A G Kelly Ltd
Chartered Certified Accountants
Client Bulletin - Winter 2017

New data protection regime

Is your business prepared for forthcoming changes in the data protection regime? There has been extensive press coverage of the subject, but UK data protection watchdog, the Information Commissioner's Office (ICO), is now concerned about misinformation being circulated in the media.

With this in mind, we set out key features of the changes, with a view to dispelling some of the myths.

General Data Protection Regulation

From 25 May 2018, a new data protection regime comes into force in the UK. The General Data Protection Regulation (GDPR) will introduce key changes to the way personal data is handled. It stands regardless of Brexit, and the ICO advises businesses to plan now for compliance.

Why it's important

The new GDPR brings with it a new enforcement regime, which reflects the growing importance of safeguarding individuals' personal data in the digital age. At present, the maximum fine for breaches of data protection law is £500,000. Under GDPR, this rises to a maximum of £17 million or, if higher, 4% of worldwide annual turnover.

However, despite heavy media emphasis on penalties, the ICO insists that alternatives, such as 'warnings, reprimands, corrective orders', will always be considered. Of 17,300 data protection cases in 2016-17, only 16 resulted in fines. 'We have always preferred the carrot to the stick,' it says.

Negative publicity for failure to protect personal data is also a significant consideration. But there's a positive side, too. Good data protection practice offers a new means to create confidence and trust in the marketplace and workforce alike.

Areas of change

There are several important areas to consider. These are who and what is affected; controllers and processors; the principles of data protection; accountability and governance; new rights for data subjects; breaches of data security. We provide an overview of each of these in turn, below.

Who and what is affected

GDPR affects anyone handling personal data - from HR or customer records, to manual data, such as might be held in a filing cabinet, or electronic data accessed via a laptop, computer, or portable device.

The definition of 'personal data' is expanded under GDPR, and in addition, includes a range of 'online identifiers', such as IP addresses. Even pseudonymised personal data may be within scope, depending on how readily the data subject might be linked to the pseudonym used.

There is a further category to consider: 'sensitive' personal data. This comes under the heading of 'special categories of personal data' and a key change is that it now includes such categories as genetic data and biometric data which is processed to uniquely identify an individual. Whilst personal data relating to criminal convictions and offences is not included, there are extra new safeguards relating to how it is processed.

Controllers and processors

GDPR affects both controllers and processors of data. A controller is in charge of how and why personal data is being processed. A processor acts on behalf of a controller to process the data. It is possible for an organisation to act both as a data controller and a data processor, or it might fulfil only one of those roles.

Under GDPR controllers now have to make sure that any contract with a data processor is GDPR compliant. For the first time data processors are also within scope: they now have to keep records of how they process personal data, and can be held legally responsible for breaches of security.

Principles of data protection

The principles underlying GDPR are broadly similar to those of the current Data Protection Act (DPA). The requirements are that personal data must be:

- processed lawfully, fairly and transparently
- collected for specified, explicit and legitimate purposes
- adequate, relevant and limited to what is necessary for the purpose
- accurate and kept up to date. Inaccurate data should be erased or corrected
- kept in an identifiable format for no longer than is necessary
- processed securely and protected from unauthorised or unlawful processing; accidental loss; destruction or damage.

However, there is now greater detail, and one major new addition to these principles. This keystone is the requirement for 'accountability.'

Accountability and governance

The new emphasis on accountability and governance means that you must demonstrate how your organisation is GDPR compliant. It is essentially about building data protection into organisational governance, from top to bottom.

Businesses must implement the necessary technical and organisational measures, including data protection policies (such as staff training; internal audits of processing activities; and reviewing HR policies). They must also keep a record of their processing activities, carry out data protection impact assessments where relevant; and appoint (in some circumstances) a data protection officer (DPO).

DPOs become a legal requirement in certain types of organisations, such as public authorities. Organisations carrying out particular types of processing, such as large scale monitoring of individuals, or large scale processing of special categories of data, or data relating to criminal convictions and offences, are also required to appoint a DPO.

The principle of data protection 'by design and default' is another key feature of GDPR. Some examples of appropriate measures suggested by the ICO include: data minimisation; pseudonymisation; transparency; allowing individuals to monitor processing; and creating and improving security features on an ongoing basis.

Organisations may also use approved codes of conduct and certification schemes to demonstrate compliance.

The ICO publishes much helpful information, including some key steps to getting prepared: **goo.gl/m2qPBE**

New rights

New rights for individuals have also been highlighted in the media. The issue of consent is one key area where much more rigorous procedures will be required under GDPR. Consent must be freely given, specific, informed, unambiguous, and methods such as pre-populated online tick-boxes will no longer be permissible. Existing consent procedures will need to be reviewed to ensure that they comply with the new rules.

Generally, GDPR sets out eight rights for the individual as follows:

The right to be informed

The right to know how personal data is processed. The GDPR promotes the idea of transparency in processing by means of a privacy notice, giving details of the controller; the source of the data; recipients of the data; data transfers made outside the EU; and the retention period of the data.

The right of access

Individuals may request details of information being held; how, why and where it is accessed; what categories of data are being accessed and who has access. The maximum time allowed to deal with such requests is reduced from 40 to 30 days. A subject access fee of £10, chargeable under the DPA, is removed under GDPR in most circumstances.

The right to rectification

The right to have inaccurate or incomplete personal data rectified, including personal data shared or given to third parties.

The right to erasure ('right to be forgotten')

The right to request deletion or removal of personal data where there is no compelling reason for its continued processing - including personal data shared or given to third parties. There are extra requirements when a request relates to a child, and some exceptions to this right, where data is held in order to comply with a legal obligation.

The right to restrict processing

Individuals may restrict the processing of personal data. Here personal data can be stored but not processed.

The right to data portability

The right to obtain and reuse personal data across different services, allowing movement, copying or transferring of personal data, and potentially enabling consumers to use applications and services to find a better deal. Personal data must be provided in a structured machine-readable format (such as .csv).

The right to object

The right to object to the processing of personal data. Processing must stop immediately unless there are 'compelling' legitimate grounds for processing, or processing is for the establishment, exercise or defence of legal claims.

Rights in relation to automated decision making and profiling

The right to ensure safeguards are in place to protect against the risk of damaging decisions being taken without human intervention. This extends to the safeguarding of personal data used for profiling purposes.

Breaches of data security

A data breach entails much more than simply losing personal data. It is defined as a security problem leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. ICO guidance gives the example of a hospital becoming responsible for a personal data breach where the health record of a patient is inappropriately accessed because of a lack of appropriate internal controls.

Media suggestions that every breach must be notified to the ICO are incorrect. Breaches must be notified when 'likely to result in a risk to the rights and freedoms of individuals' and notification must be made within 72 hours. But all organisations must plan to cope in the event of a security breach to demonstrate accountability due diligence.

How we can help

GDPR compliance cannot be achieved overnight. In this complex area, we are happy to provide further information or ongoing assistance.