General Data Protection Regulations

General Data Protection Regulation (GDPR)

- The **General Data Protection Regulation (GDPR)** is European Union (EU) law for data protection and privacy.
- The law covers all individuals in the EU and European Economic Area (EEA).
- GDPR supersedes the European Directive on Data Protection and unlike the directive, the regulation became enforceable in May 2018 without requiring enabling national legislation.
- GDPR comprises of 99 articles, gathered into 11 chapters (specific interest are the principles and rights of the data subject).

Principles

GDPR Principles (Chapter 2, Article 5)

- GDPR defines seven core principles that act as the foundation for protection of personal data:
  - lawfulness, fairness and transparency
  - purpose limitation
  - data minimisation
  - accuracy
  - storage limitation
  - integrity and confidentiality
  - accountability
- GDPR principles can be mapped to the principles of the UK Data Protection Act 1998.

GDPR Principles (Chapter 2, Article 5)

UK DPA 1998 Principles	GDPR Principles
1 – fair and lawful	1 – lawfulness, fairness and transparency
2 – specified and lawful purposes	2 – purpose limitation
3 – adequate and relevant	3 – data minimisation
4 – accurate	4 – accuracy
5 – retention	5 – storage limitation
6 – rights	Chapter 3 provisions
7 – technical and operational security	6 – integrity and confidentiality
8 – data transfers	Chapter 5 provisions
	7 – accountability

Rights of
Data subjects

GDPR Rights of Data Subjects (Chapter 3)

- The GDPR affords data subjects several rights, not all of these rights are absolute and restrictions will depend on the scenario.

GDPR Rights of Data Subjects

1. individuals have a **right to be informed** (§1), specifically about the collection and processing of personal data as well as the retention period and any shared access.
2. individuals have a **right to access** (§2, article 15), specifically the confirmation of the existence of their personal data and a copy of it.
3. individuals have the **right to rectification** (§3, article 16), specifically inaccurate personal data can be altered and completed (GDPR does not define accuracy).
4. individuals have the **right to erasure** (§3, article 17), specifically data no longer required for the collected purposes can be erased (placed beyond use in back-ups).

GDPR Rights of Data Subjects

5. individuals have the **right to restrict processing** (§3, article 18), specifically restrict processing for a time period while data is adjusted or verified.
6. individuals have the **right to data portability** (§3 article 20), specifically personal data can be obtained and utilised across services by the individual.
7. individuals have the **right to object** (§4, article 21), specifically request the processing of data (an absolute right in the case of direct marketing).
8. individuals also have **rights in respect to automated individual decision making, including profiling** (§4, article 22), , specifically individuals must be made aware of such processes and have the opportunity to challenge or request human involvement.

Material and Territorial Scope

GDPR Material Scope (Chapter 1, Article 2)

- The GDPR does not cover all aspects of personal data in the United Kingdom.
- The GDPR does cover automated processing of digital data, but also structured data on paper etc.
- The GDPR does not apply where activities are outside European Union (EU) Law, e.g. national security.
- The GDPR does not apply when activities concerning foreign policy, such as humanitarian aid or conflicts, or unstructured data (e.g. handwritten notes) held by a public authority susceptible to Freedom of Information requests.
- The GDPR does not apply to individuals in terms of their day-to-day private activities.

GDPR Territorial Scope (Chapter 1, Article 3)

- The GDPR applies to controllers and processors that are established in the European Union, even if the processing occurs outside of the EU.
- The GDPR applies to data subjects that are within in the European Union, even if the controller and/or processor are outside of the EU.
  - specifically where activities relate to a good or service, involving payment or otherwise.
  - behaviour monitoring where that behaviour is occurring within in the European Union.

Restricted transfers

International data transfers and GDPR

- GDPR restricts the transfer of data to international organisations and countries outside the European Union (EU) and European Economic Area (EEA).
  - Typical example would be making data accessible to an entity outside the realm of the GDPR.
- Transfer and transit are not the same,
  - e.g. data being transferred between two EEA countries, passing through non-EEA countries would not be a restricted transfer.
  - data being passed from an EEA country to a non-EEA country would typically be deemed a restricted transfer.
- A **restricted transfer** in accordance with GDPR requires consideration of many questions.

Restricted transfer - Adequacy Decision

- European Commission (EC) can determine if non-EEA countries have suitable safeguards in place to ensure data protection.
  - protection for data subject rights and freedoms.
  - appropriate legal frameworks.
- EC makes adequacy decision and then it permits transfer to those non-EEA countries as long as GDPR is upheld.
  - New Zealand and Switzerland have such decisions.
- If there is no adequacy decision, further questions need to be considered.

Restricted transfer - Appropriate Safeguards (Article 46)

- Restricted transfer may be possible, if sufficient safeguards are met between parties and GDPR is upheld.
- There are various different safeguards (Article 46):
  - a legally binding and enforceable instrument between public authorities or bodies;
  - binding corporate rules;
  - standard data protection clauses adopted by the Commission;
  - standard data protection clauses adopted by a supervisory authority and approved by the Commission;
  - an approved code of conduct pursuant together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards;
  - an approved certification mechanism together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards;
  - contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation;
  - provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.
- If there is no appropriate safeguard, further questions need to be considered.

Restricted transfer - Exceptions (Article 49)

- Restricted transfers may permitted despite the lack of adequacy decisions and appropriate safeguards.
- Exceptions are permitted, but they **must be actual exceptions**.
  - normal operation should not rely on exceptions to perform transfers.
- While exceptions are permitted, they are expected to be interpreted narrowly and the European Data Protection Board (EDPB) has issued guidance.
  - EDPB comprises of representatives from data protection authorities from EU member states and EEA countries.
  - EDPB develop and provide guidance to adhere to the GDPR.

Restricted transfer - Exceptions (Article 49)

1. Individuals have given explicit consent after being advised of the risks from lack of adequacy decisions and appropriate safeguards.
2. Contract between parties and a restricted transfer may occur to fulfil the contract.
3. Contract between parties, that benefits others, then a restricted transfer may occur to fulfil the contract.
4. Restricted transfer necessary in the public interest.
5. Restricted transfer necessary for initiation, exercise or defence of legal claim.
6. Restricted transfer necessary to protect vital interests of individual and then must be incapable of giving consent (e.g. threat to life).
7. Restricted transfer from a public register (e.g. criminal convictions).
8. One-off restricted transfer for which you have compelling and legitimate interests.

General Data Protection Regulations