Course:Professional Issues in IT

Data Protection, Privacy and Freedom of Information

Background :

- Public concern about data protection was first aroused when it was realized that a very large amount of data about individuals was being collected and stored in computers and then used for purposes that were not only different from those intended when the data was collected, but also unacceptable.
- There were also concerns that unauthorized people could access such data and that the data might be out of date, incomplete or just plain wrong.

Data Protection Act 1984

These concerns surfaced in the 1970s.

They were particularly strong in the UK and the rest of Europe and led to a Council of Europe Convention on the subject.

The first UK Data Protection Act, passed in 1984, was designed to implement the provisions of the Convention.

The Data protection Act 1984

It was designed to protect individuals from:

- the use of inaccurate personal information or information that is incomplete or irrelevant;
- the use of personal information by unauthorized persons;
- the use of personal information for purposes other than that for which it was collected.

Key responsibilities

- It was meant primarily to protect individuals against the misuse of personal data by large organizations, public or private.

Example :

Such misuse might occur, for example, if data-matching techniques are used on credit card records to build up a picture of a person's movements over an extended period.

- Further, errors can often creep into data that has been collected or data may be interpreted in a misleading way, and it was difficult to persuade the holders of the data to correct these.

Example:

Credit rating agencies might advise against giving a person a loan because someone who previously lived at the same address defaulted on a loan.

Progressing of the Act

By the mid-1990s, a different danger had become apparent.

As individuals began to use the internet for an ever wider range of purposes, it became possible to capture information about the way individuals use the internet and to build profiles of their habits that can be used for marketing purposes and also, perhaps, for more sinister purposes such as blackmail.

What is more, this can be done by much smaller and much shadowier organizations than those that were the object of the 1984 Act.

These and other concerns led in 1995 to the European Directive on Data Protection which, in turn, led to the 1998 Data Protection Act.

DATA PROTECTION

The first UK legislation on data protection was the 1984 Data Protection Act. However, this was taken over by the 1998 Act.

- The Act defines a number of terms that are widely used in discussions of data protection issues. In some cases these are different from the terms used in the 1984 Act.

To get a clear picture we need to be familiar with some terminologies regarding Data protection

Terminology

- *Data* means information that is being processed automatically or is collected with that intention or is recorded as part of a relevant filing system
- *Data controller* means a person who determines why or how personal data is processed. This may be a legal person or a natural person.
- *Data processor*, in this context, means anyone who processes personal data on behalf of the data controller and who is not an employee of the data controller. This might include an application service provider, such as a company that provides online hotel booking services.
- *Personal data* means data which relates to a living person who can be identified from data, possibly taken together with other information the data controller is likely to have it recorded as part of a relevant filing system.

Terminology ……

- *Data subject* means the individual who is the subject of personal data.
- *Sensitive personal data* means personal data relating to the racial or ethnic origin of data subjects, their political opinions, their religious beliefs, whether they are members of trade unions, their physical or mental health, their sexual life, or whether they have committed or are alleged to have committed any criminal offence. The rules regarding the processing of sensitive personal data are stricter than for other personal data.

Processing

- *Processing* means obtaining, recording or holding the information or data

or carrying out any operations on it, **including:**

(a) organization, adaptation or alteration of the information or data,

(b) retrieval, consultation or use of the information or data,

(c) disclosure of the information or data by transmission, dissemination or otherwise making available, or

(d) alignment, combination, blocking, erasure or destruction of the information or data.

Data protection principles

The 1998 Act lays down eight data protection principles, which apply to the collection and processing of personal data of any sort.

Data controllers are responsible for ensuring that these principles are complied with in respect of all the personal data for which they are responsible.

First data protection principle

“Personal data shall be processed fairly and lawfully and in particular shall not be processed unless (a) at least one of the conditions in Schedule 2 is met and (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.”

The most significant condition in Schedule 2 of the Act is that the data subject has given their consent. If this is not the case, then the data can only be processed if the data controller is under a legal or statutory obligation for which the processing is necessary.

For processing sensitive personal information, Schedule 3 requires that the data subject has given explicit consent.

Second data protection principle

“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.”

Data controllers must notify the Information Commissioner of the personal data they are collecting and the purposes for which it is being collected.

Third data protection principle

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

Fourth data protection principle

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

- While this principle is admirable, it can be extremely difficult comply with.

Examples: In the UK, doctors have great difficulty in maintaining up-to-date data about their patients' addresses, particularly patients who are students, because students change their addresses frequently and rarely remember to tell their doctor.

Universities have similar difficulties.

Fifth data protection principle

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

This principle raises more difficulties than might be expected:

- It is necessary to establish how long each item of personal data needs to be kept. Auditors will require that financial data is kept for seven years. Action in the civil courts can be initiated up to six years after the events complained of took place so that it may be prudent to hold data for this length of time. It is appropriate to keep some personal data indefinitely (e.g. university records of graduating students). In all cases, the purpose for which the data is kept must be included in the purposes for which it was collected.
- Procedures to ensure that all data is erased at the appropriate time are needed, and this must include erasure from backup copies.

Sixth data protection principle

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

Seventh data protection principle

“Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.”

It implies the need for access control (through passwords or other means), backup procedures, integrity checks on the data, vetting of personnel who have access to the data, and so on.

Eighth data protection principle

"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."

This principle can be viewed in two ways.

- It can be seen as protecting data subjects from having their personal data transferred to countries where there are no limitations on how it might be used.
- It can also be seen as specifically allowing businesses to transmit personal data across national borders provided there is adequate legislation in the destination country.

Rights of Data Subjects

The 1984 Act gave data subjects the right to know whether a data controller held data relating to them, the right to see the data, and the right to have the data erased or corrected if it is inaccurate.

The 1998 Act extends this right of access so that data subjects have the right to receive:

- a description of the personal data being held;
- an explanation of the purpose for which it is being held and processed;
- a description of the people or organizations to which it may be disclosed;
- an intelligible statement of the specific data held about them;
- a description of the source of the data.

Data subject rights

The 1998 Act also gives data subjects the right:

- to prevent processing likely to cause damage and distress;
- to prevent processing for the purposes of direct marketing;
- to compensation in the case of damage caused by processing of personal data in violation of the principles of the Act.

Scope of the Act

- There are a number of important exceptions or limitations to the right of subject access, for example: where disclosing the information may result in infringing someone else's rights; where the data consists of a reference given by the data controller; examination candidates do not have the right of access to their marks until after the results of the examinations have been published;
- personal data consisting of information recorded by candidates during an academic, professional or other examination are exempt from the right of access.

PRIVACY

- The starting point is the Regulation of Investigatory Powers Act 2000, which sets up a framework for controlling the lawful interception of computer, telephone and postal communications.
- The Act allows government security services and law enforcement authorities to intercept, monitor and investigate electronic data only in certain specified situations such as when preventing and detecting crime. Powers include being able to demand the disclosure of data encryption keys.

Under the Act and the associated regulations, organizations that provide computer and telephone services (this includes not only ISPs (internet service providers) and other telecommunications service providers but also most employers) can monitor and record communications without the consent of the users of the service, provided this is done for one of the following purposes:

- to establish facts, for example, on what date a specific order was placed;
- to ensure that the organization's regulations and procedures are being complied with;
- to ascertain or demonstrate standards which are or ought be to be achieved;
- to prevent or detect crime (whether computer-related or not);
- to investigate or detect unauthorized use of telecommunication systems;
- to ensure the effective operation of the system, for example, by detecting viruses or denial of service attacks;

- to find out whether a communication is a business communication or a private one (e.g. monitoring the emails of employees who are on holiday, in order to deal with any that relate to the business);
- to monitor (but not record) calls to confidential, counselling helplines run free of charge by the business, provided that users are able to remain anonymous if they so choose.

FREEDOM OF INFORMATION

- The primary purpose of the Freedom of Information Act is to provide clear rights of access to information held by bodies in the public sector. Under the terms of the Act, any member of the public can apply for access to such information.
- The Act also provides an enforcement mechanism if the information is not made available. The legislation applies to Parliament, government departments, local authorities, health trusts, doctors' surgeries, universities, schools and many other organizations. The main features of the Act are:

- There is a general right of access to information held by public authorities in the course of carrying out their public functions, subject to certain conditions and exemptions.
- In most cases where information is exempted from disclosure, there is a duty on public authorities to disclose where, in the view of the public authority, the public interest in disclosure outweighs the public interest in maintaining the exemption in question.
- There is a new office of the Information Commissioner (see the 'Further reading' section for the website) and a new Information Tribunal, with wide powers to enforce the rights, was created.
- A duty was imposed on public authorities to adopt a scheme for the publication of information. The schemes, which must be approved by the Information Commissioner, specify the classes of information the authority intends to publish, the manner of publication and whether the information is available to the public free of charge or on payment of a fee