Visimetrics
DIGITAL CCTV SYSTEMS

Data Protection Act 1998

Introduction

This is a short guide to the Data Protection Act, 1998 ("DPA") setting out implications for the CCTV industry. The guide is designed to provide information, not legal advice, about the Data Protection Act 1998, which is a complex piece of legislation. Legal advice should be sought before any action is undertaken as a result of the Act and a check should be made to see whether the law has changed since the time this guide was written.

The DPA, which was brought into force on the 1st March 2000, has superseded the 1984 Act and now covers a number of other "data" storage and retrieval systems. The new Act has more powerful and wide-ranging penalties than its predecessor and companies not complying with the terms of the Act are exposing themselves to serious breaches. The CCTV Code of Practice ("the Code") was subsequently issued in July 2000 by the Information Commissioner (previously known as the Data Protection Commissioner). The Code is based on the eight Data Protection Principles set out in the DPA and has 62 legally enforceable standards and 30 points of good practice. Together, the DPA and the Code set out a comprehensive legal framework for the use of CCTV systems. For the first time, in the United Kingdom there is now statutory regulation covering the use and management of CCTV systems that record the camera output. Consequently, the DPA has serious implications for the CCTV industry as almost every CCTV user must comply with the DPA.

The period of transitional relief under the DPA ends on 23rd October, 2001. So far, the Information Commissioner has been relatively lenient with non-compliance with the DPA since promulgation in March 2000 but after 23rd October the Commissioner will tighten up on non-compliance with both the DPA and CCTV Code of Conduct. **The changes in data protection legislation means that legally enforceable standards will apply to the collection and processing of images relating to individuals.**

Data

Data is defined in the DPA as including any information which "is being processed by means of equipment operating automatically in response to instructions given for that purpose" or "is

recorded with the intention that it should be processed by means of such equipment" (referred to as "automated data").

The Act now differentiates between **personal data** and **sensitive personal data**.

Personal data is "data which relate to a living individual who can be identified from those data, or from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, ……". This also includes information derived by merging data with data (which the Data Controller is entitled to have) from other sources. It may include the Data Controller's opinions about the individual and a statement of how that data will be used. Photographs and images of people and/or the information details about the people involved in the digitisation project are classified as personal data.

A data controller is "a person who, either alone or jointly or in common with other persons, determines the purposes for which and the manner in which any personal data are, or are to be, processed". The obligations imposed by the DPA are for the data controllers to comply with. Where they engage another to undertake the actual processing on their behalf (termed a "data processor" under the DPA) the obligations still lie with them and not with the data processor and they must ensure, by way of contract, that the data processor complies with the DPA.

As regards CCTV, this definition is not limited to circumstances where a data controller can attribute a name to a particular image. Any image of distinguishable individuals' features from which an individual could be identified is covered.

The categories of sensitive personal data are:

- racial or ethnic origin of the data subject;
- political opinion ;
- religious or spiritual belief ;
- whether on not a member of a trade union;
- physical or mental health or condition;
- sexual life;

Visimetrics
DIGITAL CCTV SYSTEMS

- the record of any alleged or actual criminal activity or sentencing.

The definition of processing is extremely wide and covers all sorts of recording and holding of images (even if just for a limited period of time or if no further reference is made to those images). Real-time transmission of the images or any further use or disclosure are also included in the definition. The definition covers:

- obtaining or recording the data;
- storing the data;
- organising, adapting, or altering the data;
- retrieving or making decisions based on the data; and
- making the data available to other processes that require it, according to registered use.

The main change for CCTV users is that the recording and storing of data on people is now considered to be "processing" and therefore comes under the scope of the DPA. This should assist the prosecution in court cases by improving management of systems. To date, up to 70% of images used to identify criminals are discarded as evidence due to poor image quality. Under the DPA, images must be clear with the time, date and location accurately recorded.

Therefore, all such CCTV schemes must comply with DPA provisions. Further, where the data are sensitive, more stringent conditions apply. The definition of sensitive data includes information about the commission or alleged commission of an offence.

As with the 1984 Act, some data are partially or completely exempt. Exemptions are:

- **data relating to national security** (MI5, Ministry of Defence, the Queen). Organisations claiming exemption may obtain a Certificate of Exemption signed by a government minister.
- **crime and taxation**. Criminals have no rights to see their own record; Customs & Excise who may be investigating money laundering or VAT fraud are exempt.
- **health, education, social work**. Subject access to examination scripts is exempt as is personal data about present/past pupils. No exemptions will be made in the case of social work unless

they prevent the carrying out of social work (e.g. children on the "At Risk" register may be have safety jeopardised by a disclosure).

- **journalism, literature, art**. Only if the publication is in the public interest.
- **research**. Data must still be registered but if individual people are not identified, then data subjects have no legal right to see it.

The Eight Principles of the DPA

The DPA sets out eight principles with which data controllers must comply:

First Principle - fair and lawful processing

"Personal data shall be processed fairly and lawfully, and, in particular, shall not be processed unless at least one of the processing conditions is met, and in the case of processing sensitive personal data the data must be processed fairly and lawfully and at least one of the conditions for processing sensitive personal data is met."

As part of the fair processing requirement, certain information must be provided, or made readily available, to the individuals - including the identity of the data controller and the purpose (in general terms) for which the data are intended to be processed. Also, in determining fairness, the method by which data are obtained will be taken into account.

Installation of appropriate signs assists in compliance with this principle. However, an exemption applies where the purpose is prevention and detection of crime or apprehension and prosecution of offenders.

Thus, processing will not be fair if the individuals are deceived or misled as to the purpose for which the data are to be processed.

The requirement for lawful processing means that other statutory or common law restrictions have to be taken into account. For example, where the information is confidential, the common law duty of confidentiality has to be complied with in addition to the specific provisions of the DPA.

The subject's consent may not be required under the following categories:

- if the processing is carried out as part of the lawful activities of any non-profit making political, philosophical, religious, or trade-union organisation. The processing must safeguard the rights and freedoms of the data subjects. It must be limited to members or persons in regular contact with the organisation **and** it must not disclose any personal data to others without the data subject's consent; or
- the Secretary of State may specify cases where this condition is excluded or modified, e.g. where the processing is necessary for medical purposes where sensitive personal data is necessary for monitoring equal opportunities for people of different racial or ethnic origins and is carried out with the usual safeguards for the rights and freedoms of data subjects.

Personal data processing conditions

- if the processing is to protect the subject e.g. urgently retrieving a subject's medical record after a serious accident; or
- for the administration of justice; or
- to comply with legal obligations; or
- in the public interest.

Sensitive personal data processing conditions

- if the Data Controller has legal obligations to process the subject's employee data; or
- if the data subject is unable to give consent, e.g. unconscious; or
- in order to protect the vital interests of the data subject or another person; or
- in a case where consent on or behalf of another person has been unreasonably withheld, e.g. parent's religious beliefs preventing their child's right to hospital treatment and life; or
- where processing is necessary for legal reasons, e.g. obtaining legal advice, exercising or defending legal rights, for the administration of justice.

SECOND PRINCIPLE - the purposes for which personal data may be processed

"*Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.*"

This means that a data controller needs to be clear about the purpose(s) for which the images are to be processed and, if disclosure is to be made to a third party, the data controller needs to consider the purpose(s) for which the third party might process the data in order to ensure compatibility.

Further, simply registering the purpose(s) is not sufficient to satisfy the requirement to specify purpose but there are two methods that a Data Controller may use to specify the purposes for which personal data are obtained:

- by informing the data subject or,
- by notifying the Information Commissioner.

This is in addition to notification (registration). All controllers must notify the Information Commissioner and pay the annual notification fee.

THIRD PRINCIPLE - requirements as to the extent of the data

"*Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.*"

Organisations are required to state the purpose for which data is processed and cannot process it for any other purposes without further notification. This principle requires data to be adequate, relevant and not excessive in relation to the purposes for which they are processed. For example, cameras installed for the purpose of recording acts of vandalism in a car park should not overlook neighbouring private residences

Visimetrics
DIGITAL CCTV SYSTEMS

FOURTH PRINCIPLE - the requirement for accuracy

"*Personal data shall be accurate and where necessary, kept up to date*"

Data Controllers must take reasonable steps to ensure the accuracy of the data. At school, students are frequently given their personal details to take home and check. They are given the opportunity to change any out of date or incorrect data. Other organisations should carry out similar checks at regular intervals; this may incur costs to print out the details, collect them in again and edit the records to bring them up-to-date but is necessary by law.

FIFTH PRINCIPLE -- requirement as to the duration for which data are to be held

"*Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.*"

The fifth principle requires that data are not held for longer than is necessary for the purpose for which it is processed. An example is data collected from applicants for a job. That data can only be stored for the period of assessment, interview and selection. After that it should be discarded.

For CCTV users images should not be retained for longer than is necessary. Once the retention 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.

SIXTH PRINCIPLE - the interrelationship with data subject rights

"*Personal data shall be processed in accordance with the rights of data subjects under this Act.*"

A data subject has the following rights:

- subject access;
- to require the data controller to cease or not begin processing that is likely to cause damage or distress and to sue for compensation if damage or distress has been caused;
- to prevent processing for direct marketing purposes, so anyone can stop the arrival of personalised junk mail by writing to the data controller;

Visimetrics
DIGITAL CCTV SYSTEMS

- to be informed of the logic used in automated decision making where automated means are used to evaluate matters, e.g. obtaining a mortgage depending on a calculation involving salary, credit worthiness and other details;
- to require rectification, blocking, destruction or erasure of inaccurate data by application to the court;
- to ask the Commissioner to check whether certain processing of their data is being carried out unlawfully.

A data subject is entitled to make a written request to the data controller (accompanied by administration fee) and be given details of their data within 40 days of the data controller receiving the required fee and information.

Details of data given to a data subject will consist of:

- a description of their data,
- what it contains,
- the purposes for which it is being processed,
- why it is being processed,
- people to whom it may be disclosed,
- who is allowed to see it,
- the name of the organisation that is actually carrying out the processing of their data,
- which organisation will perform the processing.

Specific **exemptions** that may be relevant to CCTV schemes include:

- processing for prevention or detection of crime or apprehension or prosecution of offenders;
- processing for safeguarding national security;
- processing for certain regulatory activities;
- processing for journalism, literature or art (subject to certain conditions);
- disclosures required by law or made in connection with legal proceedings etc.

Visimetrics
DIGITAL CCTV SYSTEMS

SEVENTH PRINCIPLE - the requirement for security

"*Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.*"

Data must be kept private and secure. This means that the data controller must ensure that data is backed-up regularly, virus checked, and restricted to named authorised persons by use of passwords or other security means.

Any data processors that a data controller may use for processing their data must be professional enough to guarantee the privacy and security of the data. It is also the data controller's responsibility to ensure that the data processor carries out the processing as specified according to an agreed contract.

EIGHTH PRINCIPLE - restrictions on overseas transfers

"*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 the rights and freedoms of data subjects in relation to the processing of personal data.*"

* The European Economic Area is currently the member countries of the EEC plus Iceland, Liechtenstein and Norway.

There are certain circumstances where this principle does **not apply** to a transfer of data. They are:

- the data subject has given consent to the transfer as part of a contract between the data subject and the data controller; or
- the transfer is necessary in the conclusion of a contract between the data controller or is in the data subject's interest; or
- for reasons of substantial public interest.

If the eighth principle does apply to the transfer of data, exemptions can be made under the following circumstance:

Visimetrics
DIGITAL CCTV SYSTEMS

- if the Secretary of State can order and explain such a transfer; or
- for legal reasons, such as advice, legal proceedings or defending legal rights; or
- if the transfer is part of the personal data on a public register; or
- the transfer has been authorised by the Commissioner and ensures adequate safeguards for the rights and freedoms of data subjects.

Apart from the first principle, the other seven principles have to be complied with. For present purposes, only those that appear most important in the context of CCTV and the protection of individuals' rights are highlighted. Breach of the principles by a data controller is breach of the statutory duty imposed on him by section 4(4) of the Act. Additionally, breach may result in enforcement proceedings and a claim for compensation. However, breach of the principles alone is not a criminal offence under the Act.

How does the DPA affect CCTV users?

CCTV surveillance is undertaken for various purposes and the legal framework differs according to those purposes. Broadly, these can be categorised as follows:

- Covert surveillance

  Surveillance is "covert" where it is carried out in a manner calculated to ensure that the person subject to the surveillance is unaware that it is or may be taking place. Covert surveillance covered by the Bill is of two types:

  - Directed Surveillance

    This is defined as covert surveillance undertaken in relation to a specific investigation or a specific operation which is likely to result in the obtaining of private information about a person; the surveillance is not done as an immediate response to events or circumstances that would make it impracticable to seek an authorisation. An authorisation for directed surveillance can be combined with one for intrusive surveillance. Such authorisation can be granted only by the Secretary of State.
  - Intrusive covert surveillance.

Visimetrics
DIGITAL CCTV SYSTEMS

This is covert surveillance carried out in relation to anything taking place on residential premises or in any private vehicle. It does not cover devices that only provide information about the location of a vehicle (e.g. tracking devices).

- Other covert surveillance
  e.g. of employees by employers
- Non-covert surveillance
  e.g. in shopping centres

All of these are covered by the DPA.

The only form of CCTV that is not be regulated by statute is CCTV carried out by an individual for the purpose of "personal, family or household affairs" - Section 36 of the DPA makes clear that the DPA does not apply in such circumstances. CCTV installed on a private residential property for security purposes probably falls into this category but not CCTV installed on company business premises for the same purpose.

From 1st March, 2000 any member of the public or staff of an organization, who has a justifiable reason, has the right to request access to any CCTV data that they believe a CCTV "owner" holds, and in which they appear. The Act serves to tighten up poor practice that has existed within the CCTV industry and so bring all CCTV users to a minimum standard of administration and data use. As outlined above in the discussion of the DPA, there are some exceptions to this general principle but from now on, CCTV users have to be aware of the privacy of those individuals viewed by the system. The Act currently applies to all systems irrespective of size or purpose of use. However, the Act only applies to those who record data and so any CCTV system that does not have a recording element to it is currently outside the scope of this Act.

Compliance with the Act

There is no minimum limit to the number of cameras in a system which falls within the scope of the Act and therefore needs to be registered i.e. 1 camera and 1 video recorder constitutes a system requiring registration.

Visimetrics
DIGITAL CCTV SYSTEMS

Information required by the Registrar is:

- who owns the system;
- why the data is being recorded. The DPA registration form guidance notes have some examples of typical statements of purpose which include phrases such as " for the prevention and detection of criminal activity," or " the promotion of a safer environment in which to work." The "owner's" statements of purpose should also be reflected in the company's Code of Practice and Operator Procedural Manual.

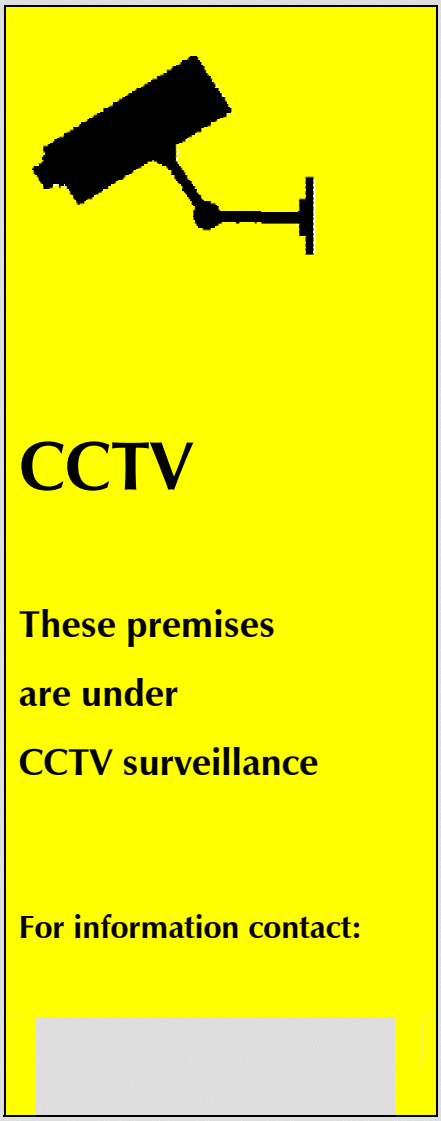
To register with the Information Commissioner costs £35 per annum.

A company or firm needs to appoint a "Data Controller". This is the person or legal entity that is liable if there is a breach of the Act and this may be the company itself. In the case of an individual they would be charged with any offences committed under the Act as well as any individual within the company who might have been personally responsible for the offence. The Data Controller must therefore take all steps to ensure that the data recorded by the company is within the terms of the Act and in accordance with the eight principles laid down by the legislation.

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

Signs: A person passing the sign is giving implied consent (principle 1) to be recorded. The DPA also gives guidance on requirements for CCTV warning signs indicating the area being covered by the cameras, informing the public that CCTV is in operation. The main development within the guidelines on signage is that the signs should now indicate who to contact for further information about the CCTV system. An example is set out below:

Visimetrics
DIGITAL CCTV SYSTEMS



Tapes: A minimum supply of 28 days, with a Home Office recommendation of 31 days, of tapes for each video recorder in the system. Theses should be labelled with some unique reference so

that the tape can be easily identified. The Data Protection Act will almost certainly give a 28-day period for the public to write to request access.

It is therefore easier to comply with the conditions of the Act if digital recorders are used as hard disc capacity can store up to 31 days' data continuously together with date and time displays.

Storage: Principle 7 states that appropriate technical and organizational measures should taken to prevent unauthorized, unlawful or accidental loss, damage or destruction of data. A secure cabinet therefore is recommended to store the tapes in. In very vulnerable areas it may be that the video recorder also needs to operate inside a secure cabinet.

Digital recorders record directly onto hard discs and therefore conform more easily to principle 7 of the Act.

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.

Playback: Consideration needs to be given as to how to playback, copy or provide information to a data subject requesting access.

Summary of Data Protection Principles applying to CCTV users

The eight principles applicable to CCTV users, in summary, are:

- Personal data must be processed fairly and lawfully e.g. with the subject's consent or for the administration of justice.
- Data shall be adequate, relevant and not excessive.
- Data should be processed for one or more lawful purposes and not further processed for incompatible purposes.
- Data shall be accurate and where necessary kept up to date.
- Data shall not be kept for longer than is necessary.

Visimetrics
DIGITAL CCTV SYSTEMS

- Data shall be processed in accordance with rights of data subjects under the Act.
- Appropriate technical and organizational measures shall be taken to prevent unauthorized or unlawful processing of data or accidental loss of, destruction of or damage to data.
- 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 personal data.

Even if a system is exempt from registration it is not exempt from being run in accordance with the principles of the Act set out above.

Public access to data

The public must put any requests to access data in writing and give enough information for the CCTV owner to be satisfied that they are who they say they are. A clear description of the time, date and location that they are interested in and a description of themselves must be provided to allow identification from the recording. This request can be made at any time within a period of 28 days from the relevant time.

Most systems will operate a 28 day rotation system of tapes or store images digitally onto a hard disk for a 28 day rotation period so it will not be too difficult to comply with this time scale. A fee must accompany any request for data. Currently a fee of £10 with the provision for this to rise to a maximum of £50 for particular complex or large scale enquiries is laid down by the Act.

The Data Controller must reply with 21 days of the written request, indicating how they will meet the request. The data subject must be provided with a copy, hard copy print, or an opportunity to view the relevant portion of the recording in an intelligible manner. 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.

It is not expected that there will be significantly high levels of demand by the public view the contents of video recordings but the DPA will have an impact where video recordings are used to support criminal proceedings. The defence will seek assurances in court that the system was registered and administered in accordance with the DPA before allowing the recording to be offered in evidence. In order to meet these requirements it is essential that a comprehensive management system is in place to record, store and then locate the relevant data. Again, digital recording is more secure and easily administered that video tape recording for the purposes of court evidence.

Offences under the Act

The main offences under the Act revolve around:

Offences by data controllers	• Processing without notification • Non compliance with notification regulation (i.e. failing to notify the Commissioner of changes in circumstances) • Failing to comply with written requests • Carrying on assessable processing within the initial period following notification • Knowingly or recklessly making false statement in compliance with an information notice
Processing without the consent of the Data Controller	• If a person either knowingly or recklessly o Obtains or discloses personal data o Obtains or discloses the information in personal form o Procures the disclosure of personal data information to another person Without the consent of the data controller
Trading in personal data	• Unlawful selling of information by commissioner/staff/agent

	• Offering to sell or selling personal data which has been obtained in contravention of section 55(1) • Any person suspected of trading illegally in personal data should be reported to the Information Commissioner
Schedule 9 offences	• Intentional obstruction of or failure to give reasonable assistance in, execution of a warrant
Directors	• If an offence is committed under Section 61 of the DPA by a body corporate and it is proved to have been committed with the consent of or connivance of or to be attributable to neglect on the part of a director; manager; the company secretary; similar officer of the body or any person purporting to act in such capacity then the person as well as the body corporate is guilty of an offence

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 has committed the offence.

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

Visimetrics
DIGITAL CCTV SYSTEMS

The CCTV Code of Practice

Whilst the DPA covers all users of CCTV (save domestic) the Code deals with surveillance in areas to which the public have largely free and unrestricted access. Nevertheless the provisions of the Code will be relevant to other users also.

Part I sets out the measures and standards that must be met to comply with the DPA as well as guidance for good practice. For example, before installing and using CCTV, the Code requires the organisers of a CCTV scheme to establish who is legally responsible for the CCTV scheme, to set out the purposes and reasons for the CCTV scheme and to notify the Commissioner of these details, to ensure that there are signs warning that CCTV is in place and to establish security and disclosure policies.

Part II sets out the interpretation of the DPA on which Part I is based.

On 1st October, 2000 the Information Commissioner issued new guidelines for CCTV systems.

1. Recordings should be kept for at least 28 days.
2. Recordings should be securely kept, and access restricted to authorised personnel only.
3. Recording tapes should be replaced after they have been used 12 times.

Where there is a breach of the DPA, the individual either can go to the Courts or make a claim to the Information Commissioner. The Information Commissioner, if satisfied of a breach, can serve an enforcement notice on the data controller – e.g., requiring the person to refrain from processing or to process only in a way that does not infringe the individual's rights. If the individual can prove actual damage too, he or she could receive compensation. Failure to comply with a notice is an offence punishable by way of a fine.