HEART OF YEW

COMMUNITY INTEREST COMPANY

No. 16147175

HEARTOFYEW.COM

Heartofyew@gmail.com

Data Protection Act 2018 (DPA 2018)

The **Data Protection Act 2018** and the **UK General Data Protection Regulation (UK GDPR)** govern the handling of personal data in the United Kingdom. These laws are designed to protect individuals' personal information and ensure that organizations process data fairly, lawfully, and transparently.

Data Protection Act 2018 (DPA 2018)

The **Data Protection Act 2018** is the UK's implementation of the European Union's General Data Protection Regulation (EU GDPR), but it also includes additional provisions specific to the UK. After Brexit, the UK retained the core principles of the GDPR, adapting it as the **UK GDPR**, but the Data Protection Act 2018 remains the primary legislation that works alongside it.

Key Provisions of the Data Protection Act 2018:

1. **Scope and Application:**
   - The DPA 2018 applies to any organization that processes personal data of individuals in the UK, regardless of whether the organization is based in the UK.
   - It covers data processing in both the public and private sectors.
2. **Personal Data:**
   - The DPA 2018 defines **personal data** as any information relating to an identified or identifiable individual. This includes names, addresses, contact details, IP addresses, photographs, and any other information that can identify a person.
   - **Special categories of personal data** (sensitive data) include information about race, ethnic origin, political opinions, religion, health, sexual orientation, and biometric data.
3. **Data Protection Principles:** Under the DPA 2018, organizations must follow these **key principles** when processing personal data:
   1. **Lawfulness, Fairness, and Transparency**: Data must be processed lawfully, fairly, and in a transparent manner.
   2. **Purpose Limitation**: Data must be collected for specified, explicit, and legitimate purposes and not further processed in a way that is incompatible with those purposes.

3. **Data Minimization**: Personal data collected must be adequate, relevant, and limited to what is necessary for the purpose for which it is processed.
4. **Accuracy**: Data must be accurate and, where necessary, kept up to date.
5. **Storage Limitation**: Personal data must not be kept for longer than necessary.
6. **Integrity and Confidentiality**: Personal data must be processed in a way that ensures appropriate security, including protection against unauthorized or unlawful processing, accidental loss, or damage.
7. **Accountability**: Data controllers are responsible for ensuring compliance with these principles and must be able to demonstrate this compliance.

4. **Lawful Basis for Processing Data:** Organizations must have a lawful basis for processing personal data. These include:
   - **Consent**: The individual has given clear consent for their data to be processed for a specific purpose.
   - **Contract**: Processing is necessary for a contract the individual has with the organization.
   - **Legal Obligation**: Processing is necessary to comply with the law.
   - **Vital Interests**: Processing is necessary to protect someone's life.
   - **Public Task**: Processing is necessary to perform a task in the public interest or for official functions.
   - **Legitimate Interests**: Processing is necessary for the legitimate interests of the organization, as long as these do not override the individual's rights.
5. **Rights of Individuals (Data Subjects):** The DPA 2018 strengthens individual rights over their personal data. These rights include:
   - **Right to be Informed**: Individuals have the right to know how their data is being collected and used.
   - **Right of Access**: Individuals can request a copy of the personal data held about them, known as a **Subject Access Request** (SAR).
   - **Right to Rectification**: Individuals can request the correction of inaccurate or incomplete data.
   - **Right to Erasure ("Right to be Forgotten")**: Individuals can request their data be deleted in certain circumstances.
   - **Right to Restrict Processing**: Individuals can ask for their data to be restricted or suppressed under certain conditions.
   - **Right to Data Portability**: Individuals can obtain their data in a machine-readable format and reuse it across different services.
   - **Right to Object**: Individuals can object to the processing of their data in certain cases, including for direct marketing purposes.
   - **Rights Related to Automated Decision-Making**: Individuals have protections if decisions are made based solely on automated processing (e.g., profiling).
6. **Data Protection Officer (DPO):** Certain organizations, especially public bodies and those processing large amounts of personal data, are required to appoint a **Data Protection Officer (DPO)** to oversee data protection strategies and compliance with the law.
7. **Breach Notification:** Organizations must report certain types of data breaches to the Information Commissioner's Office (ICO) within 72 hours if the breach is likely to result in a risk to individuals' rights and freedoms. Data subjects must also be informed if the breach is likely to result in a high risk to their rights.
8. **Enforcement and Penalties:** The **Information Commissioner's Office (ICO)** is the UK regulator responsible for enforcing data protection laws. The ICO has the

power to issue fines for breaches of the DPA 2018 and UK GDPR. Fines can be significant, with maximum penalties reaching up to:

- **£17.5 million** or **4% of annual global turnover**, whichever is higher, for serious infringements.
- **£8.7 million** or **2% of annual global turnover**, whichever is higher, for other violations.

UK General Data Protection Regulation (UK GDPR)

The **UK GDPR** is a post-Brexit adaptation of the European Union's GDPR. It retained most of the key principles and requirements of the original EU GDPR, with some changes to fit the UK context. The **UK GDPR** works in tandem with the **Data Protection Act 2018**, and together they provide the legal framework for data protection in the UK.

Key Elements of the UK GDPR:

1. **Territorial Scope:** The UK GDPR applies to:
   - Any organization operating within the UK.
   - Organizations outside the UK that offer goods or services to individuals in the UK or monitor their behaviour within the UK.
2. **Data Controller and Processor Responsibilities:**
   - A **Data Controller** determines the purposes and means of processing personal data.
   - A **Data Processor** processes personal data on behalf of the data controller. Controllers are responsible for ensuring processors comply with data protection laws.
3. **International Data Transfers:**
   - The UK GDPR places restrictions on the transfer of personal data outside the UK to ensure it is adequately protected.
   - **Adequacy Decisions** allow data to be transferred to countries deemed to have adequate data protection standards by the UK government.
   - In the absence of adequacy decisions, organizations may need to use mechanisms like **Standard Contractual Clauses (SCCs)** to ensure data protection during international transfers.
4. **Data Breach Reporting:** Similar to the DPA 2018, under the UK GDPR, data breaches must be reported to the ICO within 72 hours if there is a risk to individuals. Affected individuals must be informed if their data could be at high risk.
5. **Data Protection Impact Assessments (DPIAs):** Organizations must carry out **Data Protection Impact Assessments (DPIAs)** for any data processing activities that are likely to result in a high risk to individuals' rights and freedoms. This is especially important for large-scale data processing, sensitive data, or systematic monitoring of individuals.
6. **Children's Data:** The UK GDPR has specific provisions for protecting children's personal data, particularly in online services. Parental consent is required for the processing of data for children under 13 years old.

Differences between UK GDPR and EU GDPR:

Although the UK GDPR is closely based on the EU GDPR, the main differences relate to international data transfers and the role of the **Information Commissioner's Office (ICO)**

as the sole regulator for the UK. Post-Brexit, the UK is no longer subject to the jurisdiction of the European Data Protection Board (EDPB).

Conclusion:

The **Data Protection Act 2018** and the **UK GDPR** provide a comprehensive legal framework for the protection of personal data in the UK. They empower individuals with rights over their data, require organizations to handle data responsibly and transparently, and impose significant penalties for non-compliance. Together, they ensure that personal data is used in a way that respects individuals' privacy and security.