EU Data Protection Reform

What you and your business need to know

What are the reforms?

The EU is reforming its existing data protection rules. The wide range of changes was initially proposed by the European Commission back in 2012. The reforms have been slowly making their way through the EU legislative process and in June 2015 the EU's Justice and Home Affairs Council agreed a general approach for the proposed General Data Protection Regulation (GDPR).

Why were the reforms needed?

Current data protection legislation is derived from EU Directive 95/46/EC which came into force in 1995 when the internet was not the ubiquitous business resource it is today. Concepts such as social media and cloud storage simply did not exist. Each member state implemented the Directive in its own way leading to an uneven protection for personal data. The new rules aim to bring a codified approach across the EU and bring legislation up to date and fit for the digital age.

What are the new rules?

There are two sets of rules. First, the GDPR which sets out the EU framework for data protection and is intended to replace Directive 95/46/EC. Secondly, a Data Protection Directive specifically dealing with personal data processed in the law enforcement context.

What does the GDPR contain and how will it affect me?

The GDPR will impose numerous obligations. These obligations will also apply to **organisations outside the EU** where they offer goods or services or monitor online behaviour of EU citizens.

Each member state will appoint a **Supervisory Authority (SA)** responsible for implementing the regulation and ensuring its consistency within the EU.

Individuals will have more control over their personal data including rights of access and a **right to be forgotten.**

Companies will have to **notify the SA of any personal data breaches within 24 hours** and the individual within a reasonable time.

Companies have to produce **regular Data Protection Impact Assessments**, followed by Data Protection Compliance reviews. A high risk assessment will require consultation with the SA.

Companies with more than 250 employees may need to **appoint Data Protection Officers** to deal with the new regulatory requirements.

Severe **penalties for infringement**, including fines of up to 1 million EURO or 5% of annual turnover.

When will this come into force?

The European Parliament, the European Council and the European commission are currently engaged in a trialogue to negotiate the final wording of the GDPR. Finalisation is expected towards the end of 2015, with the GDPR coming into force some time in 2017.

What can my business do now?

This is not an IT issue. Data Protection and Cyber Security is a risk affecting all businesses and decisions need to be made at board level. In order to be prepared for the significant changes, business will need to review their current first party and business interruption policies to make sure they will be covered. There are simple but effective processes that can implemented now to make sure your business is not exposed to the significant penalties for a GDPR breach.

Samantha Wilson
Associate

T: 0203 697 1906
M: 07780 221676
E: samantha.wilson@cpblaw.com