European Regulation
Data Security

On the 18 Dec 2015 Europe's General Data Protection Regulation (The "GDPR" or the "Regulation") was, after almost three years of negotiations, agreed. Whilst the final wording hasn't been released, we know it will have a material impact on organisations that hold or handle corporate, financial or personal data in any media format whether digital or physical.

Why is the new GDPR required?

The 20 year old Data Protection Directive (DPD) which is being replaced by the Regulation is part of the overall strategy across the world to prevent and respond to cyber disruptions and attacks. The EU has recognised that cybersecurity incidents are increasing in frequency and magnitude and becoming more complex and cross border in nature. As such, incidents can cause major damage to safety and the economy, the EU Commission considered that efforts to prevent, co-operate on and be more transparent about cyber incidents, should improve.

The old DPD was limited because it was just that – a Directive. As a Directive it could only set the minimum legal standards. The member states could otherwise craft their legislation as they saw fit. This led to a patchwork of data protection laws across Europe.

The new Regulation is meant to solve this problem. As a Regulation it directly imposes a uniform data security regime across all EU members. There will be no need to enact the legislation, it will become law thereby harmonising EU data protection law across the whole of the EU.

What are some of the major ways the GDPR differs from the outgoing Directive...

1) **Increased fines for violations** – if a company violates certain provisions within the GDPR – such as basic data processing principles or the rules relating to cross border data transfers they may be subject to fines amounting to **4% of the company's worldwide annual turnover**.
2) **Data Breach Notification** – Data Controllers will be required to notify the appropriate supervisory authority (in the UK this is likely to be the Information Commissioner's Office) of the data breach within 72 hours of learning about the breach. The notification must describe the nature of the data breach, the categories and the approximate number of data subjects implicated, the contact information of the organisation's data protection office, the likely consequences of the breach and the measures the Data Controller has taken or proposes to take to address and mitigate the breach.

   Additionally a Data Processor is required to notify a Data Controller of a data breach "without undue delay". Article 32 of the GDPR requires Data Controllers to notify data subjects of breaches when the data breach is likely to result in a high risk to the rights and freedoms of individuals and must notify data subjects of the breach "without undue delay".

LOCKTON®

3) **Data Protection Officers** – Article 35 requires companies whose "core activities" involve large scale processing of "special categories" of data – defined as information that reveals a data subjects racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health or sex life or sexual orientation to designate a data protection officer. Companies should be aware that even if they don't collect this type of data from clients they may collect some of this information from their employees for human resources purposes and therefore may need to appoint a data protection officer.

4) **Greater Controls for data subjects** – Article 17 set outs the "right to erasure" also known as the "right to be forgotten" which gives a data subject the right to order a Data Controller to erase any of the data subjects personal data in certain situations. The Article requires the Data Controller to erase a data subjects personal data "without undue delay" when the personal data is no longer necessary in relation to the purposes for which it was collected or processed or the data subject withdraws his or her consent or objects to the processing and there is no other legal basis for the processing.

How can companies prepare for the GDPR?

There is no question all companies will need to determine how the new GDPR will relate to them. Our conversations with clients show that organisations are taking a moralistic view to protecting personal data and we recommend any company transacting business across the world should, if they haven't done so already, prepare for and address the following items well in advance of the GDPR coming into effect:

1) Are you a Data Controller or a Data Processor or a mixture of both? Review your contracts with third parties to understand where respective roles and responsibilities lie.

2) Get your privacy policies, procedures and documentation in order and keep them up to date: data protection authorities will be able to ask for these at any time.

3) Form a governance group that oversees all your privacy activities, led by a senior executive. If you appoint a data protection officer (recommended for companies that employ more than 250 people) they should develop metrics to measure the status of privacy efforts, report regularly and create statements of compliance that will be required as part of your organisation's annual report.

4) Implement a breach notification process and enhance your incident management processes and your detection and response capabilities. Any data breach must be notified to the relevant data protection authority, even if protective measures, such as encryption, are in place or the likelihood of harm is low.

5) Prepare your organisation to fulfil the "right to be forgotten", "right to erasure". A strategy covering topics such as data classification, retention, collection, destruction, storage and search will be required – and it should cover all mechanisms by which data is collected, including the internet, call centres and paper.

The new rules will have direct effect from early 2018 – two years from the date of formal adoption and publication of the Regulation. Businesses have time to prepare, but there is much work to do. We are moving toward the most stringent data laws in the world. Data permeates everything we do in our digital lives and touches all organisations. However, in the short time that remains before implementation, organisations will need to completely transform the way they collect and use personal information. This is not a compliance or legal challenge; it is much more profound than that. Organisations will need to adopt entirely new behaviours in the way they collect and use personal information.

If you have any questions about the new Regulation please do not hesitate to contact your normal Lockton Associate or a member of the Global Technology Privacy Practice:

Brett Warburton-Smith - Partner
Tel: +44 (0)20 7933 2242
Mobile: +44 (0)7768 917550
E-mail: brett.warburton-smith@uk.lockton.com

Cliff White - Senior Vice President
Tel: +44 (0)20 7933 2704
Mobile: +44 (0)7500 226366
E-mail: cliff.white@uk.lockton.com