

SUMMARY OF THE DATA PROTECTION ACT & CCTV CODE OF PRACTICE.

The 1998 Data Protection Act enforces that any data collected about individuals 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.

A few months after the Act came into force, it became apparent that guidelines were necessary to help CCTV owners to manage their data storage more appropriately. This is a summary of the code of practice issued by the Commissioner, intended to provide guidance as to good practice for users of CCTV.

At this time, this Code is not intended to apply to: -

- Targeted and intrusive surveillance activities.
- Surveillance techniques by employers to monitor their employees' behaviour.
- Security cameras installed for home security purposes.
- Cameras used in broadcasting for journalism, artistic or literary purposes.

Following the principals...

Before using CCTV equipment, users must establish a legitimate purpose for which they intend to use the equipment, eg, the prevention of crime.

You must also:

- Establish who is legally responsible for the scheme.
- Assess and document the purpose of the scheme.
- Notify the Office of the Data Protection Commissioner with its purposes.
- Establish and document those responsible for ensuring day-to-day compliance with the Code of Practice.

Siting the Cameras

Cameras should only cover areas related to the purpose of the system.

- If domestic areas border those spaces then the user should consult with the owner as to whether images might be recorded.
- If cameras are adjustable, they should be restricted so that they do not overlook spaces not intended to be covered.
- If it is not possible to avoid recording such images, then operators should be trained in recognising the privacy implications of viewing such spaces.

Signage

For a CCTV system to operate fairly, the public must be aware of it. Warning Signs must:

- Be clearly visible and legible.
- Be an appropriate size for who is passing the sign. Eg, A3 for a driver entering a car park.
- Have a name and telephone number for the controller of the CCTV scheme.

Covert Installations

In certain instances, the use of signs may jeopardise the purpose of the scheme. Such systems should operate under the following conditions and for no longer a duration than necessary.:

- Where specific criminal activity has been identified.
- Where evidence is required of that criminal activity.
- Where signs would prejudice success in obtaining evidence.

Quality of the Images

The system must continually operate at an appropriate quality and accurately. Regular checks must be made and their results documented. The following points should be considered:

- Only use good quality tapes, which are cleaned so that images are not recorded on top of previous images.
- Dispose of tapes when their quality has deteriorated.
- If date and time stamped, this should be accurate and regularly checked.
- Cameras should be situated so that they capture images relevant to the scheme's purpose.
- When installing, consideration must be given to the physical conditions in which the cameras are located. Eg, extra lighting may need to be installed.
- Users should assess whether 24 hour recording is necessary or excessive.
- Cameras should be maintained to ensure clear images.
- Cameras should be protected from vandalism and in good working order.
- A maintenance log should be kept.
- If a camera is damaged, it must be fixed within a specific time and the quality of the work should be monitored.

Processing the images

Images should not be retained for longer than necessary and must be kept secure with limited access. Eg - publicans may not need to keep recorded images for longer than seven days as they are quickly aware of any incident occurring on their premises.

- Once this period has expired, the images should be removed.
- If the images are retained for evidence, they must remain in a secure place with controlled access.
- On removing the cassette for evidence, the details should be documented.
- Monitors displaying images from areas where individuals expect a degree of privacy should only be viewed by designated personnel.
- Designated personnel must decide whether to allow access by third parties.
- Viewing the recorded images should take place in a restricted area where other employees do not have access when a viewing is taking place.
- Designated personnel should be aware of the procedure, they need to follow when accessing the recorded images.

Access to images by third parties/subjects

CCTV images must be kept secure to preserve the individual's rights and that evidence remains intact should they be required. Users must ensure that the reason for access is compatible with the purpose for which they obtained those images.

- Access to images should be restricted to designated personnel only and clearly documented.
- Disclosure to third parties should only be made in limited circumstances and if access is denied, the reason should be documented.
- Recorded images should not be made widely available - eg, placed on the Internet.
- If images are disclosed, individuals may need to be disguised so that they are not identifiable.
- Procedure must be followed when access is requested and the subject provided with a Subject Access Form. This can ask for necessary information to find the images of the subject and a small fee for making the search.
- If the request is not complied with, they must set out their reasons to the individual, who may ask in writing for this to be reconsidered within 21 days.

Complying with the code

Other matters to consider include:

- The contact point indicated on the Warning signs must be manned during office hours.
- Designated personnel should undertake regular reviews of procedures to ensure that the Code is being complied with.