Are you ready for the new EU data protection regulation?

The EU Council and Parliament adopted the General Data Protection Regulation (GDPR) in April 2016 and it is set to come into effect on 25th May 2018. While this may seem like a long way off, the scale of the changes means organisations should start their preparations now.

The GDPR has two primary objectives: to ensure the protection of personal data and to simplify the regulatory environment by unifying data protection laws across the EU. As a result, a number of new measures will be introduced that will require attention.

Key changes

These are some of the significant changes that will be introduced:

**Compulsory notification of personal data breaches**
A 72-hour notification requirement will be introduced for all personal data breaches, except those which pose no risk to individuals. In the case of serious incidents, there will also be a duty to notify the affected individuals of the breach.

This is a game changer. Currently, there are only requirements in the EU for organisations in certain sectors or countries to notify breaches or cyber attacks to regulators. The short time periods will also make the response to these incidents time critical.

**Higher penalties**
Under the GDPR, fines will increase to as much as EUR20 million or, if higher, 4% of annual worldwide turnover. This is a significant escalation from the current penalties under existing data protection laws. Individuals will also have the right to claim compensation for any ‘material or non-material’ damage suffered as a result of a breach of the GDPR.

**Data processor duties**
Data controllers are natural persons or organisations who decide the reasons for processing personal data and how it will be processed, whilst data processors act on behalf of a controller. Under current EU law, only data controllers have statutory obligations when processing personal data; the GDPR extends these responsibilities to data processors. This will be a major change for service providers, who may have set themselves up as processors to avoid the direct applicability of data protection law.

The GDPR specifies a number of obligations that must be included in contracts between controllers and processors and imposes joint and several liability on service providers and their customers for compensation claims by individuals. Given the increased risks and more stringent requirements, it would be prudent to review the terms of any agreements with third party suppliers of data processing services ahead of the implementation of the GDPR.
New rights for data subjects
Data subjects will have new and strengthened rights including the right of deletion, data portability and the prohibition on certain types of profiling. It will be essential that organisations understand these rights and are able to respect them.

The GDPR also imposes a higher threshold for gaining consent to process personal data and tighter limitations on the use of the data collected. Where organisations are relying on consent, the consent must be explicit and indicated by a positive action. In addition, individuals must be able to withdraw consent at any time.

Organisations should ensure systems and processes put privacy at the forefront. This includes conducting impact assessments at the start of projects and defaulting to settings that protect individuals’ privacy. Strengthened transparency obligations mean that privacy notices are going to get longer as organisations must describe their processing activities and why they use personal data in greater detail. Organisations should therefore look at the content and format of their privacy notices.

Preparing for the new regulations
With so many significant changes set to be introduced, it is important to start considering them as soon as possible. We recommend appointing a steering committee to ensure that all the implications of the new regulations are fully understood and existing systems and processes are adapted to reflect the new requirements.

Running a full risk assessment can be a useful exercise. This will highlight where there are any potential issues and enable you to take action now to avoid problems when the regulations are introduced.

Aon, together with insurers, has created a cyber product (EU Data Privacy Protect) to help organisations to understand its Cyber Risk Profile. The product address potential Cyber threats, including a solution to transfer risks into the insurance market, covering losses that may be incurred. This also ensures the right expertise is available when a data breach occurs.

Aon’s EU Data Protect includes:

1. GDPR Readiness Assessment: A tool to assist organisations in identifying, prioritising and remediating gaps in their compliance programme and understanding and mitigating data protection risks in accordance with GDPR

2. Cyber Impact Analysis: Provides sophisticated modelling of the financial impact from data breaches under GDPR and more broadly provides a comprehensive understanding of the cyber exposures facing a business

3. EU GDPR Insurance Endorsement: This acknowledges the GDPR in a qualifying Cyber Policy which includes fines and penalties where insurable by law and costs of defending regulatory action. This Endorsement also provides for some regulator-required experts’ fees arising from certain loss events

4. Incident and Claims Response: Access to specialist post-event advisory services, including incident response, digital forensics and claims handling capabilities to expedite remediation and claims settlement

Aon Cyber 360 is also available for those organisations that want to conduct a full Cyber Risk Assessment.
Data breach response plan

Given the new requirements and the higher penalties, a data breach response plan is essential. This should address the following questions:

1. **What do we need to know in order to inform our regulators?**

   Article 33 of the GDPR introduces mandatory data breach reporting without undue delay and, where feasible, not later than 72 hours after becoming aware of the breach. The Article also specifies what information must be included in the notification.

2. **Where do we access legal advice?**

   Organisations may be able to get certain firms pre-approved with their cyber insurers.

3. **How will we independently investigate a cyber-attack or incident?**

4. **How will we demonstrate we complied with our responsibilities to implement appropriate technical and organisational measures to ensure compliance?**

5. **What is our media strategy?**

   The reputational costs can be significant.

6. **How would we respond to claims for compensation?**

   Article 79 provides for data subjects to bring an action against the data controller for any breach of the GDPR while Article 82 states that any person who has suffered material or immaterial damage as a result of an infringement of the regulations has the right to receive compensation.

Insurance could be a consideration. But, whether or not insurance is appropriate, prudent risk managers should be considering their obligations and making sure the correct processes and systems are in place ahead of May 2018 when the new regulations are introduced. And, given the volume of work required to comply with the regulations, starting now is essential.