THE PRINCIPLES OF DATA PROTECTION & THE CCTV CODE OF PRACTICE

Introduction

In 1998, the scope of the Data Protection Act was broadened to enforce 8 principals of good practice regarding the personal data captured about individuals and how this is stored and processed. Personal data included facts and opinions about an individual.

It outlines that any organisation/individual or body who is collecting such information about people must then handle this data in an appropriate manner. ie, that any data collected must be:

1. fairly and lawfully processed,
2. processed for limited purposes,
3. adequate, relevant and not excessive,
4. accurate,
5. not kept longer than necessary,
6. processed in accordance with the data subject's rights,
7. secure,
8. not transferred to countries without adequate protection.

Inevitably the capturing of personal data by means of a CCTV camera was more readily covered by the Act and closer monitoring of CCTV footage, its usage and storage became paramount.

For a CCTV system owner, the Act essentially means that:

- ✓ they must register their CCTV system with the Information Commissioner,
- ✓ they must only take footage that is relevant to their property and it's security,
- ✓ they should not keep footage longer than it is necessary for a crime to come to light,
- ✓ they should warn individuals when they are in a monitored area,
- ✓ they should allow access to the footage to anyone who believes that they have been captured on one of the cameras,
- ✓ they should store captured footage securely so that access to it is strictly monitored.

By July 2000, just a few months after the Data Protection Act actually came into force, it became apparent that clearer guidelines were necessary to help CCTV system owners to run and manage their data storage more appropriately. For this reason, a CCTV Code of Practice was written by the Data Protection Commissioner as a guide to good practice for CCTV users. A summary of the code which was recently updated in 2008 follows:

A Summary

This is a summary of the code of practice issued by the Data Protection Commissioner. It is intended to provide guidance as to good practice for users of CCTV and other similar surveillance equipment.
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 Regulation of Investigatory Powers Act.
- 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. It is likely that the use of cameras by individuals to protect their own property is excluded from the provisions of the Act under the exemption at Section 36 of the Act.

- Use of cameras and similar equipment by the broadcast media for the purposes of journalism, or for artistic or literary purposes.

Following the 8 principals...

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

The First Data Protection Principle requires data controllers to have a legitimate basis for processing personal data, ie, images of individuals. This equipment may be used for a number of different purposes – for example, prevention, investigation and detection of crime, apprehension and prosecution of offenders, public and employee safety, monitoring security of premises etc.

If you are the Data Controller for your system, you must therefore:

- Establish who is the person(s) or organisation(s) legally responsible for the proposed scheme.
- Assess the purpose/reasons for using the CCTV equipment.
- Document these reasons.
- Ensure that notification is lodged with the Information Commissioner's Office covering 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 this Code of Practice (if different from above).

Siting the Cameras

This plays an important part of the Code as where the cameras are sited will determine which images are processed. Ideally, these images should only cover areas directly related to the purpose of the system. The Data Controller must ensure that the cameras are sited with this in mind.

- The equipment should be sited in such a way that it only monitors those spaces, which are intended to be covered by the scheme.
- 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.
- 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. 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.
- 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. For example - it may be appropriate for the equipment to be used to protect the safety of individuals when using cash machines, but images of PIN numbers, balance enquiries etc should not be captured.

Signage

For a CCTV system to operate fairly under the Data Protection Act, the general public must be made aware of when data is being captured about them. CCTV Warning Signs are appropriate for this purpose as when an individual enters a camera zone, by having passed the warning sign they have given their consent to be filmed. Your Warning Signs must:

- Be clearly visible and legible to members of the public.
- Be an appropriate size for who is passing the sign. Eg, A4 size at eye level for someone passing the sign on foot or A3 for a driver entering a car park.
- Have a means of contacting the controller of the CCTV scheme.

Covert Installations

In certain instances, the use of signs may be inappropriate and jeopardise the purpose of the scheme. In this case the Data Controller must ensure that the CCTV cameras are operating under the following conditions:

- In areas where specific criminal activity has been identified.
- Where surveillance is required to obtain evidence of that criminal activity.
- Where the use of signs would prejudice success in obtaining evidence.
- For no longer a duration than necessary.

Quality of the Images

It is important that the images produced by the equipment are as clear as possible in order that they are effective for the purpose for which they are intended. 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 Data Controller must ensure that the system continually operates at an appropriate quality and accurately. Regular checks can be made to ensure that this is the case and these checks should be documented. An initial check should be undertaken to ensure that the equipment performs properly and the following points should be considered:

- If the system records features such as the location of the camera and/or date and time reference, these should be accurate and their accuracy should be regularly checked and recorded.

- Cameras should be situated so that they will capture images relevant to the purpose for which the scheme has been established.

  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.

- When installing cameras, consideration must be given to the physical conditions in which the cameras are located. Eg, extra lighting or infra-red lighting may need to be installed to capture appropriate images.
- 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.

  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

- Cameras should be properly maintained and serviced to ensure that clear images are recorded.
- Cameras should be protected from vandalism in order to ensure that they remain in working order.
- A maintenance log should be kept.
- If a camera is damaged, there should be clear procedures for ensuring that the camera is fixed within a specific time period and monitoring the quality of the maintenance work.

Processing the images

Images, which are not required for the purpose for which the equipment is being used, should not be retained for longer than is necessary. While images are retained, it is essential that they are kept secure with limited

access. It is therefore important that access to and security of the images is controlled in accordance with the requirements of the 1998 Act.

- Images should not be retained for longer than is necessary.

  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 cash machines 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 this period has expired, the images should be removed or erased.

  If the images are retained for evidential purposes, they should be retained in a secure place to which access is controlled.

- When backing up the images that have been recorded, the details should be documented. This should include the date that the images were removed from the general system, the reason why they were removed from the system, any relevant crime incident number, the location where the images will be taken including who will view them, the signature of who has collected the recording and the outcome of the viewing.

- 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.

- 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.

- Viewing of the recorded images should take place in a restricted area, for example, in a manager's office. Other employees should not be allowed to have access to that area when a viewing is taking place.

- All operators and employees with access to images should be aware of the procedure, which need to be followed when accessing the recorded images.

Access to and disclosure of images to third parties.

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 for which they may disclose copies of the images are compatible with the reason or purpose for which they originally obtained those images. 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.

- Access to recorded images should be restricted to those staff who need to have access in order to achieve the purpose of using the equipment.

- All access to the medium on which the images are recorded should be documented.
- Disclosure of the recorded images to third parties should only made in limited and prescribed circumstances.
- All requests for access or for disclosure should be recorded. If access or disclosure is denied, the reason should be documented.
- 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.
- 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.
- 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.

Access by data subjects

There is a right in the 1998 Act to allow anyone believing that they have been captured on a CCTV camera to have access to that data. It is necessary for staff involved with the CCTV system at your premises to be aware of this right and to handle it appropriately.

Staff should be aware of the necessary procedure to be followed when a request is made and be able to provide the subject with a Subject Access Request Form. This may ask for the necessary information to find the images of the subject on the recording, eg, the date & time when the individual believes that they have been captured, a photo if necessary. A charge of up to £10 may be made for such a search for images.

Individuals should also be provided documentation, which describes the types of images, which are recorded and retained, the purposes for which those images are recorded and retained. This should be provided at the time that the standard subject access request form is provided to an individual.

The manager or designated member of staff should determine whether showing images to the individual would entail disclosing images of third parties. It may be necessary to consider here if a third party's privacy should be maintained. 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.

If the manager or designated member of staff decide that the request will not be complied with, they must set out their reasons in the response to the individual.

If, within 21 days of that notification, the individual requires, in writing, the decision to be reconsidered, the manager or designated staff member shall reconsider the decision.

Monitoring compliance with this code of practice.

To ensure appropriate compliance with the Act, other matters to consider include:

- The means of contact indicated on the CCTV Warning signs should be available to members of the public during office hours. Employees handling that contact should be aware of the policies and procedures governing the use of this equipment.

- 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.