Data protection

Data protection

- *EU* has sought to harmonise national data protection laws:
  - European Directive on Data Protection 1995
  - General Data Protection Regulation (GDPR) 2018
- *USA* has no comprehensive data protection law, but a patchwork of state laws and regulations.
- Many other countries have weak data protection laws or none at all.
- Much potential for conflict:
  - where data is sent from one country to another
  - where data is held by multinationals (e.g., Google, Facebook).

UK Data Protection Acts

- **Data Protection Act 1984 (DPA)** protected individuals from misuse of data by large organisations:
  - use of inaccurate/incomplete/ irrelevant personal data
  - use of personal data by unauthorised persons
  - use of personal data for purposes other than those for which it was collected.

UK Data Protection Acts

- **Data Protection Act 1998 (DPA)**
  - conforms to European Directive on Data Protection 1995
  - covers Internet data as well as stored data
  - no longer assumes that large organisations are the only possible offenders.

UK Data Protection Acts

- **Data Protection Act 2018 (DPA)**
  - Updates and supersedes the Data Protection Act 1998.
  - Supplements the GPDR and refines the application of it in the UK.
  - Also covers areas such as law enforcement and intelligence services.

Data Protection Acts

Terminology

- *Data:* information that is processed or collected.
- *Personal data:* data that relates to a living person who can be identified.
- *Data subject:* the person that the data refers to.
- *Data controller:* a person within an organisation who determines how or why personal data is processed.
- *Processing:* obtaining, recording, or holding information or data, or carrying out operations on it.
- *Information Commissioner:* government-appointed official responsible for enforcing the DPA.

Terminology

- *Sensitive personal data:*
  - racial/ethnic group
  - political/religious views
  - physical/mental health
  - sexual orientation
  - criminal record (including allegations)
  - genetic information.
- Sensitive personal data is subject to stricter rules for processing.

Principles

Data Protection Act 1998

1. “Personal data shall be processed fairly and lawfully and in particular shall not be processed unless (a) [the data subject grants consent], and (b) in the case of sensitive personal data, [the data subject grants explicit consent].”

We will retain your data to provide you with the best possible service. Do you agree?

☑

Opting-out is not explicit consent.

2. “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.”

- E.g., individuals’ medical records may not be used for research (even if anonymised), except with their consent.

Principles

Data Protection Act 1998

3. “Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.”
4. “Personal data shall be accurate and, where necessary, kept up to date.”
5. “Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.”
   - E.g., financial data must be kept for 7 years, for auditing and taxation.

Principles
Data Protection Act 1998

6. “Personal data shall be processed in accordance with the rights of data subjects under this Act.”
   - Data subjects are entitled to be told what data is held about them, why it is held, which other organisations the data may be disclosed to, etc.
7. “Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.”
   - The organisation must keep the personal data secure (integrity checks, access controls, backups, employee vetting).

Principles

Data Protection Act 1998

8. “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.”

UK Data Protection Act 2018

- The General Data Protection Regulations (GDPR) permits member states to supplement or deviate from it with national laws.
- Data Protection Act 2018 updates data protection laws in the United Kingdom to supplement the GDPR.
  - covering aspects beyond the scope of the GDPR, such as national security.
  - permitted deviations, e.g. lower age of consent.
- Data Protection Act 2018 does not transpose GDPR into UK law, for the purposes of leaving the European Union this is achieved by other legislation.

Data protection