Professional Issues: Data Protection, Privacy and Freedom of Information

Massimo Felici

School of informatics

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 unauthorised 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 membership).
- **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

DTA Principles

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

- 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.

DTA Principles

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

DTA Principles

- 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

DTA Principles

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,...)

DTA Principles

- 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 withheld 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

DTA Principles

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

DTA Principles

- 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.

Activity 10

- Read the paper describing *Clique – a social network supporting identity management*
- Identify issues that relate to Data Protection and Privacy
- Identify critical aspects of the discussed solution addressing specific issues of Data Protection and Privacy
- Discuss implications either for end-users or service providers
- Discuss or question any relevant aspect in the course wiki

Freedom of Information

Massimo Felici

School of informatics

The Freedom of Information Act 2000

- The FOI act 2000 gives individuals the right to access information about certain public bodies by two routes:
  - Publication Scheme
  - General Right of Access
- Any member of the public can apply for access to information held by a public body
- The act has enforcement mechanisms if the body fails to release the information

The Freedom of Information Act 2000

- General right of access by any member of the public
- There are exemptions but disclosure can be forced on grounds of public interest
- New office of the Information commissioner with an Information Tribunal with powers to enforce rights of access
- Public bodies must have a publication scheme that makes release of information routine

Public Rights

- To know whether relevant information exists: the duty to confirm or deny
- To have the information released (and, where possible, in the manner requested)
- To be provided with reasons for a decision to withhold information
- All requests must be in "permanent form"
- Reply must be sent within 20 working days

Publication Scheme

- Guide to the information a public body is making available without the need for an FOI request
  - This is relatively inexpensive and is a way of avoiding many FOI requests
  - Guide to types of information available NOT a list of all of it
- Scheme has to be approved by Information Commissioner
- Model schemes available on Information Commissioners web site
- Scotland has its own Information Commissioner
  - Scottish guidance:
    http://www.itspublicknowledge.info/PublicationSchemeGuidance/
  - Edinburgh University Publication Scheme:
    http://www.pubs.recordsmanagement.ed.ac.uk/index.cfm

Exemptions

- Many exemptions, some absolute, some qualified e.g.
  - Commercial Interest
  - Communicating with the Queen
  - Law enforcement
  - Legal Professional Privilege
  - Parliamentary Privilege
- Need to Apply Tests before using Qualified Exemptions
  - Prejudice & Adverse Affect
  - Public Interest (not same as of Interest to the Public)
- FOI does not override DPA but DPA is not an excuse not to comply with FOI requests
  - Data protection will often take priority
  - FOI requests may be partially fulfilled avoiding release if personal data
  - Public interest may allow release of personal data

Vexatious or Repeated Requests

- Vexatious means:
  - clearly does not have any serious purpose or value
  - is designed to cause disruption or annoyance
  - has the effect of harassing the public authority
  - can otherwise fairly be characterised as obsessive or manifestly unreasonable.

- Repeated means:
  - More often than a "reasonable interval"
  - Requests asking if previously requested information has changed are OK
  - Reply can say when info is next to be updated and a request before then would be "repeated"

Key points to note

- Requests can be received by anyone within the organisation and do not need to refer to the Freedom of Information Act
- Requests must be in writing (including e-mail, fax etc)
- Requests must be dealt within 20 working days
- No obligation to provide information which is already in the public domain/accessible by other means (e.g. via the publication scheme or in a book the organisation may hold)
- No obligation to create information that the Organisation does not already hold (e.g. statistical summaries)
- Organisation may charge a fee for the provision of information — Charges must be calculated in accordance with the fees regulations prescribed by the Department for Constitutional Affairs. Currently £50 maximum.

Activity 11

- Read the paper on *MPs' allowances and FoI requests*
- Write your opinion on the section discussing the release of MPs addresses (§4 Members' addresses)
- Construct an argument for the release of the addresses and one against the release of addresses
- Comment who you think has written the stronger argument
- Discuss or question any relevant aspect in the course wiki

Required Readings

- Textbook (Bott)
  - Chapter 14 on Data protection, privacy and freedom of information