General Data Protection Regulation (GDPR)

1. Background

The GDPR will apply in the UK from 25 May 2018 and when it comes into force will replace all the data protection legislation including the UK's Data Protection Act of 1998. The government has confirmed that the UK's decision to leave the EU will not affect the implementation of the GDPR. The text has now been finalised and the Information Commissioner's Office (ICO) is providing guidance to firms throughout 2017 to enable them to comply from May 2018.

Much of the current DPA regulation will remain however GDPR enhances some of the regulation and brings in new regulation. These are set out in the sections below.

2. Data Controllers and Data Processors

The GDPR applies to 'controllers' **and** 'processors'. The definitions are broadly the same as under the DPA – i.e. the controller says how and why personal data is processed and the processor acts on the controller's behalf. If you are currently subject to the DPA, it is likely that you will also be subject to the GDPR.

If you are a processor, the GDPR places specific legal obligations on you; for example, you are required to maintain records of personal data and processing activities. You will have significantly more legal liability if you are responsible for a breach. These obligations for processors are a new requirement under the GDPR.

However, if you are a controller, you are not relieved of your obligations where a processor is involved – the GDPR places further obligations on you to ensure your contracts with processors comply with the GDPR.

- The GDPR applies to processing carried out by organisations operating within the EU. It also applies to organisations outside the EU that offer goods or services to individuals in the EU.
- The GDPR does not apply to certain activities including processing covered by the Law Enforcement Directive, processing for national security purposes and processing carried out by individuals purely for personal/household activities.

3. Principles

The data protection principles, as set out in the DPA, remain but they have been condensed into six as opposed to eight principles. Article 5 of the GDPR states that personal data must be:

1. Processed fairly, lawfully and in a transparent manner in relation to the data subject.

2. Collected for specified, explicit and legitimate purposes and not further processed for other purposes incompatible with those purposes.

3. Adequate, relevant and limited to what is necessary in relation to the purposes for which data is processed.

4. Accurate and, where necessary, kept up to date.

5. Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.

6. Processed in a way that ensures appropriate security of the personal data including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Firms will need to review data retention processes including electronic data. The ICO has yet to provide full guidance on retention of data records.

Once full guidance has been provided firms will need to review on line data retention. Changes may need to be made to this so only base data is kept which cannot be used to identify a customer.

Consent

Like the DPA, the GDPR will require data controllers to have a legitimate reason for processing personal data. If they rely on the consent of the data subject, they must be able to demonstrate that it was freely given, specific, informed and unambiguous for each purpose for which the data is being processed. Consent can be given by a written, including electronic or oral statement. This could include the data subject ticking a box when visiting a website, choosing technical settings for social network accounts or by any other statement or conduct which clearly indicates their acceptance of the proposed processing of personal data. Silence, pre-ticked boxes or inactivity will no longer constitute consent.

There will need to be a change regarding marketing preferences. The marketing preferences will need to be opt in boxes rather than opt out and it is likely they will need to be made separate for email, social media, post, phone and text.

Children

The preamble to the GDPR states: “Children deserve specific protection of their personal data, as they may be less aware of risks, consequences, safeguards and their rights in relation to the processing of personal data. This concerns especially the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of child data when using services offered directly to a child.”

Article 8 requires that where the personal data of a child under 16 is being processed to provide ‘information society services’ (for example, on-line businesses, social networking sites, etc) consent must be obtained from the holder of parental responsibility for the child. Member states are allowed to lower this threshold where appropriate but not below the age of 13 which the UK is likely to do.

Firms need to review whether this applies to them.

4. Data subjects' rights

The list of rights that a data subject can exercise has been widened by section 2 of the GDPR.

The GDPR provides the following rights for individuals:-

1. The right to be informed;
2. The right of access;
3. The right to rectification;
4. The right to erasure;
5. The right to restrict processing;
6. The right to data portability;
7. The right to object;
8. Rights in relation to automated decision making and profiling.

The subject access right, rectification and being able to object to direct marketing remain. The right to have personal data processed for restricted purposes and the right to transfer data/have it transferred to another data controller (data portability) are new rights.

In addition, article 17 introduces a 'right to be forgotten', which means data subjects will be able to request that their personal data is erased by the data controller and no longer processed. This will be where the data is no longer necessary in relation to the purposes for which it is processed, where data subjects have withdrawn their consent, where they object to the processing of their data or where the processing does not comply with the GDPR. However, the further retention of such data will be lawful in some cases where it is necessary for compliance with a legal obligation or for reasons of public interest in the area of public health or for the exercise or defence of legal claims.

To strengthen the 'right to be forgotten' online, the GDPR requires that a data controller who has made the personal data public should inform other data controllers which are processing the data to erase any links to, or copies or replications of, that data.

Firms will need to review processes to ensure that they are able to delete data where the customer requests it and meet the requirement where data has been shared or made public.

5. Accountability and Governance

The GDPR includes provisions that promote accountability and governance. These complement the GDPR's transparency requirements. While the principles of accountability and transparency have previously been implicit requirements of data protection law, the GDPR's emphasis elevates their significance.

You are expected to put into place comprehensive but proportionate governance measures. Good practice tools that the ICO has championed for a long time such as privacy impact assessments and privacy by design are now legally required in certain circumstances.

Ultimately, these measures should minimise the risk of breaches and uphold the protection of personal data. Practically, this is likely to mean more policies and procedures for organisations, although many organisations will already have good governance measures in place.

Accountability Principle

The new accountability principle in Article 5(2) requires you to demonstrate that you comply with the principles and states explicitly that this is your responsibility.

Firms must:

- Implement appropriate technical and organisational measures that ensure and demonstrate that they comply. This may include internal data protection policies such as staff training, internal audits of processing activities, and reviews of internal HR policies.
- Maintain relevant documentation on processing activities.
- Where appropriate, appoint a data protection officer.
- Implement measures that meet the principles of data protection by design and data protection by default. Measures could include:
    - Data minimisation;
    - Pseudonymisation;
    - Transparency;
    - Allowing individuals to monitor processing; and
    - Creating and improving security features on an ongoing basis.
- Use data protection impact assessments where appropriate.

Records of processing activities (documentation)

As well as your obligation to provide comprehensive, clear and transparent privacy, if your organisation has more than 250 employees, you must maintain additional internal records of your processing activities.

If your organisation has less than 250 employees you are required to maintain records of activities related to higher risk processing, such as:

• processing personal data that could result in a risk to the rights and freedoms of individual;

or

• processing of special categories of data or criminal convictions and offences.

Records that need to be kept

You must maintain internal records of processing activities. You must record the following information - there are some similarities with 'registrable particulars' under the DPA which must be notified to the ICO.

- Name and details of your organisation (and where applicable, of other controllers, your representative and data protection officer);
- Purposes of the processing;
- Description of the categories of individuals and categories of personal data;
- Categories of recipients of personal data;
- Details of transfers to third countries including documentation of the transfer mechanism safeguards in place;
- Retention schedules;
- Description of technical and organisational security measures.

You may be required to make these records available to the relevant supervisory authority for purposes of an investigation.

Data protection by design

Organisations will be expected to include data protection controls at the design stage of new projects involving the processing of personal data. Where they wish to process personal data that poses potentially high risks they will have to, prior to the processing, carry out a data protection impact assessment.

Data protection impact assessments (DPIAs) (also known as privacy impact assessments or PIAs) are a tool which can help organisations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. An effective DPIA will allow organisations to identify and fix problems at an early stage, reducing the associated costs and damage to reputation which might otherwise occur.

While not a legal requirement under the DPA, the ICO has promoted the use of DPIAs as an integral part of taking a privacy by design approach.

Data protection officer

Section 4 of the regulation introduces a statutory role of data protection officer (DPO). Most organisations handling personal data, both data controllers and data processors, will require a DPO who will have a key role in ensuring compliance with the GDPR. A group of undertakings may appoint a single DPO provided that s/he is easily accessible. Public bodies may also have a single DPO for several such authorities or bodies, taking account of their organisational structure and size.

The DPO, who can be a staff member or contractor, shall be designated on the basis of professional qualities and, in particular, knowledge of data protection law and practices, and the ability to fulfil the tasks referred to in article 37. These are:-

- to inform and advise the controller or the processor and the employees who are processing personal data of their obligations pursuant to the GDPR;
- to monitor compliance with the GDPR, including the assignment of responsibilities, awareness-raising and training of staff involved in the processing operations, and the related audits;
- to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to article 33;
- to co-operate with the supervisory authority (the ICO); and
- to act as the contact point for the supervisory authority on issues related to the processing of personal data.

Codes of conduct and certification mechanisms

The GDPR endorses the use of approved codes of conduct and certification mechanisms to demonstrate that you comply.

The specific needs of micro, small and medium sized enterprises must be taken into account.

Signing up to a code of conduct or certification scheme is not obligatory. But if an approved code of conduct or certification scheme that covers your processing activity becomes available, you may wish to consider working towards it as a way of demonstrating that you comply.

Adhering to codes of conduct and certification schemes brings a number of benefits over and above demonstrating that you comply. It can:

- improve transparency and accountability - enabling individuals to distinguish the organisations that meet the requirements of the law and they can trust with their personal data;
- provide mitigation against enforcement action; and
- improve standards by establishing best practice.

When contracting work to third parties, including processors, you may wish to consider whether they have signed up to codes of conduct or certification mechanisms.

Review current process to ensure that it meets GDPR requirements.

6. Security breaches

Under the current DPA, even in the most serious data breaches, there is no requirement to inform the ICO. Article 31 of the GDPR requires that, as soon as the organisation becomes aware a personal data breach has occurred, it should, without undue delay and, where feasible, not later than 72 hours after becoming aware of it, notify the personal data breach to the ICO, unless the organisation is able to demonstrate that the breach is unlikely to result in a risk for the rights and freedoms of individuals. Where this cannot be achieved within 72 hours, an explanation of the reasons for the delay should accompany the notification to the ICO and information may be provided in phases without undue further delay.

Furthermore, data subjects should be notified without undue delay if the personal data breach is likely to result in a high risk to their rights and freedoms to allow them to take the necessary precautions. This notification should describe the nature of the personal data breach as well as recommendations for the individual concerned to mitigate potential adverse effects. This should be done as soon as reasonably feasible, and in close cooperation with the ICO and respecting guidance provided by it or other relevant authorities (for example, law enforcement authorities).

Firms will need to review current data breach processes to assess when a notification to ICO is required. There will need to be a process in place to make the notification within the 72 hour deadline.

7. Transfers of Data

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.

8. Fines

Currently, the ICO can issue a monetary penalty notice of up to £500,000 for serious breaches of the DPA.

The GDPR introduces much higher fines.

For some breaches of the GDPR, organisations can receive a fine of up to 4% of global annual turnover for the preceding year (for undertakings) or €20m. For other breaches (for example, failing to keep records or complying with security obligations) the fine can be up to €10m or 2% of global annual turnover (for undertakings).

Branko Ltd provides general insurance FCA compliance consultancy, support services, general management consultancy and project management.

For FCA work all advice given is based upon our current understanding of the regulations and the regulators' normal practice as at the date of any report or recommendations. As regulation is a dynamic process, any advice given must be reviewed from time to time to ensure that it remains appropriate and up to date.

Current hot topics include evaluation of Conduct Risk, implementation of the Insurance Distribution Directive and effective complaints management. Please contact us to discuss your own individual needs.