Gibraltar Regulatory Authority
Data Protection Division

Data Protection Division
Guidance Note Number 17/07

Guidance for Users of CCTV Systems

Guidance for Users of CCTV Systems

Introduction

Closed Circuit Television (CCTV) is used by many organisations and businesses. 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 Act 2004 (DPA) 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 DPA and adopting good standards of practice will help towards realising these objectives.

This guidance 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 centres, car parks, night clubs, schools, banks, airports, etc.

It does not apply to the following:

- Employers who use surveillance techniques to monitor the conduct of employees within the workplace
- 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.

1. Fair and Lawful

To comply with the DPA and its underlying principles, there must be a fair and lawful basis for using CCTV systems.

Examples of lawful bases allowed for in the DPA are:

- Prevention, investigation and detection of crime
- Apprehension and prosecution of offenders
- Public and employee safety
- Security of premises

The purpose(s) for the use of CCTV must be established prior to it being installed.

The fairness element 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 large public areas such as car parks should be bigger, A3 size being acceptable.

2. Accurate and Up To Date

The DPA states that personal data should be accurate, complete 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 recorded images are clear and accurate. If the system uses features such as time references and / or location references then 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 to maintain the system
- Keep a maintenance log

3. Data must be Collected and Used for the Purpose(s) for which it was Intended

It will be a breach of the DPA if data are collected and used for purpose(s) for which they were not originally intended.

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.

4. Data must not be Further Processed in an Incompatible Manner

Even though images may have been obtained and kept in a fair and lawful manner and for specified purposes, data controllers should be aware that the images must not be used in a manner which is incompatible with the purposes for which it was collected.

For example, if a night club informs clients that CCTV is used for security purposes and the film footage is later used as part of an advertising campaign, then the clients may claim that the club has breached the DPA as the clients' personal data were used in a manner which was incompatible with the original purpose.

5. Adequate, Relevant and not Excessive

Data controllers must give careful consideration to where the CCTV cameras are sited as the DPA 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 it will breach the DPA.

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 whether 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 is 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.

6. No Longer than Necessary

To comply with the DPA, images which are not required for the purpose(s) for which they were required should not be retained for longer than 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 DPA.

To decide on how long images should be retained the data controller must consider the purposes of the processing. For instance a club or bar owner may need to keep the images for no longer than 7 days as they will soon be aware of any incidents on their premises. Images recorded by equipment covering a main street may not need to be retained for longer than 1 month unless they are required as evidence in legal proceedings. Images recorded from equipment protecting individuals' safety and security at ATMs 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.

7. Appropriate Organisational and Technical Security Measures

The DPA requires data controllers to consider the harm that data subjects could experience due to the lack of appropriate organisational and technical 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 offices of the manager or designated member of staff. 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 of the viewing
- Date and time images returned to secure place if they are to be retained for evidential purposes

It is important to note that any images of individuals committing offences or alleged offences are defined as sensitive personal data under the DPA. 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 trying on clothes or even sunbathing in their gardens. Needless to say individuals could suffer some degrees of stress and / or distress if restrictions are not placed on who has access to viewing rights.

Subject Access Requests

The DPA 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 (SAR) to the data controller for a copy of the recording of his or her image.

In certain circumstances a SAR can be denied. For example, a SAR could be denied 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. The data controller is required to inform the data subject in writing within 28 days if such circumstances apply. A data subject must put their request in writing. The data must be supplied within 28 days and this period will not begin until receipt of the written request. In the case of a SAR regarding CCTV images, 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. There is a provision in the DPA which states that access to data can be refused if disproportionate effort has to be spent in its retrieval and so it is to the data subject's advantage to give a specified time period. It is emphasised that SAR's 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:

- If possible, a designated member of staff 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

Transfers Outside of the EEA

The DPA requires a data controller not to export any recorded images to countries outside of the European Economic Area. While such transfers are unlikely, the Commissioner would remind data controllers that they should refrain from putting CCTV images on the Internet or their websites.