Introduction to risk management

I11: 2018 edition

Web update 1: 27 April 2018

Please note the following update to your copy of the **I11 2018** study text:

General Data Protection Regulation (GDPR)

Once adopted on 25 May 2018 the **General Data Protection Regulation (GDPR)** will have the force of law across all EU Member States. The Government has confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR.

Who does the GDPR apply to? The GDPR applies to 'controllers' and 'processors'. The definitions are broadly the same as under the Data Protection Act 1998 (DPA) – i.e. the controller says how and why personal data is processed and the processor acts on the controller's behalf. Firms currently subject to the DPA are likely to be subject to the GDPR.

The GDPR places specific legal obligations on processors; for example, firms are required to maintain records of personal data and processing activities. A firm will have significantly more legal liability if it is responsible for a breach. These obligations for processors are a new requirement under the GDPR.

Controllers are not relieved of their obligations where a processor is involved – the GDPR places further obligations on controller firms to ensure their contracts with processors comply with the GDPR.

What information does the GDPR apply to? Like the DPA, the GDPR applies to personal data. However, the GDPR's definition is more detailed, reflecting changes in technology and in the way in which information is collected. It makes it clear that information such as an online identifier – e.g. an IP address – can be personal data.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This is wider than the DPA's definition and could include chronologically ordered sets of manual records containing personal data. Personal data that has been anonymised – e.g. key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

Sensitive personal data: The GDPR refers to sensitive personal data as 'special categories of personal data'. These categories are broadly the same as those in the DPA, with some minor changes.

Principles: Under the GDPR, the data protection principles set out the main responsibilities for organisations. They are similar to those in the DPA, with added detail, although the GDPR does not have principles relating to individuals' rights or overseas transfers of personal data. The most significant addition is an accountability principle: the GDPR requires firms to show how they comply with the principles – for example by documenting the decisions they take about a processing activity.

Lawful processing: For processing to be lawful under the GDPR, firms need to identify a lawful basis before they can process personal data and document this. This is significant, because what this lawful basis is has an effect on an individual's rights: where a firm relies on someone's consent, the individual generally has stronger rights, for example to have their data deleted.

Consent: Consent under the GDPR must be a freely given, specific, informed and unambiguous indication of the individual's wishes. There must be some form of positive opt-in – consent cannot be inferred from silence, pre-ticked boxes or inactivity, and firms need to make it simple for people to withdraw consent. Consent must also be separate from other terms and conditions and be verifiable.

Firms can rely on other lawful bases apart from consent – for example, where processing is necessary for the purposes of an organisation's or a third party's legitimate interests. They are not required to automatically refresh all existing DPA consents in preparation for the GDPR, but if a firm relies on individuals' consent to process their data, it must make sure it will meet the GDPR standard. If not, firms must either alter the consent mechanisms and seek fresh GDPR-compliant consent or find an alternative to consent.

Rights: The GDPR creates some new rights for individuals and strengthens some of those that currently exist under the DPA. These are:

- The right to be informed.
- The right of access.
- The right to rectification.
- The right to erasure.
- The right to restrict processing.
- The right to data portability.
- The right to object.
- Rights in relation to automated decision making and profiling.

Accountability and governance: Accountability and transparency are more significant under the GDPR. Firms are expected to put into place comprehensive but proportionate governance measures. Good practice tools such as privacy impact assessments and privacy by design are now legally required in certain circumstances. Practically, this is likely to mean more policies and procedures for organisations, although many will already have good governance measures in place.

Breach notification: The GDPR introduces a duty on all organisations to report certain types of data breach to the relevant supervisory authority, and in some cases to the individuals affected.

Transfers of personal data to third countries or international organisations: The GDPR imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations, in order to ensure that the level of protection of individuals afforded by the GDPR is not undermined.

Data Protection Bill (DP Bill)

The Data Protection Bill (DP Bill) was published on 14 September 2017 and has entered Parliament. It aims to modernise data protection laws to ensure they are effective in the years to come.

Although the GDPR has direct effect across all EU Member States and organisations have to comply with it, it does allow Member States limited opportunities to make provisions for how it applies in their country. In the UK these have been included as part of the DP Bill. It is therefore important the GDPR and the DP Bill are read side by side.

The main elements of the DP Bill include:

General data processing

- Implement GDPR standards across all general data processing.
- Provide clarity on the definitions used in the GDPR in the UK context.
- Ensure that sensitive health, social care and education data can continue to be processed to ensure continued confidentiality in health and safeguarding situations can be maintained.
- Provide appropriate restrictions to rights to access and delete data to allow certain processing currently undertaken to continue where there is a strong public policy justification, including for national security purposes.
- Set the age from which parental consent is not needed to process data online at age 13, supported by a new age-appropriate design code enforced by the Information Commissioner.

Regulation and enforcement

- Enact additional powers for the Information Commissioner who will continue to regulate and enforce data protection laws.
- Allow the Commissioner to levy higher administrative fines on data controllers and processors for the most serious data breaches; being up to £17m (€20m) or 4% of global turnover.
- Empower the Commissioner to bring criminal proceedings for offences where a data controller or processor alters records with intent to prevent disclosure following a subject access request.

The DP Bill also transposes the so-called Law Enforcement Directive (LED) into UK law. The plan is for the DP Bill to be ready to take effect in May 2018 – as the (new) **Data Protection Act 2018** – to coincide with when the LED and GDPR take effect.

These changes affect the following section(s):

- Chapter 3, section B9, page 3/11.