One thing Brexit is not going to change is new EU data protection law

Here's what you need to know about the General Data Protection Regulation.

The European Commission ratified a new data protection regulation that will come into effect in May 2018. The General Data Protection Regulation will replace the current Data Protection Directive and provide a uniform data protection law across the whole of the EU.

The changes brought about by the GDPR are substantial and broaden the scope of personal privacy laws to protect the data rights of EU citizens.

In a series of blogs, we explore this regulation in detail - we explain the different provisions of the GDPR and also offer practical advice on how to comply with the new provisions.

The Chamber also offers training courses in GDPR.

Important measures introduced by the GDPR include:

1. The introduction of the "right to be forgotten"
2. The need to document IT procedures
3. The requirements on organizations to report breaches within 72 hours
4. The requirement of privacy by design and security by design
5. The introduction of new, stringent rules for obtaining consent from individuals
6. The introduction of the principle of accountability to demonstrate compliance with the provisions

The provisions in the GDPR cover capture, control and transmission of data. To attain compliance with provisions, companies will need to create and demonstrate awareness of what sensitive data they control, where they store such data and who has access to it.

Data Protection Principles

The data protection principles in the GDPR remain more or less similar to the key principles of the Data Protection Act 1998.

- Companies must process personal data in lawful, fair and transparent ways.
- Personal data must be collected for exactly specified purposes and further processing that is incompatible with the previously stated purposes is prohibited.
- Personal data that is not relevant or more than what is needed for the stated processing requirements must not be collected.
- Where companies store personal data, they are responsible for keeping the data accurate and update. This means companies may face new challenges in ensuring that data such as CVs and records of former employees are kept up to date. In such situations, companies must evaluate whether the data needs to be kept or whether it should be erased entirely.
- Inaccurate data must be rectified.

The confidentiality of personal data must be maintained and companies face severe penalties if there is any unauthorised or unlawful processing of personal data, including accidental loss, which could lead to penalties.

The GDPR introduces a legal accountability obligation under which data controllers will be required to implement appropriate technical controls and data handling procedures to ensure compliance with privacy requirements.

Businesses must renew and update the controls through continuous assessments.

Business must also implement procedures for continuous assessments and improvements to the controls, and businesses must determine what controls are appropriate for the scope and purposes for which they collect and process personal data.

In addition, measures to objectively demonstrate compliance must be implemented. Therefore, businesses will need to maintain thorough documentation of their data protection measures.

Documentation could cover inventories of personal data, processing activated privacy impact assessments, controls to preserve confidentiality retention policies and procedures for handling data breaches. Organisations must provide adequate training to staff and foster a culture of privacy.

The Chamber also offers half day introductory training courses in GDPR and also an in depth two day training course. Details can be found here.