Introduction

The European General Data Protection Regulation (GDPR) comes into effect from 25 May 2018.

Territories

GDPR applies to all EU based organisations that collect or process the personal data of EU individuals. It also applies to organisations outside the EU that either monitor the behaviour or provide goods and services to individuals within the EU.

Personal Data

It is safe to assume that any data covered by the Data Protection Act 1998 (DPA) will be covered by GDPR. For most organisations, keeping HR records, customer lists, or contact details etc, the change to the definition should make little practical difference. We are used to thinking in terms of personal records comprising: name, address, telephone numbers, and e-mail addresses along with other information depending upon the nature of business or types of employment. GDPR provides a wider definition of Personal Identifiable Information (PII) which covers

- online indicators such as IP addresses and cookies
- video records such as CCTV
- usage records and transactional history (utility companies, financial organisations etc.)

Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing.

Sensitive Personal Data

GDPR prohibits the processing of special categories of personal data which is described as

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- processing of genetic data
- biometric data for the purpose of uniquely identifying a natural person
- data concerning health
- data concerning a natural person's sex life or sexual orientation

There are circumstances where the processing of sensitive personal data is permitted and this is covered in the PII module.

Data Processors and Controllers

GDPR applies to both “controllers” and “processors”. The definitions of these are basically the same as the under the DPA. The Controller says how and why personal information is processed and the Processor acts on behalf of the Controller. Processors include cloud services, call centres and payroll services.

Stronger Privacy Rights for Individuals

Consent must be freely given

1. The right to be informed
   The right to be informed encompasses your obligation to provide 'fair processing information', typically through a privacy notice. It emphasises the need for transparency over how you use personal data.

2. The right of access
   Under the GDPR, individuals will have the right to obtain:
   - confirmation that their data is being processed;
   - access to their personal data; and
   - other supplementary information – this largely corresponds to the information that should be provided in a privacy notice (see Article 15).

   These are similar to existing subject access rights under the DPA.

3. The right to rectification
   Individuals are entitled to have personal data rectified if it is inaccurate or incomplete.
   If you have disclosed the personal data in question to third parties, you must inform them of the rectification where possible. You must also inform the individuals about the third parties to whom the data has been disclosed where appropriate.

4. The right to erasure
   The right to erasure is also known as 'the right to be forgotten'. The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

5. The right to restrict processing
   Under the DPA, individuals have a right to 'block' or suppress processing of personal data. The restriction of processing under the GDPR is similar.

   When processing is restricted, you are permitted to store the personal data, but not further process it. You can retain just enough information about the individual to ensure that the restriction is respected in future.

6. The right to data portability
   The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.

   It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability. Some organisations in the UK already offer data portability through the "midata" and similar initiatives which allow individuals to view, access and use their personal consumption and transaction data in a way that is portable and safe. It enables consumers to take advantage of applications and services which can use this data to find them a better deal, or help them understand their spending habits.

7. The right to object
   Individuals have the right to object to:
   - processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
   - direct marketing (including profiling);
   - processing for purposes of scientific/historical research and statistics.

8. Rights in relation to automated decision making and profiling.
   The GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention. These rights work in a similar way to existing rights under the DPA. Identify whether any of your processing operations constitute automated decision making and consider whether you need to update your procedures to deal with the requirements of the GDPR.

Obligations for Organisations

1. Accountability
   Demonstrate compliance by maintaining records of all data processing activity.

2. Data Security
   Keep personal data secure through appropriate technical and organisational measures.

3. Data Protection Impact Assessment (DPIA)
   Mandatory if the processing activity is likely to result in a high risk to the rights of individuals.

4. Data Breaches
   Report data breaches to the ICO within 72 hours and inform the individuals affected.

5. Data Transfer
   Transfer of data outside the EU to a "Third Country" is only permitted if appropriate safeguards are in place. The UK will be considered a "Third Country" post Brexit.

6. Data Protection Officer (DPO)
   Mandatory
   - Public authority
   - Monitoring individuals on a large scale
   - Processing sensitive data

   Good practice for others

Cost of Non-compliance

Fines of up to €20 million or 4% of global turnover

Compensation claims for damages suffered

Reputational damage and loss of consumer trust

Good News

There is an upside to all the doom and gloom, scaremongering and talk about fines. Organisations will no longer be able to maintain relationships with suppliers who fail to be GDPR compliant, therefore organisations that are will be able to promote their businesses by marketing themselves as being GDPR compliant and win business as a result.

Useful References:

General Data Protection Regulation
http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN

midata
https://www.gov.uk/government/news/the-midata-vision-of-consumer-empowerment