

EC Directive 95/46/EC on Data Protection came into force on 1st March 2000. This article addresses some of the issues raised by the Directive, which have been enacted in the UK by the Data Protection Act 1998.

### The 1984 Data Protection Act (DPA 84)

Stated that to be liable for registration under the DPA, you must be 'capturing personal data that is processed automatically by reference to the data subject'. That is the official definition of the Act. All CCTV systems that record images are classed as recording personal data. The third part of the DPA asks 'is the data processed automatically by reference to the data subject?' If the answer to this question is yes to this section, then the system must be registered.

All CCTV systems that process data must be notified to the Information Commissioner (formerly the Data Protection Commissioner). This is the same as registering computer systems under the DPA 84 for being able to 'automatically process' data. Failing to register may lead to fines. A system is deemed as 'automatically processing' data, when that data can be retrieved automatically, by a method of sequences. Therefore, if a system has a fast forward or rewind facility on the VCR as its only means of searching for an image, it means you are effectively using your eyes and judgement, which means it would **not** be classified as 'automatic processing'. If the VCR records and permits immediate location of an image, e.g. by time and date, or frame numbering, where it is known that particular data is stored, the system **will** come under the Data Protection Act. So if a digital VCR can use technology which enables it to search automatically for a known incident, then it falls within the Act. A conventional VCR that still requires an operator to use a manual search for a known incident, by fast forward or rewind facilities, though still operating a time and date generator, it is not classed as 'automatic processing'.

All new systems since 1st March 2000 are required to register (now called notification) under the DPA 98 making the question of 'automatic processing' a redundant issue. However, systems installed since 24th October 1998, but before 1st March 2000, have until October 2001 to notify. Systems installed before 24th October 2000 have until October 2001 to notify. Any additions or expansions are not classed as new schemes and don't have to immediately notify, unless there has been a change to 'automatic processing'.

### EC Directive – 1st March 2000

1. This Directive first came out on 24th October 1998, but was implemented on 1st March 2000.
2. All new CCTV systems installed from 1st March 2000 are now required to be registered under the DPA. The issue of 'automatic processing' has now become redundant for new systems.
3. Systems that have been installed **since** 24th October 98, and currently claim exemption (don't 'automatically process data') have until October 2001 to register.
4. Systems installed **before** 24th October 98 which don't 'automatically process data', have until October 2001 to register.
5. Any additions or expansions are not classed as new systems and don't need to be immediately registered, unless there has been a change in 'automatic processing'.

### Registration/Notification

1. When registering a system it must be stated what 'the purpose of the system' is. This 'purpose' can cover several sites. It costs £ 35 to register and registration lasts for 1 year.
2. Check whether the company/organisation is already registered for DPA, because if it is, they can simply extend their entry to include CCTV as well.
3. Once registered/notified, compliance with a number of legally enforceable Principles is required.
4. All organisations, whether registered or not are expected to adopt these Principles. If a complaint is made against any system, the first area Data Protection will investigate is adherence to these Principles.

### Principles

The DPA requires information to be obtained fairly and lawfully. For CCTV, this means that appropriately sized and placed signs are positioned in and around the area under surveillance; these should be A4 and A3 depending on application. They should contain a simple 'purpose for the system message' e.g. to prevent and detect crime, and who owns the system with a contact telephone number.

Obtaining information fairly means that the images/data captured by the system must be used for the original purpose intended for the scheme. Therefore it would be misuse if CCTV footage were sold to a commercial company or TV.

The DPA requires careful consideration to the siting and direction of CCTV cameras to ensure that they avoid capturing data/images that are irrelevant or intrusive - a good example would be minimising the possibility of cameras over looking private property. This can also be achieved by fitting blockers or having privacy zones.

All recorded data/images need to be accurate. This is particularly true if they are used as evidence or in a disciplinary dispute with employees. The Information Commissioner recommends that every effort be made to ensure clarity of image (recognition - 50% or identification standard 110%.) A significant factor in avoiding image degradation is proper tape management: use a 31-day cycle and record all uses in a tape management log. Use good quality SVHS tapes and store them correctly in a data cabinet (BS 7799). Use them no more than 12 times and then electronically wipe the tape using a degausser or by destroying the tapes using another method. Users of CCTV systems must prevent unauthorised access to

CCTV control rooms/areas; all visitors must be authorised and recorded in the visitors log and have signed the confidentiality proforma. Operators/staff must be trained in equipment use and tape management. They should also be fully aware of the Codes of Practice and Procedures for the system. The observation of the data by a third party is to be prevented e.g. no unauthorised staff must see the CCTV monitors.

The DPA supports the right of the individual to a copy of any personal data held about them. Therefore data controllers are obliged to provide a copy of the tape if the individual can prove that they are identifiable on the tape, and they provide enough detail to locate the image (e.g. 1 hour before/after the time they believe they were captured by CCTV, their location and what identifiable features to look for). They must submit an appropriate application to the Data Controller and pay a £10 fee. However, the request can be refused if there are additional data/images on the tape relating to a third party. These additional images must be blurred or pixelated out, if shown to a third party. A good example would be a car accident where one party is attempting to claim against another. The data controller is obliged to say no to a civil request to view the tape, as consideration must be given to the other party. A request by the police is a different matter though. Remember, only the DP Registrar can withhold tapes to protect third parties; it is generally considered they can arbitrate in these sorts of matters. Also, if any individual suffers damage or distress because of any contravention of any of the requirements of the DPA, they are entitled to compensation.

## **Summary**

1. Automatic processing means automatic registration.
2. New systems from 1st March 2000 means automatic registration.
3. Systems installed after 24th October 1998 have until October 2001 to register.
4. Systems installed before 24th October 1998 must be registered by 2001.
5. All CCTV users now have to comply to the DPA Principles, whether registered or not.
6. The purpose of the system must be registered and can cover several sites.
7. Whoever sets the 'purpose of the system' is responsible for the Data Protection of that scheme.

Further information

If you have any further questions contact the Data Protection Office on 01625 545700

Or <http://www.dataprotection.gov.uk/>