# General Data Protection Regulation

The way in which personal data is used and protected is set to change in May 2018. At present, the Data Protection Act 1998 (DPA) sets out the rules and principles that must be followed when someone is using personal data. A lot has changed since 1998, in particular the technologies used to communicate with each other – communicating online creates new issues in respect of protecting data which are arguably not covered by current legislation.

In response to the changing landscape, the EU has updated the current Data Protection Directive with the **General Data Protection Regulation (GDPR)**. Organisations in the EU will have to comply with its provisions from **25th May 2018**.

The Information Commissioner's Office (ICO) has produced detailed guidance on the new rules, which can be found here. The purpose of this note is to give a brief overview of the main provisions and what steps organisations should be taking to prepare for the implementation of the GDPR.

**As a result of Brexit, will the UK have to follow the provisions in the GDPR?**

Yes – the UK will still be part of the EU on 25th May 2018. Therefore, these rules will apply to the UK. The UK Government has said they are committed to implementing the new rules in May 2018.

**What are the main points to look out for?**

Main definitions

The definitions of data controllers, data processors and personal data are much the same as within the DPA. Sensitive data will be called "special categories of personal data" but again, will be much the same (although it will also include genetic and biometric data).

Data Protection Principles

The data protection principles are similar to those in the DPA. There is more detail than in the DPA, and there is the addition of an "accountability principle". This requires those processing data to show how they have complied with the principles (see below for more details).

Lawful reasons for processing data

In order to process data and special categories of data, there needs to be a lawful reason to do so. They include such reasons as the consent of the data subject and necessity in order to comply with a legal obligation.

Consent

One lawful reason for processing data is that the data subject has provided their consent. Consent is different under the GDPR in that it needs to be freely given, specific, informed and unambiguous. There needs to be some form of clear affirmative action. Therefore, silence, pre-ticked boxes or

inactivity will not be enough. “Explicit consent” needs to be obtained for special categories of data, although it is not clear how this differs from “normal” consent. If you are currently relying on implied consent, this will not be sufficient when the GDPR comes into force. The ICO has been consulting on draft detailed guidance regarding consent, which was due to be published in June 2017.

Children’s personal data

There are new rules in relation to children’s data. For example, where services are offered directly to a child, clear privacy notices must be given. In respect of online services offered to children, consent from the parent or guardian will be required in order to process the child’s data.

**What are the specific rights of data subjects?**

The GDPR provides the following rights for individuals:

The right to be informed. This is much the same as under the DPA, although there is an emphasis on the need for transparency over how personal data is used – this would usually be done in a privacy notice – the ICO’s code of practice regarding privacy notices can be found here.

Right of access. Again, this is similar to the DPA (referred to as subject access requests), with a couple of notable changes. Firstly, the information must be provided free of charge (currently a fee of £10 can be charged). A charge can be levied if the request for information is manifestly unfounded or excessive, but the charge would be limited to the administrative costs incurred. Secondly, the requested information must be provided within 1 month of the request (currently 40 days). This can be extended by 2 months where the request is complex and numerous.

Right of rectification. Any request for information to be rectified must be dealt with within 1 month of the request – this can be extended by up to 2 months if the request is complex. If information has been passed to third parties, they must also be informed of the rectification as soon as possible.

The right to erasure (AKA the right to be forgotten). This is not an absolute right and will only apply in certain circumstances. This reflects the current position in the DPA, although the requirement for the individual to show that they have suffered unwarranted and substantial distress has been removed. Enhanced protection is provided to children, especially when involving social networking sites.

Right to restrict processing. This reflects the current position under the DPA. When; (i) an individual contests the accuracy of data or objects to the processing of it, (ii) the processing is unlawful and the individual doesn’t want to rely on the right to be forgotten, or (iii) the organisation no longer needs the personal data but the individual requires the data to establish, exercise of defend a legal claim, processing of data must be restricted, i.e. the information can be stored but not processed.

Right to data portability. Where data is processed by automated means, individuals will be entitled to re-use that information for their own purposes across different platforms – for example, this will be particularly relevant for price comparison websites where information can be moved from one site to another. Any request from an individual must be dealt with within 1 month (extended by 2

months if the request is complex). Information must be provided in a structured, commonly used and machine readable form.

Right to object. Individuals can object to the processing of information. However, the extent of that right depends on the processing purpose. If data is processed for the performance of a legal task or the organisation's legitimate interest then there are some exemptions available. If the data is processed for direct marketing purposes, then processing must stop upon a request being made. If data is processed for research purposes, the individual must have grounds for objecting.

Automated decision making and processing. This provides protection for individuals when certain decisions are made by the organisation which produces a legal effect or similarly significant effect and is automated without human intervention. This works in a very similar way to the DPA. The GDPR also provides protection for individuals regarding profiling, defined as "any form of automated processing of data ... to analyse or predict aspects concerning that natural person's performance at work, health, reliability, behaviour, location or movements". Such processing must be fair and transparent, using appropriate mathematical procedures. There must be appropriate measures to enable inaccuracies to be corrected and must be secure.

**What is the new "accountability principle" mentioned earlier?**

As mentioned, the accountability principle requires organisations to demonstrate that the protection principles have been complied with – this is perhaps the biggest change being implemented by the GDPR. This can (and in some situations, must) be done in a number of ways:

- Implementing and maintaining data protection policies and procedures.
- Maintaining relevant documents on processing activities. This is required for the processing of all data for employers with more than 250 employees. For those with less than 250 employees, documents will need to be maintained for higher risk activities, for example where there is a risk to the rights and freedoms of the individual and processing of special categories of data.
- Appointing a data protection officer (DPO), where appropriate. A DPO must be appointed where the organisation is a public authority, they carry out large scale systematic monitoring of individuals, or they carry out large scale processing of special categories of data or data relating to criminal offences/convictions.
- Follow the principles of data protection by design and default. The ICO has provided some guidance on this, which can be found here. Organisations will be expressly required to take into account and incorporate data protection into any matters that require data processing.
- Use impact assessments, where appropriate. These must be carried out when using new technologies, and where the processing is likely to result in a high risk to individuals. ICO's guidance and code of practice can be found here.

**What should organisations do if there is a breach of the GDPR?**

The GDPR will introduce strict notification rules where a breach has occurred. A breach for these purposes is a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data where it is likely to result in a risk to the rights and freedoms of individuals. Any such breach must be reported to the relevant supervisory authority (in the UK, this will be the ICO) within 72 hours of the breach. If the breach is likely to result in a high risk to individuals, data subjects must be informed "without undue delay".

**What are the penalties for breaches of the GDPR?**

The maximum fine that can be issued by the ICO for a breach of the DPA currently stands at £500,000. This will be increased to **20 million Euros (about £16.75m)** or **4% of the total annual worldwide turnover in the preceding financial year for the organisation**, whichever is higher. This is a huge increase in potential liability, reflecting the increased level of importance that has been given to the protection of personal data. The UK is currently consulting on the enforcement provisions of the GDPR, so there should be more clarity on this shortly.

**What steps should organisations be taking?**

The ICO has issued a 12 step guide to preparing for the GDPR coming into force. In addition, the ICO has prepared a tool kit to assist with preparing for the GDPR's introduction.

**Is there any other guidance available?**

As well as the links provided within this note, the ICO has a specific home page on this topic. Also, the ICO's Blog is regularly updated and has lots of information on this subject.