General Data Protection Regulation (GDPR) – What you need to know now

The GDPR will change the way your business can collect, use and transfer data. It comes into force on 25th May 2018. It includes major changes and businesses need to start preparing for its implementation well in advance.

Why was it introduced?

The aim of GPPR was to harmonise existing data protection legislation across the EU and to strengthen data protection rights for individuals. It was also felt that data protection law needed to be updated to take into account the advances in information technology and fundamental changes in the way in which individuals and organisations communicate and share information.

What does Brexit mean for GDPR?

The government has confirmed that the UK will be implementing the GDPR irrespective of Britain's exit from the EU.

What is the difference between the Data Protection Act and the GDPR?

The GDPR is an EU wide piece of legislation and will eventually replace the Data Protection Act 1998 and all similar legislation in other EU countries.

What's changing?

The underlying data protection principles will remain broadly the same but there are many new requirements that organisations will have to be aware of and implement as necessary. Here are some key examples of the changes:

- the definition of personal data will be wider and will include information generated from cookies and IP addresses if they can identify an individual;
- individuals will have the right to have their data erased ("right to be forgotten");
- individuals will have the right to object to their data being used for profiling. Profiling includes most forms of online tracking and behavioural advertising and this new right will make it harder for businesses to use data for these activities;
- individuals will have the right to obtain a copy of their personal data in a machine-readable format and have the right to transmit that data to another controller. This is called the right to data portability;
- much stricter rules on notifying the Information Commissioner's Office (or other national data protection agency) of a data breach. The data controller will be required to notify **within 72 hours of the breach** unless the data breach is unlikely to result in a risk to individuals;
- new rules on pseudonymisation (i.e. the processing of personal data where it can no longer be attributed to a specific individual without additional information). There will also be new rules on anonymisation;
- new safeguarding for consumers has been introduced relating to automated decision-making;
- Consent, as a legal basis for processing, will be harder to obtain. The GDPR requires a **very high standard of consent**, which must be given by a **clear affirmative action** establishing a **freely given,**

specific, informed and unambiguous indication of the individual's agreement to their personal data being processed, such as by a written (including electronic) or oral statement.

- new rules on accountability and governance will mean organisations must prove that they process data in line with the new rules and build "data protection by design" into their systems and processes.

Why do I need to worry about it?

There will be much tougher penalties for breaches of the GDPR. The maximum fines will be significantly increased and the information Commissioner will have the ability to impose fines of up to 2% of annual worldwide turnover of the preceding financial year or €10 million (whichever is the greater). Fines can go up to 4% of annual worldwide turnover or €20 million for certain very serious breaches of the GDPR.

If I'm outside of the EU then why should I worry?

Unlike the Data Protection Directive the GDPR will have expanded territorial scope. Any non-EU data controllers and data processors will be subject to the GDPR if they either:

- offer goods or services to data subjects in the EU irrespective of whether payment is received; or
- monitor data subjects behaviour in so far as their behaviour takes place within the EU.

This means that many non-EU businesses that were not required to comply with the data protection directive will be required to comply with the GDPR.

What do I need to do now?

Although the GDPR will not come into force for another year, it is important that businesses start taking the steps necessary to ensure compliance well in advance. This is particularly crucial in light of the increased penalties which may be imposed for failure to comply. The ICO has published a helpful 12-step guide to assist businesses: https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf which recommends that businesses:

- Create awareness among the senior decision makers in the business;
- Audit and document the personal data they hold, recording where it came from and who it is shared with;
- Review the legal basis for the various types of processing that they carry out and document this; and
- Review privacy notices and put in place a plan for making any changes to comply with the GDPR.

If you would like a specific advice on how your business can prepare for GDPR then please contact either Alex (alex@mortonlegal.co.uk) or Matthew (matthew@mortonlegal.co.uk) at Morton Legal.

This legal briefing provides general information on the GDPR and is provided for general guidance only. If you have any specific questions then please contact Morton legal or seek advice from your usual advisor on data protection issues.