General Data Protection Regulation

Based on the Pinsent Mason Paper

New Features of the GDPR

- Accountability measures: GDPR requires compliance and *evidence* of compliance:
  - documented policies and procedures,
  - records of consents etc.
  - Registration with supervisory authorities (e.g. ICO) no longer required.
    - internal record-keeping obligations
    - supervisory authorities can demand information, conduct audits, order remediation etc.
- Territorial scope (Article 3)
  - extending to non-EU controllers and processors in some cases.
  - "one stop shop": organisations operating in multiple EU Member States report to only one main supervisory authority.
  - Consistency mechanism to promote harmonisation across EU Member States and resolve cross-border issues.

New Features of the GDPR

- Amended definitions (Article 4), e.g.
  - expanded definitions of "personal data" and "data subject" (catching more types of data and processing operations)
  - new definitions e.g. "pseudonymisation" and "profiling".
  - Consent will be more difficult to use as a legal basis.
- Direct statutory obligations (Articles 28, 30, 44-49, 33(2)) and liability (Article 82) on processors, and additional requirements regarding the minimum terms that must be included in personal data processing contracts (Article 28).
- Tighter rules on international transfers, applicable to both controllers and processors.

New Features of the GDPR

- Requirement for data protection impact assessments before initiating certain types of processing or other processing operations likely to result in a high risk to individuals:
  - must consider at least the issues specified by the Regulation (Article 35)
  - consultation with the supervisory authority required in some circumstances (Article 36).
- Controllers and processors required to appoint a data protection officer in certain circumstances (Articles 37-39).
- Mechanisms for the purposes of demonstrating compliance with the Regulation, involving codes of conduct (Articles 40-41) or certifications (Articles 42-43) approved under the Regulation for these purposes.

New Features of the GDPR

- Responses to a subject access request will have to be provided within a tighter timescale and free of charge (Article 12).
- New data subject rights:
  - "right to be forgotten" or right to erasure (Article 17),
  - "data portability" (Article 20).
- Security breach notification:
  - mandatory "personal data breach" notifications to the supervisory authority without undue delay (within 72 hours where feasible) (Article 33)
  - personal data breach notifications to the data subject without undue delay where there is a high risk to their privacy (Article 34).

New Features of the GDPR

- The introduction of the Board (Section 3 - Articles 68-76) to replace the Article 29 Working Party, with an enhanced role and powers.
- Harsher sanctions and a new framework for fines (in two tiers), which will be substantially higher than under the DPA(Article 83).
  - DPA: the maximum fine is £500,000,
  - GDPR: two tiers of administrative fines levied by supervisory authorities:
    - up to 20 million EUR or 4% of total worldwide turnover if higher
    - up to 10 million EUR or 2% of total worldwide turnover if higher.

DPA Principles in the GDPR

DPA (1998)

1. Personal data shall be processed **fairly and lawfully** and, in particular, shall not be processed unless: (a) at least one of the conditions in Schedule 2 is met, and (b) in the case of sensitive personal data, at Least one of the conditions in Schedule 3 is also met.
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.
3. Personal data shall be **adequate, relevant and not excessive** in relation to the purpose or purposes for which they are processed.

GDPR

1. Personal data must be:

a) processed **lawfully, fairly and in a transparent** manner in relation to the data subject ("Lawfullness, fairness and transparency").

b) collected for **specified, explicit and legitimate** purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ("purpose limitation")

c) **adequate, relevant and limited** to what is necessary in relation to the purposes for which they are processed ("data minimisation").

DPA Principles in the GDPR

DPA (1998)

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.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

GDPR

d) **accurate and, where necessary, kept up to date**; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are **erased or rectified without delay** ("accuracy").

e) kept in a form which permits identification of data subjects for **no longer than is necessary for** the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ("storage limitation").

DPA Principles in the GDPR

7. Appropriate technical and organisational measures shall betaken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
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 LeveE of protection for the rights and freedoms of data subjects in relation to the processing of personaL data.

f) processed in a manner that **ensures appropriate security** of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or dam age, using **appropriate technical or organisational measures** ("integrity and confidentiality").

No equivalent principle, although the area of transferring personal data to a third country or international organisation is dealt with at length in the GDPR.

2. The controller shall be **responsible for and be able to demonstrate compliance with** paragraph 1 ("accountabiLity").