On 25 May 2018 the General Data Protection Regulation will start to apply. The two-year period since it was adopted was intended to give organisations in the EU time to get their house in order and become compliant. The Regulation presents numerous new challenges requiring changes to procedures; documentation; contracts and IT systems. It also introduces obligations involving the appointment of roles; allocation of responsibilities; training; and preparation to handle events such as data subject access requests; data breach incidents or inspections.

Many organisations have mobilised internal resources to prepare for the new regulation. Others have asked for assistance to get an understanding of what sort of affects the new obligations and data subject rights will have of the organisation. Others still are just awakening to the complexities and intricacies of the regulation.

The big innovations in the GDPR

Compliance
Strict new compliance requirements will be imposed. For example, entities will have to perform “Privacy Impact Assessments” and privacy audits as a matter of course. They will have to implement “Privacy by Design” methodologies into their business, so that compliance is baked-in to everything they do. They will have to deliver on a new “Accountability” obligation, which means creating written compliance plans, which they will have to deliver to regulators on demand.

Usage controls
Personal data will be subject to strict new usage controls. These include “data minimisation”, “data portability” and “right to be forgotten” principles, which will require entities to limit the use of data, to enable individuals to take their data with them at the end of a relationship and to delete and destroy data on request.

Consent
Obtaining consent to use personal data will be much harder to achieve and to prove.

Bundling
The provision of a service that is conditional upon the individual giving permission for their data to be used for non-essential purposes (such as marketing) will be banned.

Aggregation
The ability to aggregate data to enable an individual to be profiled (a common objective in new digital projects) will be severely curtailed.

Supervision
Regulators will also be empowered to carry out audits and inspections of entities on demand.
Breach disclosure
Entities will be required to report serious contraventions of the law to the regulators and to people affected. Public disclosure of failure is likely to fuel regulatory sanctions and compensation claims, as well as causing damage to brand and reputations.

Pinch points
The features of business that are most affected by the GDPR are:
- Consumer facing activities
- Tracking
- Activities relating to children
- Public services
- Marketing and advertising
- Mass communications
- Digital transformations
- Joint ventures
- Geolocation
- Global or multi-national business operations
- Profiling
- Litigation

Citizens and pressure groups have the right to engage in group litigation ("class actions") to recover compensation for mere distress caused by contraventions of the law.

Fines
Serious contraventions of the law will be punishable by fines of up to either 4% or €20 million of group annual worldwide turnover.

What can you do to become compliant?
- Develop a vision and strategy for compliance with the GDPR
- Document processing activities and data flows
- Assess gaps between your current compliance programme and the requirements of the GDPR and analyse risk
- Review lawful processing bases and third party contracts
- Create an accountability framework for data protection compliance
- Create processes for privacy by design and privacy impact and risk assessments
- Identify and prioritise key remediation activity to reduce your risk profile
- Tracking
- Public services
- Mass communications
- Joint ventures
- Global or multi-national business operations.