Is your business ready for the GDPR?

The EU General Data Protection Regulation (the "GDPR"), was adopted on 25 May 2016. It repeals the current, less onerous, EU Data Protection Directive, and must be complied with by 25 May 2018. It has direct effect on all member states, so there is no requirement for national implementation laws. The Government has confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR, although it remains to be seen whether implementation will continue post-Brexit.

The GDPR broadens the reach of current legislation, enhances the rights of the individual (the "data subject") and introduces new rights.

Key rights of the individual

- Right of access – individuals will have the right to obtain confirmation that their data is being processed, and have access to that data;
- Right to rectification – individuals are entitled to have personal data rectified if it is inaccurate or incomplete, and must receive a response to any rectification request within one month;
- Right to erasure ("right to be forgotten") – an individual may request the deletion or removal of personal data where there is no compelling reason for its continued processing;
- Right to restrict processing – individuals are entitled to restrict further processing of their data. Their personal data may be stored, but not further processed.
- Right to data portability – individuals may obtain and reuse their personal data for their own purposes across different services;
- Right to object – individuals can object, amongst other things, to the processing of personal data for direct marketing purposes (including profiling), and in certain other circumstances too (such as research) where the individual objects on "grounds relating to his or her particular situation".

Assessing the risk

Most businesses will become accountable for measuring the level of risk that processing data will have on data subjects. This may require the appointment of a data protection officer.

Data protection impact assessments must be performed prior to any data processing requiring the use of new technologies, if that processing could cause a high risk to the data subjects. If it is revealed that the processing does, in fact, pose a high risk to the data subject, businesses are required to consult with their "supervisory authority" (see below) before any action is taken.

Adequate risk assessment procedures should be set up as soon as possible, to ensure familiarisation with the new system prior to the GDPR becoming law.

Accountability

The GDPR requires businesses to demonstrate compliance. How you do so will depend largely on the size and nature of your business but, as a minimum, you should be prepared to maintain documentation such as records of internal audits of data processing activities and reviews of internal HR policies.

Some businesses will be expected to implement internal data protection policies, and to carry out regular staff compliance training.

Consent

This area sees the biggest change to current protections for the individual. Consent to data processing must be freely given, specific, informed and unambiguous. There must be some form of clear affirmative action – a positive opt-in – consent cannot be inferred from silence, pre-ticked boxes or inactivity. Consent must also be separate from other terms and conditions, and simple ways must be provided for people to withdraw consent. This is likely to severely restrict the ability of businesses to purchase personal data.

The rules are more stringent around consent of children. In most cases, the consent of the parent will be necessary.

A thorough review of how and when you obtain consent should be undertaken to ensure your business does not fall foul of the new regulation.

Supervisory authorities

Compliance with the GDPR will be overseen by a "supervisory authority", such as the Information Commissioner's Office in the UK. Since one of the GDPR's main aims is to harmonise data compliance throughout the EU, businesses who operate in more than one EU country will only be required to work with one "lead supervisory authority", determined by the location of their "main establishment" in the EU. This simplification will hopefully reduce the administrative burden on business.

Data Breach Notification

Businesses must notify their supervisory authority within 72 hours of a data breach - unless it is unlikely to create risk to the subject. This could prove to be administratively convoluted and costly. It is therefore imperative for businesses to have a breach response plan in place to ensure prompt compliance.

Fines

Every business that processes customer and other personal data needs to comply with the GDPR. There will be a significant increase in fines of up to 4% of annual worldwide turnover, or €20 million, for violating the data protection principles, conditions for consent or the rights of data subjects. Further fines of up to 2% of annual worldwide turnover or €10 million could be issued for breaches such as internal record keeping and breach notification. The ICO has increasingly shown a willingness to take enforcement action over data protection breaches, and this looks set to rise significantly.

It's not all doom and gloom

The GDPR is intended to make data protection more suitable for a modern environment. The introduction of a lead supervisory authority will be welcomed by those businesses with establishments in more than one EU country, and the GDPR will hopefully reduce the amount of redundant administrative tasks. However, the GDPR is primarily about empowering those whose data is on file. Due to the severity of the fines a business could face for a breach of the GDPR, it is imperative to review current data protection procedures and prepare to install new mechanisms where required.

To ensure your business is ready for the GDPR, contact Peter Kouwenberg in Taylor Walton's Commercial Team for expert guidance on 01582 390411 or by email at Peter.Kouwenberg@taylorwalton.co.uk.