

Data Protection Act 1998 & CCTV

A Managers Guide *

Introduction

If ever a piece of legislation can be described as a “sledgehammer to crack a nut,” this is it. Variously described as “draconian,” or “interface with justice,” The Data Protection Act 1998 is the first statute to directly affect the use and management of CCTV. This new law affects every CCTV system and it is the first of three pieces of legislation to be implemented this year that will have a major impact on CCTV.¹

This article seeks to provide you with a guide to the legislation, notify you of the implications that this may have for your business, and provide you with some solutions to the demands made of your business. The article is aimed at those who use CCTV to monitor public spaces or places to which members of the public have access. This includes visitors, salesmen etc. to sites that have CCTV inside their perimeter or offices.

At the time of writing this article there are still issues that the Data Protection Registrar, now known as the Data Protection Commissioner, has to clarify. However the information is the very latest interpretation we can give of the legislation.

Scope of the Act

The Data Protection Act 1998 has superseded the 1984 Act and now covers a number of other “data” storage and retrieval systems. For the first time in the United Kingdom there is now a statutory regulation which covers the use and management of CCTV systems that record the camera output. The Act was introduced as part of the UK Government’s response to the growing un-ease by the House of Lords and some sections of the public, on the use and abuse of CCTV generated material². It is also a part of the Government’s response to the European Directive on Privacy Issues³ and will be complimented in

¹The other two being the Human Rights Act 1998 and the proposed Regulation of Investigatory Powers Act.
²e.g the case of *Peck* involving the showing of CCTV footage depicting a man attempting suicide and the case of *Vigon* which involved a market trader selling swimwear who was recording women trying on his wares in a changing room provided by him.

October 2000 by the incorporation into UK law of the Human Rights Act 1998 (A glossary of some terms and definitions is included at the end of this document).

The Data Protection Act was passed in 1998 and came into effect from 1 March 2000. From that date any member of the public or staff or an organisation, has the right to request access to any CCTV data that they believe a CCTV “**owner**” holds, and in which they appear. It is important to note that they do not have to give a reason for the request and Data Controllers are not entitled to ask for one. There are some exceptions to this principle but the watchword now for those using CCTV has to be “consider the privacy of those who you view.” Whilst the protection of personal privacy is the main aim of few systems, European law places a high value on privacy and this is something which CCTV Managers will have to take on board. By definition the Standards set in the Code associated with this Act apply to those who record data and so any CCTV system that does not have a recording element to it, is currently outside many of the standards. However it is not outside the Act. Viewing personal data for the purposes of crime prevention, detection or the promotion of public safety is regarded as processing and as such requires the system to be registered. The owner would then have to meet at least Principle 1+ 2 + 3 + 7.

How does this impact on CCTV users?

The Act currently applies to all systems irrespective of size or purpose of use. There is no minimum limit to the number of cameras in a system etc. 1 camera to 1 video recorder or indeed a camcorder if used for crime prevention and detection or the promotion of public safety falls within the scope of the Act and so the owner needs to notify the commissioner. The Act serves to tighten up poor practice that has dogged the industry and so bring all CCTV users to a minimum standard of administration and data use.

What criteria should be applied to determine if a system should be registered?

(Notification) See Appendix 1

There are two elements to consider in determining how the Act applies to your system. Firstly the date it was installed. Secondly, how you record your system output. Remember the Act requires you to comply to the Data Protection Principles even if you are now required to register or “notify” as it is now called. If your system was installed before 24 October 1998 and uses videotape based recording systems which require you to manually find the images by using the fast forward or rewind buttons then you benefit from the 1st transitional period. If you have not registered under the 1984 legislation you have until October 2001 to register and comply with the current Act. If you have registered under the 1984 legislation then you will move to the 1998 legislation when you first

register after 24th October 2001. Whilst technically you do not need to comply with the legislation until you are required to register, it is strongly advised that you operate your system as if you are complying. This is for the reason given above and because the Law courts will have to operate with the legislation in place from the 1 March. Challenges to the admissibility of CCTV evidence in the Courts can be expected from 1 March 2000.

³ Directive 95/46/EC

If your system was installed after 24 October 1998 irrespective of what method of recording you are using the whole of the Act **INCLUDING** the right to access applies from 1 March 2000. You must register your system as soon as possible after that date.

As an “owner” of a CCTV system, you will almost certainly be required to notify your system to the Data Protection Commissioner. You will need to give details of who owns the system and for what purpose the data is being recorded. Statements of purpose might include phrases such as “for the prevention and detection of criminal activity,” or “the promotion of a safer environment in which to live and work.” These statements should also be reflected in your company ‘s Code of Practice and Operator Procedural Manual. It is important that the purposes of your system are clearly specified and adhered to. These two documents are crucial to effective compliance with the Data Protection Act 1998. If your system operates without either or both of these documents, this will also seriously weaken the evidential value of any material gleaned from CCTV footage.

As a company you will need a “**Data Controller**”, this is “a person who (either jointly or in common with other persons) determines the purpose for which and the manner in which any personal data are, or are to be, processed.” The Data Controller will be required to take all steps to ensure that the data recorded by the company is within the terms of the Act and in accordance with the “**Principles**” laid down by the legislation. The Data Controller can appoint a Manager to oversee the compliance to the Act,

“however if that manager of the scheme is an employee of one or more of the Data Controllers, then they will not have data protection responsibilities. However, the manager should be aware that if he or she acts outside the instructions of the data controller(s) in relation to obtaining or disclosing the images, they may commit a criminal offence contrary to Section 55 of the 1998 Act, as well as breach their contract of employment.”⁴

⁴ “Code of Practice for Users of CCTV and Similar Surveillance Equipment Monitoring Spaces to which the Public Have Access” Page 18, issued by the Office of the Data Protection Registrar. Feb. 2000. At the time of writing the Code is only in Draft form.
22 October 2004

If the management is devolved to a third party such as a security company employed by the Data Controller to run the scheme, then the security company manager will be deemed a “data processor”. As such they process data on behalf of the Data Controller and are not themselves Data Controllers. Consideration must be given to the Seventh Data Protection Principle in terms of the contractual relationship between Controller and Processor. The Controller will have to satisfy themselves of the adequacy of the Processor’s security arrangements.

Data Protection Principles

The Act lays down eight “Principles” by which the system must comply. In practice, the vast majority of users will only be concerned with the first seven, the eighth deals with transporting data outside the UK.

The Principles

1. Personal data must be processed fairly and lawfully. E.g. with the subject’s consent or because it is necessary to do so, i.e. for the administration of justice.
2. Data should be processed for one or more lawful purposes and not further processed for incompatible purposes.
3. Data shall be adequate, relevant and not excessive.
4. Data shall be accurate and where necessary kept up to date.
5. Data shall not be kept for longer than is necessary
6. Data shall be processed in accordance with rights of data subjects under the Data Protection Act 1998.

7. Appropriate technical and organisational measures shall be taken to prevent unauthorised / unlawful processing of data or accidental loss of, destruction of or damage to data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for rights and freedoms of data subjects in relation to the processing of persona data.

As far as managers are concerned Principle seven is of particular relevance. Appropriate security measures will have to be taken both to protect the contents of tapes and to ensure that their location can be identified at all times. Secure storage systems and effective records of who has had access to tapes, when and why will have to be implement. Failure to implement these could prejudice legal proceedings and lead to action from the Data Protection Commissioner. Leaving all tapes in an unlocked drawer or having a logging system which nobody adheres to will be insufficient to satisfy the Data Protection Commissioner if your tape falls into the wrong hands.

Whilst it is not expected that there will be significantly high levels of demand by the public to view the contents of video recordings, it will have an impact where video recordings are used to support criminal proceedings. The defence is almost certain to ask in court and seek assurances that the system was registered and administered in accordance with the Data Protection Act 1998 before allowing the tape to be offered in evidence. Remember even if a system is exempt from notification, it is not exempt from being run in accordance with the principles of the Act set out above.

What you could expect

The public must put any requests to access the data you hold in writing and give enough information for you to be satisfied that they are who they say they are. They must provide a clear description of the time, date and location that they are interested in and a description of themselves to allow you to identify them from the recording. This request can be made at any time after the event. The Standards being introduced by the Data Protection Commissioner indicate that the recording medium should be replaced after 13 uses. Most systems will operate a 31 day tape rotation system so this time scale is not too onerous and provides ample opportunity for someone to request access to the data. A fee may be required to accompany any request for data; currently the legislation is stipulating a maximum fee of £10. As can be appreciated, this is not a large fee. Accordingly, those systems with effective logs and secure storage will be the least inconvenienced as footage should be must easier to find.

As a company the Data Controller must reply fully within 40 days of the receipt of the request or, if later, the first day on which the Data Controller has both the required fee and the information referred to in subsection (3).¹ The Data Controller must provide the enquirer with accompanied access to see the recording or a video copy and or a hard copy print. It is not acceptable to provide a copy of a multiplexed image in time lapse mode without first decoding the relevant camera and slowing the recording down to normal playback speed. The Data Controller must also make every effort to ensure that other “**data subjects**” are not identified from the showing of the material or that they have given their consent to the showing of the material. In some cases this may mean that the pictures provided need to have some faces blanked out.

In order to meet these requirements it is expected that a comprehensive management system will be in place to record, store and then locate the relevant data ADT have worked with a number of suppliers to locate appropriate products to help you meet these meets.

What will it cost?

To register your system with the Data Protection Commissioner will cost £35 per year.

In order to comply with the principles set out in the Act the following equipment together with appropriate procedures will provide the minimum requirement:-

- | | |
|---------|---|
| Signage | Signs indicating the area being covered by the cameras. A person passing the sign is giving implied consent (Principle 1) to be recorded. The sign needs to give details of the “owner” purpose and contact point or number. |
| Tapes | A minimum supply of 28 days, with a Home Office recommendation of 31 days of tapes for each video recorder in the system. These should be labelled with some unique reference so that the tape can be easily identified. This will provide a minimum 28-day period for the public to write to request access. |
| Storage | Principle 7 states that appropriate technical and organisational measures should be taken to prevent unauthorised / unlawful or accidental loss, damage or destruction of data. A secure cabinet therefore is recommended to store the tapes in. In very |

¹ See Section 7 (10) of the Data Protection Act 1998.
22 October 2004

vulnerable areas it may be that the video recorder also needs to operate inside a secure cabinet. In addition, access to the tapes must be restricted and effectively controlled.

Log book Following on from the storage issue, data needs to be carefully tracked and its history followed for legal purposes. A comprehensive logging system should be in place for large systems with smaller systems adopting a short form of the same system. These systems must be regularly checked to ensure that operators are adhering to them at all times. Merely having a system is not enough, it must be monitored to ensure that it is working efficiently and effectively. Any logging system must also identify any third parties to whom tapes have been passed and the circumstances surrounding the decision to release data to a third party.

Bulk eraser ***THIS IS NOT MANDATORY*** however it is government recommended best practice and will be expected in large town centre or shopping centre schemes. *“Simply recording over old material is not satisfactory, not least because this will compromise a tape’s acceptability for evidential purposes”*.⁵ This together with principle 5 of the Data Protection Act means that a bulk eraser is a necessary investment.

You will also need to consider how you will playback, copy or provide the information that any data subject requesting access.

Managers will need to give careful consideration to their systems ability to meet the purposes for which the system was installed. If through poor maintenance, badly positioned or operated cameras the system fails to provide the quality of images that the system purposes demand then it may be that an offence under Principle 3 of the Act has been committed. E.g. If one of the system purposes is “for the prevention and detection of criminal activity” and the images are not capable of identifying the individual in the picture that may lead to a complaint against the system. The images will also be useless as evidence in a criminal trial, this may make the difference between conviction and acquittal. Acquittals arising out of a failure to spend a few pounds on good quality tapes for example, would demonstrate the false economy involved.

⁵ “CCTV Looking Our For You” Home Office Nov. 1994

Managers will also have to pay attention to training matters. Operators need to be adequately trained to make them aware of their responsibilities under the Act. Such training needs to be reaffirmed at regular intervals to ensure that standards do not slip. To take an example, if an operator habitually completes logbooks the day after because he needs to get a bus home, one day the tape might be required immediately for the investigation of a serious criminal offence. The failure to log the tape properly may lead to its exclusion from a subsequent court case. If that operator has been given training some months before which has not been repeated or refreshed and the logbooks have not been regularly inspected, it is arguable that the Data Controller is in breach of principle seven.

Offences under the Act

The main offences under the Act revolve around

- Processing without notification
- Failing to notify the Commissioner of changes in your circumstances
- Failing to comply with written requests
- Knowingly or recklessly making false statement in compliance with an information notice
- Intentional obstruction of, or failure to give reasonable assistance in, execution of a warrant

It is also an offence for a person without the consent of the Data Controller, knowingly or recklessly to:-

- Obtain or disclose personal data or the information contained in personal data.

There are exceptions to this in respect of criminal activity but they are carefully constructed and need to be fully understood by the Data Controller.

- Unlawful selling of personal data

All the above offences are triable in either the Magistrate's Court or the Crown Court. Upon conviction in the Magistrate's Court, an offender is liable to a maximum fine of £5,000 whilst in the Crown Court an unlimited fine may be imposed.

The Act also provides for separate personal liability for the offences in the Act for Directors or other officers of the company that have committed the offence.

Definitions

- "Personal Data" = Data relating to a living individual who can be identified from the data
- "Data Subject" = An individual who is the subject of personal data.
- "Processing" = 'obtaining, receiving or holding' information or data. This includes recording, storing, disclosing and erasing such data.
- "Data Controller" = A legal person (or company) who decides how and what for what purposes the data is to be processed.
- "Data Processor" = A person (not an employee of the data controller) who processes data on behalf of the controller.