Professional Issues

Data Protection

(Bott, Ch 14)

Overview

- Overview of the 1998 Data Protection Act (DPA)
  - Definitions
  - Changes since 1984 Act
  - Sensitive Personal Data & Consent
  - The eight principles
- Freedom of Information Act 2000 (FOI)
  - Who it affects
  - Public Rights
  - Publication Schemes
  - Exemptions
  - Key Points
- Computer Misuse

Motivation for the DPA

- To protect individuals from:
  - The use of inaccurate, incomplete or irrelevant personal information
  - The use of personal information by unauthorized people
  - The use of personal information for purposes other than the purpose for which it was gathered
  - Also some sensitivity to transborder data flows and the need to avoid data havens in unregulated jurisdictions
- Rough timeline:
  - Concerns surface in the 1970's (Lindop report more or less says "free text systems should not be used).
  - First act in 1984 – protect people from misuse of data by organisations
  - European directive on Data Protection 1995 – protection from misuse of data on the Internet)
  - Revised act repeals the first act in 1998 – balancing freedom to process against personal privacy

Definitions

- Data: information in electronic or manual form
- Data subject: individual who is the subject of the personal data
- Personal Data: Expression of opinion, or fact, E-mail address, photos, video footage… New category of *sensitive data (e.g. ethnic origin, trade union memership)*.
- Data Controller: determines why or how personal data is processed
- Data Processor: anyone processing data for the data controller who is not an employee of the data controller
- Processing: Reviewing, holding, sorting, deleting, correlating, modifying, …
- Relevant Filing System: Readily accessible information about living individuals
- Information Commissioner: New name for Data Protection Registrar

New Provisions in the 1998 Act

- Broader than the old act to comply with European requirements and new threats.
- Strengthened rights for data subjects.
- Extended to cover manual filing systems.
- Sensitive data is a new category and has stronger processing requirements.
- Rules about export of data to non-EEA countries.

Principles of the act – 1.

- Non-sensitive Personal data must be processed *fairly* and *lawfully* and shall not be processed unless one of the below is met (schedule 2).
  - Consent – *most important*
  - Contract
  - Legal Obligation
  - Vital interests of subject (life or death!)
  - Public functions
  - Balance of interest

Sensitive Personal Data

- Racial or ethnic origin
- Political opinions
- Religious/similar beliefs
- Trade Union Membership
- Health
- Sexual Life
- Offences

Sensitive Personal Data

- May only be held if one of the below is met:
  - Explicit and *informed* consent
  - Employment Law
  - Vital Interests of Subject
  - Legal Proceedings
  - Medical Purposes (by medical professionals)
  - Equal opportunities monitoring

Consent

- "Freely given specific and *informed* indication of wishes by which the data subject signifies agreement to personal data relating to him/her being processed."
- Can't use implied consent – must get forms back.
- Can't use blanket consent as condition of entry.

Fair processing

- Must not intentionally or otherwise deceive or mislead subject as to purpose of data use/collection.
- Must identify to subject data controller/nominated representative.
- Must identify to subject purpose of processing data.
- Exceptions are disproportionate effort (direct marketing not allowed) or legal obligation.

DPA Principle 2

- Data must be obtained only for one or more specified lawful purposes and shall not be further processed in any manner incompatible with that purpose or purposes.
  - Must not use data for a new incompatible purpose without subject's consent.
  - Have a data protection statement that explains why data will be held and requesting consent in the case of sensitive personal data#
  - The Information Commissioner must be notified by Data Controllers specifying what data will be collected and for what purpose

DPA Principles 3 & 4

- Personal data must be adequate, relevant and not excessive in relation to the purpose or purposes for which they are to be processed.
  - Volume and type of data can only be justified in relation to the purposes registered with the Information Commissioner
- Personal data shall be accurate and, where necessary, kept up to date.
  - Data holdings must be under continuous review and policies need to be in place to delete old data. Issues about things like addresses for students.

DPA Principle 5

- Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or purposes.
  - Establish how long data needs to be retained. Some needs to be retained forever. (Should School Qualifications be retained forever?)
  - Ensure that such data is really erased (e.g. from dumps, backups, …).

DPA Principle 6

- Personal data must be processed in accordance with the rights of data subjects
  - This means that you cannot do things that violate the rights given to data subjects under the new act, especially denying access to data.

Rights of data subjects

- Must be informed if personal data are being processed and given a description of the personal data
- Be informed of the purpose for which data is being held and processed
- Must be informed of people or organisations to whom personal data might be disclosed
- Be provided with an intelligible description of the specific data held about them
- Be provided with a description of the source of personal data
- May prevent processing for purposes of direct marketing
- May prevent processing likely to cause damage and distress
- Right to compensation in the case of damage caused by processing of personal data in violation of the act.
- Right to see the methods used to score the individual used by credit scoring agencies.

Access rights

- Right to have communicated to him/her in an intelligible form the information constituting the data.
- No right to rifle through filing systems, computers etc.
- Right to be informed of logic involved in automated processing.
- Request must be in writing, fee up to £10 may be charged and identity may be thoroughly checked.

Access rights

- Data may be witheld if disclosure would disclose data about a third party unless:
  - Third party has consented to disclosure
  - It is reasonable to comply without the third party's consent.
  - Duty of confidentiality, steps taken to seek consent, express refusal of third party.
  - Witnesses, confidential reports, access to references .

Access rights

- Don't have to disclose references you have written but must disclose those you have received unless the writer explicitly asked them to kept confidential.
- 40 days to comply (or state reason for refusal to comply) with requests.
- Don't need to comply with repeat requests until a reasonable amount of time has elapsed.
- Don't need to comply if disproportionate effort would be involved.
- Subject must provide reasonable data you request to assist in finding the data.

Enforced Access

- It is an offence to force subjects to exercise their access rights to data held by others
  - Includes data about cautions, criminal convictions and certain social security records

Right to prevent processing

- Unwarranted substantial damage or distress to subject.
- 21 days to comply with request.
- Exemption if processing is necessary for performance of contract with subject or there is a legal obligation, or the vital interests of the subject are at stake.

Exemptions to access rights

- Prevention and detection of crime
- Apprehension or prosecution of offenders
- Collection of tax or other duty
- Research, history, statistics.
- Exam marks – 40 days after date of announcement or 5 months of access request.
- Confidential references.

DPA Principle 7

- Appropriate technical or organisational measures shall be taken against unauthorised or unlawful processing of data and against accidental loss, damage or destruction of personal data.
  - Careful selection of IT staff
  - Appropriate backup policies
  - Use of passwords, encryption etc
  - Use of integrity checking

DPA Principle 8

- Personal data shall not be transferred to a country or territory outside the EEA 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.
  - Websites are problematic in terms of jurisdiction.

Notifying the Information Commissioner

- Each legal entity intending to hold or process personal data must register with the Information Commissioner.
- The register is public.
- Penalties for failure to comply are substantial.
- The Information Commissioner has strong powers of search and seizure if violations of the DPA are suspected.

Exercise

- Get into a group of four people.
- Look at the entry in the Data Protection Register for TESCO.
- As a group choose one of the Purposes listed
- Do the following:
  - Individually, list your top three or four likely violation of the DPA for the data collected under the purpose chosen by your group
  - Get together with one other group member and combine your list to create a joint top three potential violations. List what principle they violate and how you think a violation could arise.
  - Come together as a group of four and combine your lists to create a top three for your group of four.
  - As a group, choose one of the violations and suggest what kind of countermeasures would be appropriate to reduce the liklihood of such a violation