WILL **BREXIT** PUT DATA PROTECTION ON NOTICE?

by Glenn Watterson, Solicitor in Mills Selig

Changes to the data protection rules are imminent which seek to improve the rights of individuals in an increasingly digital age. Will they affect businesses in Northern Ireland if the UK leaves the EU?

The new EU General Data Protection Regulation (GDPR) is scheduled to come into force on 25 May 2018, replacing the existing 1995 Data Protection Directive, and will be directly applicable in all Member States without the need for implementing national legislation.

These regulations aim to unify and expand data protection for individuals in the EU. They contain a number of new features – for example, the obligation to notify of a breach within 72 hours and the requirement for data portability. Fines and penalties for non-compliance are significantly increased.

Will UK data controllers or processors be able to hide behind Brexit?

Although the post-Brexit picture remains unclear, it's likely some if not all of GDPR will continue to apply in the UK and will affect an increasing number of businesses.

- The GDPR will apply in the UK automatically from 25 May 2018 - prior to the UK's exit from the EU, which is now likely to occur in spring/summer 2019.
- The GDPR will apply to UK businesses that have an establishment processing personal data within the European Economic Area and/or that process the personal data of individuals who are resident in the European Economic Area.
- Many commentators believe the UK will leave the EU and join the European Economic Area thus remaining part of the single market. In this scenario, the UK would have to adhere to certain EU regulations which would include the GDPR.
- The Secretary of State for Exiting the EU has stated that at the date of exit existing laws are likely to be adopted into UK laws, but with the power to amend or cancel any of these laws.
- The UK Information Commissioner is advocating that the UK adopt all EU data protection and privacy laws including GDPR so as to ensure consistent standards on the use of data and its flow between the UK and Europe.

It remains to be seen what approach will be taken, and there are two years of negotiations ahead, but it is clear that UK businesses need to be ready to comply with the new stricter regime of GDPR.

How is GDPR different from the existing Data Protection Act 1998 (DPA)?

- Stricter obligations on both controllers and processors – but with separate responsibilities for each. Processors will have significantly more legal liability if they are responsible for a breach.
- Obligation on controllers to ensure processors guarantee they will meet the requirements of GDPR.
- Data processors will for the first time have direct statutory obligations including: (i) maintaining a written record of processing activities; (ii) appointing a DPO as required; and (iii) notifying a controller on becoming aware of a personal data breach.
- GDPR contains suggestions as to what security actions controllers and processors should take – and if the approved code of conduct is followed, this will demonstrate compliance with the GDPR's security standards.
- Data breach notification requirements – even if the breach does not lead to loss of information that could be used for fraud or identity theft (as is the case in the US).
- Data portability – the right for data subjects to transfer personal data from one data controller to another without hindrance.
- Subject Access Requests must now be dealt with within one month rather than 40 days.
- The scope of a person's consent has finally been explained in detail. A data subject's consent to processing of their personal data must be as easy to withdraw as to give. Consent must also be explicit when processing sensitive data. A data controller must be able to demonstrate that consent was given.
- Where personal data is processed for direct marketing the data subject will have a right to object. This right will have to be explicitly brought to their attention. The GDPR also provides a list of additional information that must be provided to data subjects.
- Penalties for non-compliance are increasing:-
  - breaches of the key obligations contained in the GDPR (including the basic principles for processing and conditions for consent will be subject to administrative fines of up to €20,000,000 or, in the case of undertakings, 4% of global turnover, whichever is the higher;
  - other infringements such as failure to keep records or implement technical or organisational controls are subject to administrative fines up to €10,000,000 or, in the case of undertakings, up to 2% of global turnover, whichever is higher.; and
  - furthermore, the GDPR provides that compensation may be recovered by data subjects who are the victim of a breach of the legislation.

What should Northern Ireland businesses do now?

Businesses here should continue to prepare for GDPR. Consider what part of your operations may be affected by these changes and identify data flows from the EU to the UK as regardless of whether the UK adopts GDPR post Brexit, the Regulations will apply to that data flow

The position will undoubtedly fluctuate over the next two years but harmonisation of data protection will likely remain a priority regardless of Brexit.

For more information contact Glenn at 028 90 243 878 or **glenn.watterson@millsselig.com**

Mills Selig
Understanding. Expertise.

www.millsselig.com