act; and
c) must necessarily be carried out without the explicit consent of the data subject so as not to prejudice those purposes”

It is for the data controller to be sure that he or she has legitimate grounds for their processing and therefore it is essential that the data controller has identified:

- what categories of data are processed, and
- why.

d) Are the information/images processed lawfully?

The fact that the data controller has a legitimate basis for processing does not mean that this element of the First Data Protection Principle is automatically satisfied. The data controller will also need to consider whether the information/images processed are subject to any other legal duties or responsibilities such as the common law duty of confidentiality. Public sector bodies will need to consider their legal powers under administrative law in order to determine whether there are restrictions or prohibitions on their ability to process such data.

They will also need to consider the implications of the Human Rights (Jersey) Law 2000 which is due to be implemented.

e) Are the information/images processed fairly?

The fact that a data controller has a legitimate basis for processing the information/images will not automatically mean that this element of the First Data Protection Principle is satisfied.

The interpretative provisions of the Law set out what is required in order to process fairly. In order to process fairly, the following information, at least, must be provided to the individuals at the point of obtaining their images:

- the identity of the data controller
- any information which is necessary, having regard to the specific circumstances in which the data are or are to be processed, to enable processing in respect of the individual to be fair.
- the identity of a representative the data controller has nominated for the purposes of the Law.
- the purpose or purposes for which the data are intended to be processed, and the Law does not make specific reference to the use of covert processing of (sensitive) personal data but it does provide a limited exemption from the requirement of fair processing. Because fair processing (as indicated above) requires that individuals are made aware that they are entering an area where their images may be captured, by the use of signs, it follows that the use of covert processing i.e. removal or failure to provide signs, is prima facie a breach of the fairness requirement of the First Data Protection Principle. However, a breach of this requirement will not arise if an exemption can be relied on.

Such an exemption may be found at Article 29(l) of the Law, which states that:

“Personal data processed for any of the following purposes:

- prevention or detection of crime
- apprehension or prosecution of offenders are exempt from the first data protection principle (except to the extent to which it requires

compliance with the conditions in Schedules 2 and 3) ... in any case to the extent to which the application of those provisions to the data would be likely to prejudice any of the matters mentioned..."

This means that if the data controller processes images for either or both of the purposes listed in the exemption, he or she may be able to obtain and process images without signs without breaching the fairness requirements of the First Data Protection Principle.

The Second Data Protection Principle

This requires that "Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes".

In order to ascertain whether the data controller is complying with this Data Protection Principle, it is essential that there is clarity about the purpose(s) for which the images are processed.

Specified purposes may be those which have been notified to the Commissioner or to the individuals. There are a number of issues to be considered when determining lawfulness:

- Whether the data controller has a legitimate basis (see First Data Protection Principle) for the processing.
- Whether the images are processed in accordance with any other legal duties to which the data controller may be subject e.g. the common law duty of confidence, administrative law in relation to public sector powers etc.

It is quite clear from the interpretative provisions to the Principle that the requirement of compatibility is particularly significant when considering making a disclosure to a third party or developing a policy on disclosures to third parties. If the data controller intends to make a disclosure to a third party, regard must be had to the purpose(s) for which the third party may process the data.

This means, for example, that if the purpose(s) for which images are processed is:

- Prevention or detection of crime
- Apprehension or prosecution of offenders

The data controller may only disclose to third parties who intend processing the data for compatible purposes. Thus, for example, where there is an investigation into criminal activity, disclosure of footage relating to that criminal activity to the media in order to seek assistance from the public in identifying either the perpetrator, the victim or witnesses, may be appropriate. However, it would be an incompatible use if images from equipment installed to prevent or detect crime were

disclosed to the media merely for entertainment purposes. For example, it might be appropriate to disclose to the media images of drunken individuals stumbling around a town centre on a Saturday night to show proper use of policing resources to combat anti-social behaviour. However, it would not be appropriate for the same images to be provided to a media company merely for inclusion in a "humorous" video. If it is determined that a particular disclosure is compatible with the purposes for which the data controller processes images, then the extent of disclosure will need to be considered. If the footage, which is to be disclosed, contains images of unrelated third parties, the data controller will need to ensure that those images are disguised in such a way that they cannot be identified.

If the data controller does not have the facilities to carry out such editing, he or she may agree with the media organisation that it will ensure that those images are disguised. This will mean that the media organisation is carrying out processing, albeit of a limited nature on behalf of the data controller which is likely to render it a data processor. In which case the data controller will need to ensure that the relationship with the media organisation complies with the Seventh Data Protection Principle.

The Third Data Protection Principle

This requires that "Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed".

This means that consideration must be given to the situation of the cameras so that they do not record more information than is necessary for the purpose for which they were installed. For example cameras installed for the purpose of recording acts of vandalism in a car park should not overlook private residences. Furthermore, if the recorded images on the tapes are blurred or indistinct, it may well be that this will constitute inadequate data. For example, if the purpose of the system is to collect evidence of criminal activity, blurred or indistinct images from degraded tapes or poorly maintained equipment will not provide legally sound evidence, and may therefore be inadequate for its purpose.

The Fourth Data Protection Principle

This requires that "Personal data shall be accurate and, where necessary, kept up to date".

This principle requires that the personal information that is recorded and stored must be accurate. This is particularly important if the personal information taken from the system is to be used as evidence in cases of criminal conduct or in disciplinary disputes with employees. The Commissioner recommends that efforts are made to ensure the clarity of the images, such as using only good quality tapes in recording the information, cleaning the tapes prior to re-use and not simply recording

over existing images, and replacing tapes on a regular basis to avoid degradation from over-use.

If the data controller's system uses features such as time references and even location references, then these should be accurate. This means having a documented procedure to ensure the accuracy of such features are checked and if necessary, amended or altered.

Care should be exercised when using digital-enhancement and compression technologies to produce stills for evidence from tapes because these technologies often contain pre-programmed presumptions as to the likely nature of sections of the image. Thus the user cannot be certain that the images taken from the tape are an accurate representation of the actual scene. This may create evidential difficulties if they are to be relied on either in court or an internal employee disciplinary hearing.

The Fifth Data Protection Principle

This requires that "Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes".

This principle requires that the information shall not be held for longer than is necessary for the purpose for which it is to be used. The tapes that have recorded the relevant activities should be retained until such time as the proceedings are completed and the possibility of any appeal has been exhausted. After that time, the tapes should be erased.

Apart from those circumstances, stored or recorded images should not be kept for any undue length of time. A policy on periods for retention of the images should be developed which takes into account the nature of the information and the purpose for which it is being collected. For example where images are being recorded for the purposes of crime prevention in a shopping area, it may be that the only images that need to be retained are those relating to specific incidents of criminal activity; the rest could be erased after a very short period.

The Commissioner understands that generally town centre schemes do not retain recorded images for more than 28 days unless the images are required for evidential purposes.

The Sixth Data Protection Principle

This requires that "Personal data shall be processed in accordance with the rights of data subjects under this Law".

The Law provides individuals with a number of rights in relation to the processing of their personal data. Contravening the following rights will amount to a contravention of the Sixth Data Protection Principle:

- The right to be provided, in appropriate cases, with a copy of the information constituting the personal data held about them – Article 7.
- The right to prevent processing which is likely to cause damage or distress - Article l0.
- Rights in relation to automated decision-taking - Article 12

The Seventh Data Protection Principle

This requires that "Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data".

In order to assess the level of security the data controller needs to take to ensure compliance with this Principle, he or she needs to assess: -

- the harm that might result from unauthorised or unlawful processing or accidental loss, destruction or damage of the personal data.

While it is clear that breach of this Principle may have a detrimental effect on the purpose(s) of the scheme e.g. the evidence or images might not stand up in court, or the public may lose confidence in your use of surveillance equipment due to inappropriate disclosure, the harm test required by the Law also requires primarily the effect on the people recorded to be taken into account;

- the nature of the data to be protected must be considered. Sensitive personal data was defined at the beginning of this part of the Code, but there may be other aspects, which need to be considered.

For example, a town centre scheme may coincidentally record the image of a couple kissing in a parked car, or a retailer's scheme may record images of people in changing rooms (in order to prevent items of clothing being stolen).

Whilst these images may not fall within the sensitive categories as set in Article 2 (described above), it is clear that the people whose images have been captured will consider that information or personal data should be processed with greater care.

The Eighth Data Protection Principle

This requires that “Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data”.

This Principle places limitations on the ability to transfer personal data to countries and territories outside of the EEA.

It is unlikely that the data controller would want, in general, to make such transfers of personal data overseas, but the data controller should refrain from putting the images on the Internet or on their website. In order to ensure that this Principle is not breached, the data controller should consider the provisions of Schedule 4 of the 2005 Law.

Right of subject access

Upon making a request in writing (which includes transmission by electronic means) and upon paying the fee to the data controller an individual is entitled:

- To be told by the data controller whether they or someone else on their behalf is processing that individual’s personal data.

If so, to be given a description of:

a) the personal data,
b) the purposes for which they are being processed, and
c) those to whom they are or may be disclosed.

- To be told, in an intelligible manner, of:

a) all the information, which forms any such personal data. This information must be supplied in permanent form by way of a copy, except where the supply of such a copy is not possible or would involve disproportionate effort or the individual agrees otherwise. If any of the information in the copy is not intelligible without explanation, the individual should be given an explanation of that information, e.g. where the data controller holds the information in coded form which cannot be understood without the key to the code, and
b) any information as to the source of those data. However, in some instances the data controller is not obliged to disclose such information where the source of the data is, or can be identified as, an individual.

A data controller may charge a fee (subject to a maximum – currently £10.00) for dealing with subject access. A data controller must comply

with a subject access request promptly, and in any event within forty days of receipt of the request or, if later, within forty days of receipt of:

- the information required (i.e. to satisfy himself as to the identity of the person making the request and to locate the information which that person seeks); and
- the fee.

However, unless the data controller has received a request in writing, the prescribed fee and, if necessary, the said information the data controller need not comply with the request. If the data controller receives a request without the required fee and/or information, they should request whichever is outstanding as soon as possible in order that they can comply with the request promptly and in any event within 40 days.

A data controller does not need to comply with a request where they have already complied with an identical or similar request by the same individual unless a reasonable interval has elapsed between compliance with the previous request and the making of the current request. In deciding what amounts to a reasonable interval, the following factors should be considered: the nature of the data, the purpose for which the data are processed and the frequency with which the data are altered.

The information given in response to a subject access request should be all that which is contained in the personal data at the time the request was received. However, routine amendments and deletions of the data may continue between the date of the request and the date of the reply. To this extent, the information revealed to the individual may differ from the personal data which were held at the time the request was received, even to the extent that data are no longer held. But, having received a request, the data controller must not make any special amendment or deletion which would not otherwise have been made. The information must not be tampered with in order to make it acceptable to the individual.

A particular problem arises for data controllers who may find that in complying with a subject access request they will disclose information relating to an individual other than the individual who has made the request, who can be identified from that information, including the situation where the information enables that other individual to be identified as the source of the information. The Law recognises this problem and sets out only two circumstances in which the data controller is obliged to comply with the subject access request in such circumstances, namely:

- where the other individual has consented to the disclosure of the information, or
- where it is reasonable in all the circumstances to comply with the request without the consent of the other individual.

The Law assists in interpreting whether it is reasonable in all the circumstances to comply with the request without the consent of the other individual concerned. In deciding this question regard shall be had, in particular, to:

- any duty of confidentiality owed to the other individual,
- any steps taken by the data controller with a view to seeking the consent of the other individual,
- whether the other individual is capable of giving consent, and
- any express refusal of consent by the other individual.

If a data controller is satisfied that the individual will not be able to identify the other individual from the information, taking into account any other information which, in the reasonable belief of the data controller, is likely to be in (or to come into) the possession of the individual, then the data controller must provide the information.

If an individual believes that a data controller has failed to comply with a subject access request in contravention of the Law they may apply to Court for an order that the data controller complies with the request. An order may be made if the Court is satisfied that the data controller has failed to comply with the request in contravention of the Law.

Exemptions to subject access rights

There are a limited number of exemptions to an individual's right of access. One of potential relevance to CCTV images is found at Article 29 of the Law. This provides an exemption from the subject access rights, which is similar to that discussed in relation to the exemption to the fairness requirements of the First Data Protection Principle. This means that where personal data are held for the purposes of: -

- prevention or detection of crime,
- apprehension or prosecution of offenders,

the data controller will be entitled to withhold personal data from an individual making a subject access request, where it has been adjudged that to disclose the personal data would be likely to prejudice one or both of the above purposes. Like the exemption to the fairness requirements of the First Data Protection Principle, this judgement must be made on a case-by-case basis, and in relation to each element of the personal data held about the individual. It is likely that this exemption may only be appropriately relied upon where the data controller has recorded personal data about an individual in accordance with guidance set out in relation to the fairness requirements of the First Data Protection Principle.

Other rights

Right to Prevent Processing Likely to Cause Damage or Distress

Under Article 10 of the Law, an individual is entitled to serve a notice on a data controller requiring the data controller not to begin, or to cease, processing personal data relating to that individual. Such a notice could only be served on the grounds that the processing in question is likely to cause substantial, unwarranted damage or distress to that individual or another person. There are certain limited situations where this right to serve a notice does not apply. These are where the individual has consented; the processing is in connection with performance of a contract with the data subject, or in compliance with a legal obligation on the data controller, or in order to protect the vital interests of the individual. If a data controller receives such a notice they must respond within 21 days indicating either compliance with the notice or why the notice is not justified.

Rights in Relation to Automated Decision-Taking

Under Article 12 of the Law, individuals also have certain rights to prevent automated decision taking where a decision, which significantly affects them is based solely on automated processing. The Law draws particular attention to decisions taken aimed at evaluating matters such as the individual's performance at work and their reliability or conduct. The Law does provide exemption for certain decisions reached by automated means and these cover decisions which have been taken in the course of contractual arrangements with the individual, where a decision is authorised or required by statute, where the decision is to grant a request of the individual or where steps have been taken to safeguard the legitimate interests of individuals. This latter point may include matters such as allowing them to make representations about a decision before it is implemented.

Where no notice has been served by an individual and a decision which significantly affects the individual based solely on automated processing will be made, then there is still an obligation on the data controller to notify the individual that the decision was taken on the basis of automated processing as soon as reasonably practicable.

The individual may, within 21 days of receiving such a notification, request the data controller to reconsider the decision or take another decision on a new basis. Having received such a notice the data controller has 21 days in which to respond, specifying the steps that they intend to take to comply with the notice.

In the context of CCTV surveillance it may be the case that certain automated decision-making techniques are deployed, such as with automatic facial recognition. It is important therefore that any system takes account of an individual's rights in relation to automated decision taking. It should be noted that these rights are founded on decisions, which are taken solely on the basis of automated processing. If a decision

whether to take particular action in relation to a particular identified individual is taken further to human intervention, then such a decision would not be based solely on automated processing.

The individual's rights to prevent processing in certain circumstances and in connection with automated decision taking are underpinned by an individual's right to seek a Court Order should any notice served by the individual not be complied with.

Compensation for Failure to Comply with Certain Requirements

Under Article 13 of the Law, individuals who suffer unwarranted damage or damage and distress as a result of any contravention of the requirements of the Law are entitled to go to court to seek compensation in certain circumstances. This right to claim compensation for a breach of the Law is in addition to an individual's right to request the Data Protection Commissioner to make an assessment as to whether processing is likely or unlikely to comply with the Law.

CONTACT THE COMMISSIONER:

Enquiries and Publication Requests:
T: 01534 441064
F: 01534 441065
E-Mail: dataprotection@ gov.je
W: www.dataprotection@gov.je

Office of the Data Protection Commissioner
Morier House
Halkett Place
St.Helier
Jersey
JE11DD