

UK UNIX User Group

Winter Conference 1999

Data Protection Issues

by

Shelagh Gaskill

Partner, Masons Solicitors



Fair and lawful processing

- ✦ The first data protection principle: data must be processed fairly and lawfully and must not be processed unless:
 - ✦ Schedule 2 is satisfied and
 - ✦ Schedule 3 is also satisfied for processing sensitive data

Schedule 2

- ◆ Schedule 2 conditions:
 - ◆ consent
 - ◆ performance of a contract
 - ◆ compliance with a legal obligation
 - ◆ protect the vital interests of the data subject
 - ◆ exercise of a government function
 - ◆ legitimate interests

Sensitive data

- ◆ Sensitive data comprise:
 - ◆ racial or ethnic origin
 - ◆ political opinions
 - ◆ religious beliefs
 - ◆ trade union membership
 - ◆ physical or mental health
 - ◆ sexual life
 - ◆ criminal offences/criminal sentences
- ◆ Financial information is not sensitive

Schedule 3

◆ Schedule 3 conditions:

- ◆ explicit consent
- ◆ purposes in connection with employment
- ◆ vital interests of the data subject
- ◆ non-profit making body
- ◆ information made public by data subjects
- ◆ establishing, exercising or defending legal rights

more ...

Schedule 3



- ◆ Schedule 3 conditions continued:
 - ◆ government functions
 - ◆ medical purposes by a health professional
 - ◆ monitoring of equality of opportunity

Consent

- ◆ Difference between consent and explicit consent:
 - ◆ Schedule 2 = consent
 - ◆ Schedule 3 = explicit consent
 - ◆ Transfers abroad = consent

Consent



- ◆ How to obtain consent
- ◆ Difference between notification and consent

Article 10/11 notices

- ✦ Processing **will not** be fair unless certain information is given to data subjects where:
 - ✦ the data are obtained directly from the data subject (**Article 10 Notice**)
 - ✦ the data are obtained from a third party in respect of the data subject (**Article 11 Notice**)
- ✦ Do not have to give Article 11 Notice where disproportionate effort or legal requirement

Contents of Notices

- ◆ Identity of the data controller
- ◆ Description of the data (in particular sensitive data and transactional data)
- ◆ Data controllers' purposes
- ◆ Description of recipients and their purposes

Contents of Notices

- ◆ Categories of data to be disclosed
- ◆ Existence of the right of subject access
- ◆ Consequences of failure to give information
- ◆ Transfers outside the EEA
- ◆ Right to have inaccuracies corrected
- ◆ Absolute right to opt-out of direct marketing

Manual files

- ✦ Policy decision whether or not to give access
- ✦ If **yes**:
 - ✦ need training to ensure employees know that what they write may be disclosed
 - ✦ try to avoid a secret file culture emerging
- ✦ If **no**:
 - ✦ need to review files (audit) and decide whether they are caught under the Act

Manual files



- ✦ Not all manual files are caught
- ✦ Only those that fall within the definition of a relevant filing system

Manual files

“Any **set** of information relating to **individuals** to the extent that ... the set is **structured**, either by **reference to individuals** or ... **criteria** relating to individuals, in such a way that **specific** information relating to a **particular** individual is **readily accessible**.”

Manual files



- ◆ Files that are not caught:
 - ◆ unstructured, miscellaneous collections of documents
 - ◆ files arranged by reference to corporate entities

Transfers abroad

- ◆ Eighth data protection principle
- ◆ Personal data must not be transferred to a country outside the EEA unless it ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data

Transfers abroad



- ◆ Various factors to consider:
 - ◆ the nature of the personal data
 - ◆ the country of origin and final destination
 - ◆ the purposes for the processing
 - ◆ the law in force in that country
 - ◆ international obligations of that country
 - ◆ security measures

Exemptions

- ◆ Do not need an adequate level of security if:
 - ◆ data subject has given consent
 - ◆ transfer is necessary for contract between the controller and data subject
 - ◆ transfer is for establishing, exercising or defending legal rights

Main Areas of Cost

- ◆ Subject information requests for archived and back-up data
- ◆ Contracts with third party processors
- ◆ Issuing Article 10 and Article 11 notices
- ◆ IT systems implications

Archived and Back-up Data

- ✦ Back-up data used to be excluded from subject access requests under section 34(4)
- ✦ So long as they were copies which duplicated originals

Archived and Back-up Data

- ✦ Archived data were excluded from subject access requests under the old Act so long as they did not fall under the definition paragraph (c) of section 1(5) which described a data user. Data had to be in a form in which they have been or are intended to be processed or (though not for the time being in that form) are in a form into which they have been converted after being so processed and with a view to being further so processed on a subsequent occasion.

Archived and Back-up Data

- ✦ Now applies to manual files as well as to computerised data but only to manual files which form part of a relevant filing system

Section 7 - Rights of Access to Personal Data

- ◆ Request in writing and payment of fee
- ◆ Right to be informed:
 - ◆ whether his personal data are being processed and if so:
 - ◆ to be given a description of the personal data
 - ◆ the purposes for the processing
 - ◆ the recipients of the data
 - ◆ recipient includes employees and data processors

Section 7 - Rights of Access to Personal Data

- ✦ Also right to have communicated to him in an intelligible form:
 - ✦ the information constituting the personal data and
 - ✦ information about the source of those data

Section 7 - Rights of Access to Personal Data

- ✦ And where the individual's personal data have been processed by automatic means and this has constituted the sole basis for any decision significantly affecting him, the logic involved in that decision taking (excluding trade secrets)

Cost Implications of Section 7

- ◆ New processes and procedures:
 - ◆ sources
 - ◆ recipients (including own employees)

Data Protection Audit

- ✦ What kinds of data are processed?
- ✦ Does the processing comply with data protection law, the general law and best practice?
- ✦ Distribute questionnaires to those with managerial or operational responsibility for information within the organisation

Data Protection Audit

◆ The questionnaire should cover:

- ◆ collection
- ◆ storage
- ◆ access
- ◆ processing
- ◆ disclosure
- ◆ subject information procedures
- ◆ data quality
- ◆ security
- ◆ destruction and archiving
- ◆ transfer overseas

Data Protection Audit

- ✦ Most importantly the audit should gather information on all the internal and external third parties who will be data processors and with whom the organisation must have written contracts

Who is a data processor?

- ◆ Anyone instructed by the controller to perform any operation on personal data
- ◆ Excludes employees
- ◆ New requirements: contract in writing
 - ◆ adequate security measures
 - ◆ must only act on controller's instructions
 - ◆ imposes obligations similar to the seventh principle

Data Processors



- ◆ Seventh principle:
 - ◆ security measures against the unauthorised or unlawful processing of personal data and
 - ◆ accidental loss or destruction of personal data

Contracts with Processors

◆ Typical Clauses

- ◆ Definitions
- ◆ Standards or performance
- ◆ Length of term
- ◆ Obligations of the data controller
- ◆ Obligations of the data processor

Contracts with Processors

- ◆ Ownership of data
- ◆ Confidentiality
- ◆ Termination for breach
- ◆ Consequences of termination
- ◆ Schedule of data controller's requirements or authorised activities of the data processor

IT Systems Implications

- ✦ Amendments to legacy systems or the design of new systems
- ✦ Operative date is 24 October 2001 so three years in which to design, build, implement and roll-out compliant systems
- ✦ Thirty four systems implications of the new Act involving new fields, new functionality and new inter-relationships