THE OFFICE OF THE
DATA PROTECTION
COMMISSIONER

CCTV
GUIDANCE FOR USERS

Overview – Closed Circuit Television (CCTV) is used by many organisations, businesses and private households throughout the Bailiwick of Guernsey. Although its usage is generally considered to be advantageous in the reduction and prevention of crime, concerns have been expressed that it is an intrusion into the privacy of individuals.

The Data Protection (Bailiwick of Guernsey) Law, 2001 ("the Law") provides a means of regulatory control of the use of CCTV systems so that individuals may enjoy security of their safety and possessions whilst being assured that rights to personal privacy will not be unduly compromised. Complying with the Law and adopting good standards of practice will help towards realising these objectives.

The aim of this booklet is to provide guidance on how to achieve compliance. It is intended for those who are responsible for the operation of CCTV and similar surveillance schemes in areas where members of the public have largely free and unrestricted access such as shopping areas, car parks, night clubs, schools, banks, etc.

It does not apply to the following:

- Private householders who use cameras within their own property for personal security
- Cameras and similar equipment used by the media for journalistic, literary or artistic purposes.

Table of Contents

Some Useful Definitions 3

The Data Protection Principles 4

Notification 15

CCTV Small User Checklist: Operation of the CCTV System 16

Contact the Commissioner 18

Some Useful Definitions

There is some terminology that is very specific to data protection and it will be useful at this stage to explain these terms in their relation to CCTV usage.

Data	Information that is processed by equipment operating automatically
Personal data	Data that relate to a living individual who can be identified from those data; someone's image that is recorded on CCTV may therefore be personal data.
Data subject	The individual whose image is recorded.
Sensitive personal data	Where CCTV is concerned the most significant sensitive personal data category is that of the commission or alleged commission of any criminal offence.
Data processing	Monitoring, recording, keeping, storing, viewing, editing and disclosing the images.
Data controller	A person or an organisation who alone or jointly or in common with others determines the purpose(s) for which and the manner in which any personal data are, or are to be, processed. The police, publicans, States Committees, schools, night clubs, banks, shops are all examples of data controllers. Data controllers may operate joint schemes, for instance when the police and retailers within a town area share a purpose of trying to reduce crime.

The Data Protection Principles

The Law is based on eight principles of good information handling practice. A concise and easy to follow checklist to help the data controller establish if the principles are being followed is available at the end of this booklet.

The principles are that data must be:

1. Fairly and lawfully processed

2. Processed for limited purposes and not in any manner incompatible with those purposes

3. Adequate, relevant and not excessive

4. Accurate and, where necessary, kept up to date

5. Not kept for longer than necessary

6. Processed in accordance with individuals' rights

7. Kept secure

8. Not transferred to countries which do not have adequate protection laws unless there are measures in place between the exporting and importing country to ensure adequate protection

Each principle will now be explained in depth.

1st Principle

To comply with the 1st principle there must be a lawful basis for using CCTV systems. The purpose(s) for the use of CCTV must be established prior to it being installed.

In addition, it is essential that at least one of the conditions from Schedule 2 of the Law and for sensitive personal data, such as criminal offences, at least one of the conditions from Schedule 3 of the Law can be relied upon.

The following are the lawful processing conditions for the processing of any personal data :-

- the individual has given his or her consent to the processing;
- the processing is necessary for the performance of a contract with the individual;
- the processing is required under a legal obligation;
- the processing is necessary to protect the vital interests of the individual;
- the processing is necessary to carry out public functions;
- the processing is necessary in order to pursue the legitimate interests of the data controller or third parties (unless it could prejudice the interests of the individual).

The following are the conditions for lawful processing of sensitive personal data that are most likely to be relied upon for the use of CCTV :-

- having the explicit consent of the individual;
- needing to process the information in order to protect the vital interests of the data subjects or another;
- the administration of justice or legal proceedings.

Good practice
Document the reason(s) why CCTV is used and the lawful processing conditions relied upon.

The fairness element of the 1st principle also has to be satisfied. To comply with this requirement the following information must be given to individuals at the point of obtaining their images:

- The identity of the data controller unless this is self evident
- The identity of any local representative nominated by the data controller
- The purposes for the use of CCTV
- Any other necessary information to do with the specific processing of the information.

Signs must be placed in a prominent position to inform the public that they are entering an area where their images are being recorded.

If the sign contains an image of a camera then it need only state who the data controller is and give a contact number where further information can be obtained. If no image is depicted then it must state that CCTV is being used and the purpose of its use.

The signs must be legible, there is no specified colour but they are traditionally yellow and black.

Good practice
- Signs on doors to buildings should be at least A4 size and at eye level of those entering the building;

- Signs to car parks should be bigger, A3 size being acceptable.

Permission to erect signs may be required from the Development & Planning Authority.

2nd Principle

It will be a breach of the 2nd principle if data are used for purposes for which they were not originally intended. For example if a night club informs clients that CCTV is used to detect perpetrators of hooliganism and the film footage is later used as part of an advertising campaign, then the clients may, under the Law, claim that the club has violated the 2nd principle as the clients' personal data were used in a manner which was incompatible with the original purpose.

Prior to disclosing recordings to any third party the data controller should establish that information will only be used for the purpose(s) for which it was obtained. Where the purpose is for the prevention and detection of crime then the third parties should be limited to:

- Law enforcement agencies
- Prosecution agencies
- Legal representatives

Good practice
Document the following:

- Date and time disclosure was made
- Name of any third party to whom disclosure was made
- The reason for disclosure
- The extent of the information disclosed

If recordings are released to the media so that alleged perpetrators of crime can be identified by the public then it is necessary to blur or disguise the images of any third parties.

Good practice
If the data controller does not have the skills to do this then an editing company should be hired

It is a legal requirement that if a data controller uses an editing company then a contract which binds the editing company to the same legal obligations as the data controller is entered into.

3rd Principle

Data controllers must give careful consideration to where the CCTV cameras are sited as the 3rd principle states that processing of personal data must be adequate, relevant and not excessive.

Again the purposes why the cameras are used should be considered and the data controller must ensure the operators are aware of these purposes. Enough information should be recorded to meet the purposes but they must not record information that exceeds the purposes

This means that care has to be taken as to where the cameras are situated. For example if a supermarket installs them to detect acts of vandalism to customers' cars they should not record callers to a neighbouring property such as a doctor's surgery. Such processing is excessive and irrelevant and will not only breach the 3rd principle but also the 1st principle.

In the event that it may not be possible to avoid filming an adjoining property then the owners should be consulted as to whether or not images from that property might be recorded.

Furthermore if the recorded images on the tapes are blurred or indistinct then they may well be inadequate to be produced as evidence in court, and so the intended purpose will not have been served.

It is important that staff operating the equipment are made aware of why it is used and that they are well trained not just in its operation but also in the privacy implications of filming spaces not covered by the scheme.

4th Principle

The 4th principle states that personal data should be accurate and where necessary kept up to date. CCTV recordings could be used as evidence during criminal proceedings or during disciplinary disputes with employees. It is essential that images recorded are clear and accurate. If the system uses features such as time references and / or location references then obviously these too must be accurate.

Data controllers must ensure that equipment is in good working order, good quality tapes are used, and that they are properly cleaned instead of images being recorded on top of images. Tapes should not be reused if it becomes apparent that the quality of images is deteriorating

When an automatic facial recognition system is used to match images captured against a database of images then both sets must be clear enough to ensure an accurate match and the result of the assessment must be verified by a human operator.

Attention must also be paid to the physical condition in which the system is operated, e.g. infrared equipment should be used in poorly lit areas.

The maintenance of the system is therefore a priority and if it is damaged in any way it should be repaired within a specific time period.

Good practice

- Designate a person, if possible, to maintain the system
- Keep a maintenance log

5th Principle

To comply with the 5th principle 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 is maintained, this is to ensure accuracy of the data as advocated by the 4th principle.

To decide on how long images should be retained the data controller must consider the purposes of the processing.

For instance a publican may need to keep the images for no longer than 7 days as they will soon be aware of any incidents, such as a fight, on their premises.

Images recorded by equipment covering a main street may not need to be retained for longer than 31 days unless they are required as evidence in legal proceedings.

Images recorded from equipment protecting individuals' safety and security at ATMs (automatic cash dispensers) might need to be retained for a period of 3 months in order to resolve customer disputes about cash withdrawals. The retention period of 3 months is based on the normal interval at which most individuals receive their account statements.

Every data controller can decide on what is the most suitable retention period for the purposes of their business or organisation. Once the retention period has expired the tapes should be cleaned or erased.

If they are needed as evidence for legal proceedings they should be stored in a secure place to which access is controlled.

6th Principle

The Law states that individuals may have access to their personal data and as previously mentioned their images are construed as personal data as they may be identified from those images.

An individual may make a subject access request to the data controller for a copy of the recording of his or her image. In certain circumstances a subject access request can be denied; this would be if the release of the recording would be likely to prejudice the purposes of the prevention and detection of crime and the apprehension or prosecution of offenders.

A data subject must put their request in writing and forward a fee of £10 to the data controller. The data must be supplied within 60 days and this period will not begin until the written request and fee has been received, provided there is no undue delay in requesting the fee.

An up to date photograph which is a true likeness may have to be supplied by the data subject to enable designated staff of the data controller to effect positive identification.

It is helpful for the data subject to supply a date and (approximate) time as to when the recording was made otherwise considerable time and effort might have to be spent by the data controller in retrieving the data.

It is emphasised that subject access requests cannot be denied due to the expense incurred by a data controller for tapes to be edited and copied; in deciding to use CCTV systems the data controller must accept the right of individuals to access their recorded personal data.

Good practice

- A designated member of staff, if possible, should be responsible for dealing with subject access requests.
- An information leaflet should be available for data subjects.
- A standard subject access request form could be made available

7th Principle

The 7th principle requires data controllers to consider the harm that data subjects could experience due to the lack of and / or inappropriate security measures. The nature of the personal data is a significant factor in assessing the degree of harm that could result.

If a data controller makes an unauthorised disclosure of the recordings then public confidence in that data controller could be adversely affected. When recordings are lost, destroyed or damaged then reliable evidence will be unavailable for court proceedings thus possibly resulting in justice not being upheld.

Images that are held for evidential purposes must be stored securely and back up tapes stored in an alternative secure environment.

Access to the recordings should be restricted to a manager or designated member of staff.

Viewing of the images should take place in a restricted area, e.g. in the manager's or designated member of staff's office. Other employees should be disallowed access when viewing is taking place.

Good practice
Document the following

- Date and time of removal of tapes for viewing
- Name of the person removing the tapes
- Name(s) of the person(s) viewing the images
- Reason for the viewing
- Outcome, if any, of the viewing
- Date and time images returned to secure place if they are to be retained for evidential purposes.

As previously mentioned any images of individuals committing offences or alleged offences are defined as sensitive personal data under the Law. However, many individuals may feel that CCTV monitors and records them in locations and situations which they consider to be sensitive. For instance they could be in a doctor's waiting room, in a retailer's changing room or even sunbathing in their gardens. Needless to say individuals could suffer some degrees of distress if restrictions are not placed on who has access.

8th Principle

This principle requires the data controller not to export any recorded images to countries outside the Bailiwick of Guernsey unless adequate protection is in place. Our international transfers guidance goes into more detail of this requirement.

While transfers of CCTV are unlikely the Commissioner would remind data controllers that they should refrain from putting CCTV images on the Internet or their websites.

There are certain exceptions to the 8th principle and these are:

- If the data subject has given consent to the transfer
- If the transfer is necessary for the entering into, the performance or the conclusion of a contract.
- Where substantial public interest is concerned, e.g. if the images can help identify terrorists.
- To provide evidence for legal proceedings.
- Where the vital interests of the data subject or another person are at stake.

Notification

Data controllers must by law notify the Data Protection Commissioner of their use of CCTV; it is a criminal offence not to do this. The notification must include the following information:

1. The identity of the data controller
2. The purpose(s) for the use of CCTV
3. A description of data subjects, e.g. customers, pupils, suspected offenders
4. A description of the types of data being processed, e.g. offences
5. A description of any person or organization that the images are passed to, e.g. police, law courts
6. The security measures in place to protect the images
7. Whether images are transferred outside the Bailiwick of Guernsey

This information is kept on a public register maintained by the Data Protection Commissioner. The register can be viewed on line at www.dataci.org.

The notification is renewable on an annual basis. It is an offence liable to prosecution not to notify; it is also an offence for a data controller not to notify the Commissioner about any changes in his processing. The notification fee is £50, there is no fee to remove or alter a register entry.

CCTV Small User Checklist: Operation of the CCTV System

This CCTV equipment and the images recorded by it are controlled by …… who is responsible for how the system is used and for the notifying the Data Protection Commissioner about the CCTV system and its purpose (this is a legal requirement of the Data Protection (Bailiwick of Guernsey) Law, 2001.

The above controller has considered the need for using a CCTV system and has decided it is required for the prevention and detection of crime and for protecting the safety of customers. It will not be used for other purposes.

	Checked (Date)	By	Date of next review
The controller is aware that notification to the Data Protection Commissioner is necessary and must be renewed annually.			
Notification has been submitted to the Data Protection Commissioner and the next renewal date recorded			
Cameras have been sited so that their images are clear enough to allow the police to use them to investigate a crime.			
Cameras have been positioned to avoid capturing the images of persons not visiting the premises.			
There are signs showing that a CCTV system is in operation visible to people visiting the premises and the controllers contact details are displayed on the sign where it is not obvious who is responsible for the system.			
The recorded images from this CCTV system are securely stored, where only a limited number of authorised persons may have access to them			

The recorded images will only be retained long enough for any incident to come to light (e.g. for a theft to be noticed).			
Recordings will only be made available to law enforcement agencies involved in the prevention and detection of crime, and no other third parties.			
The operating equipment is regularly checked to ensure that it is working properly (e.g. the recording media used is of an appropriate standard and that features on the equipment such as the date and time stamp are correctly set).			
The controller knows how to respond to requests from individuals for access to images relating to that individual. If unsure the controller knows to seek advice from the Data Protection Commissioner as soon as such a request is made.			

Please keep this checklist in a safe place until the date of the next review.

Contact the Commissioner

Enquiries and Publication Requests

Jersey

Office of the Information Commissioner
Brunel House
Old Street
St Helier
Jersey
JE2 3RG

T: +44 (0)1534 716530
W: www.dataci.org
Email: enquiries@dataci.org

Guernsey

Office of the Data Protection Commissioner
Guernsey Information Centre
North Esplanade
St Peter Port
Guernsey
GY1 2LQ

T: +44 (0)1481 742074
W: www.dataci.org
Email: enquiries@dataci.org