

IT Law

Data protection

Solution: create Data Protection Acts

| Regulates how data are stored and who has access.

Personal Data

Data stored and processed about a data subject.

GDPR applies to any organisation anywhere in the world if data are collected relating to any EU resident.

Data protection officer:

Required for:

- all public authorities
- all entities involved with monitoring of data subjects
- all entities conducting large scale processing of “special” personal data

Data Protection Principles - 7

- Processing of personal data must be **lawful, fair and transparent**
- Purposes of processing of personal data **must be specified, explicit and legitimate**
- Personal data must be adequate, relevant and not excessive
- Personal data must be accurate and kept up to date
- Personal data must be kept for **no longer than is necessary**
- Personal data must be **processed in a secure manner**
- The controller is accountable

Rights

- Right of access by the data subject, responds within 1 month (normally)
- Right to rectification
- Right to erasure (to be forgotten)
- Right to restriction of processing
- Right to data portability
- Right to object and automated decision-making

Freedom of Information

Publication schemes: lists of information published by a public authority

Requests

- In writing
- Response must say whether the information exists and give it
- Fee may be charged
- Limit of 20 working days (of customer can pay fee to extend to 3 months)

Some organisations are excluded from FOI 2000:

- Security services
- Trade secrets
- Court records
- “Vexacious” requests

Since

Covers all **public** bodies in the UK — includes local government, NHS, universities, police, parliament ...

Which of the following organisations are NOT covered by the Freedom of Information Act 2000?

- ☐ Local authorities
- ☐ National Park authorities
- ☐ Government Departments
- ☒ Newspapers
- ☒ MI5
- ☐ Universities
- ☐ Schools

Publication Schemes ~

Lists of information published (or intended to be) by a public authority

Enforcement ~

Information Commissioner can adjudicate and can enforce disclosure, but the public authority's complaints process must be followed first.

Computer Misuse

To protect unauthorised access of data via computer

CMA, Act 1990

Liable to 3 offences:

- Unauthorised access to computer material
- Unauthorised access with intent to commit or facilitate further offences
- Unauthorised modification of computer material

Police and Justice Act 2006

- Fixes Denial of Service attacks
- Increase penalty for hacking

Monitoring and recorded by businesses is legal, for:

- Standards purposes
- Compliance with regulation
- Effective system use

- Prevention or detection of crime
- Detecting unauthorised use