13. DATA PROTECTION, PRIVACY AND FREEDOM OF INFORMATION

13.1 INTRODUCTION

- **GDPR**: General Data Protection Regulation became law on 25 May 2018 across EU countries.
    - Evolution of EU data protection laws from the 1970s.
    - Modern concern: organisations collecting, tracking, and using personal data.
    - Potential financial penalties drive senior executives to improve data protection.
- **UK GDPR**: After Brexit, the UK adopted UK GDPR, part of the Data Protection Act (DPA) 2018.
- **Privacy Concerns**:
    - Individuals want to keep personal information private (bank info, medical history, voting).
    - UK Human Rights Act 1998 ensures privacy rights (European Convention on Human Rights, Section 8(1)).
- **Investigatory Powers**:
    - Regulation of Investigatory Powers Act 2000 and Investigatory Powers Act 2016 regulate monitoring (emails, phone calls).
- **Freedom of Information**:
    - Governments often reluctant to release information.
    - Pressure led to Freedom of Information laws (e.g., UK FOI Act 2000).
    - Other countries: Australia, Canada, USA (1970s–1980s).

IT context:
Modern IT systems are central to data collection, surveillance, communication and record keeping, making IT professionals directly responsible for protecting privacy and complying with data protection and freedom of information laws.

13.2 DATA PROTECTION

Data protection laws evolved in response to increasing use of computers and digital storage from the 1970s onwards. Early concerns included:

- large-scale data collection
- data misuse
- unauthorised access
- inaccurate or outdated data

These concerns led to **Convention 108** and later UK legislation such as the **DPA 1984** and **DPA 1998**.

By the 2010s, the rise of:

- social media
- online tracking
- data profiling
  created new risks, including targeted political and commercial influence.

This resulted in the introduction of the **GDPR (2016)**, enforced in 2018, and later the **UK GDPR (2021)**.

IT context:
IT systems enable data analytics, profiling, cloud storage and cross-border data flows, making compliance with modern data protection law essential in system design.

13.2.1 Protected Data

The DPA 2018 applies to **personal data relating to identified or identifiable living individuals**. Examples include:

- names, addresses, emails
- IP addresses and cookies
- CCTV footage
- biometric and genetic data
- political or religious beliefs

The law does not distinguish between **data and information**, treating both equally.

- **Anonymous data** is not covered
- **Pseudonymous data** is covered if re-identification is possible

Excluded categories include:

- domestic or household data
- law enforcement and intelligence data (covered separately)
- special purposes (journalism, academia, art)

IT context:
Developers must consider whether datasets can be re-identified by combining multiple data points, especially in analytics and AI systems.

13.2.2 Terminology

Data Controller: Determines **why and how** personal data is processed.

Data Processor: Processes data on behalf of the controller (e.g. cloud providers, SaaS platforms).

Data Subject: The individual whose data is processed.

Processing: Any operation on data, including collection, storage, use or deletion.

Special Categories of Personal Data

Includes:

- ethnicity, race
- political/religious opinions
- health data
- biometric and genetic data

Processing is **prohibited by default**, unless a valid exemption applies.

IT context:
Cloud providers, hosting companies and analytics services often act as data processors and must meet contractual GDPR obligations.

13.2.3 Principles of UK GDPR

UK GDPR defines **seven principles**.

1. Lawfulness, Fairness and Transparency

Data must be processed lawfully, fairly and transparently.

IT context:
Privacy notices, cookie banners and clear user consent flows are required in digital systems.

2. Purpose Limitation

Data must be collected for **specific and legitimate purposes**.

IT context:
Reusing data for analytics or marketing requires reassessing lawful basis and possibly new consent.

3. Data Minimization

Only necessary data should be collected.

IT context:
Forms and databases should avoid collecting unnecessary attributes (e.g. marital status).

4. Accuracy

Data must be accurate and kept up to date.

IT context:
Systems should allow users to update their personal information easily.

5. Storage Limitation

Data should not be kept longer than necessary.

IT context:
Automated retention policies and secure deletion of backups are essential.

6. Security

Appropriate technical and organisational security measures must be applied.

IT context:
Includes encryption, access controls, MFA, staff training and regular security reviews.

7. Accountability

Data controllers must **demonstrate compliance**.

IT context:
Documentation, audit logs, DPIAs and staff training records support accountability.

13.2.4 Lawful Basis for Processing

Six lawful bases exist:

1. **Consent:** Clear, informed and revocable permission.
2. **Contract:** Necessary for fulfilling a contract.
3. **Legal Obligation:** Required by law.
4. **Legitimate Interests:** Processing expected and not harmful to individuals.
5. **Public Task:** Processing required for public interest tasks.
6. **Vital Interests:** Used to protect life in emergencies.

IT context:
Different parts of online forms may require different lawful bases (e.g. checkout vs marketing).

13.2.5 Rights of Data Subjects

Rights include:

1. right to be informed
2. right of access

3. right to rectification
4. right to erasure
5. right to restrict processing
6. right to data portability
7. right to object
8. rights related to automated decision-making

IT context:
Systems must support data export, deletion and explanation of automated decisions.

13.2.6 Personal Data Breaches

A breach includes:

- unauthorised access
- accidental loss
- data corruption
- service unavailability

Notifiable breaches must be reported to the ICO within **72 hours**.

IT context:
Incident detection, logging and breach response workflows are critical in IT systems.

13.2.7 Operation and Enforcement

The ICO can impose fines of:

- up to **£17.5 million or 4% turnover**
- lower tier: **£8.7 million or 2% turnover**

High-profile enforcement actions highlight the importance of compliance.

IT context:
Security failures, weak authentication and poor system design are common causes of fines.

13.2.8 Organisational Responsibilities

- Staff training is essential
- Most employees process personal data
- Some organisations must appoint a **Data Protection Officer (DPO)**

IT context:
DPOs work closely with IT teams on system architecture, security and compliance decisions.

13.3 Privacy

Focus: Privacy in IT systems and internet communications.

Key Principles for Organisations:

- Organisations (telecoms, IT service providers, businesses) **can monitor or record communications** without user consent if done for legitimate purposes:
    1. Establish facts (e.g., date/time of an order).
    2. Ensure compliance with company policies/procedures.
    3. Assess or demonstrate standards.
    4. Prevent or detect crime (computer-related or general).
    5. Investigate unauthorized use of IT/telecom systems.
    6. Ensure effective system operation (virus/DoS detection).
    7. Identify business vs personal communications.
    8. Monitor confidential counseling services (users may remain anonymous).

Requirements for Lawful Monitoring in IT Context:

- Must be carried out by the **system controller** (e.g., business running the telecom or IT system).
- Users should be **informed where reasonable**.
- Recording must be **relevant to business/system activity** (e.g., call center training).
- Organisations must maintain **security and privacy safeguards** while monitoring.

Government Powers:

- Police, intelligence, and tax authorities may request **interception warrants** for specific targets.
- Interception is highly controlled; general monitoring applies more widely.

IT Application Notes:

- Ensure monitoring systems include **logging, consent notices, and access controls**.
- Implement monitoring only for **business objectives or system security purposes**.
- Any personal data collected must comply with **Data Protection Act 2018 (DPA)** and **UK GDPR**.
- Examples: email monitoring during employee absence, network monitoring for malware/DoS attacks.

13.4 Freedom of Information (FOI)

Focus: Access to public sector information; implications for IT/document systems.

Key Principles:

- Any **member of public** can request information from **public authorities**.
- FOI does **not apply to personal data**; personal information must comply with GDPR/DPA.

- Authorities must **publish certain information routinely** (publication scheme approved by ICO).
- Public interest can override exemptions: some sensitive info may still be disclosed.

IT / System Context:

- FOI compliance requires **record/document management systems** to track, store, and retrieve public records efficiently.
- **Redaction tools** needed to remove personal or confidential data before disclosure.
- Routine publication examples: senior staff salaries, public contracts.
- FOI requests must be **assessed for exemptions**, and guidance may involve legal/ICO advice.

Case-Study Notes for IT Application:

- Maintain clear **metadata and audit trails** in IT systems for FOI requests.
- Implement **role-based access** so staff handling FOI requests can redact sensitive data.
- Ensure **public contract and document storage systems** allow fast retrieval for compliance.