BY
Hugh Jones

Hugh Jones is a co-founder of Sytorus Ltd, a specialised provider of Data Protection consultancy, assessment and training services. Hugh provides professional Data Protection guidance, and is a frequent speaker at Privacy and Data Management events in Ireland and overseas. Hugh offers consultancy support and tailored training to organisations in the areas of data management and regulatory compliance.

GDPR – Debunking some Myths

Human nature being what it is, we often grasp at straws when confronted with substantial challenges – those facing the reality of the recent introduction of GDPR on May 25th are not immune to this phenomenon.

In this article, I wanted to outline some of the more impressive myths which have sprung up around the new Regulation and its implementation, to identify the kernel of truth on which they are based and to debunk the dangerous complacency which might settle if they are believed.

"The GDPR doesn't apply to SMEs"

While some elements of the GDPR will not apply to smaller organisations, any organisation processing personal data, whether a Data Controller or a Data Processor, will have obligations under the Regulation.

For example, SMEs will not qualify for the obligation to draft a Data Processing Activity Log since this only applies where the entity has more than 250 staff. However, where an organisation systematically processes medical, religious or trade union membership information (the special categories), even smaller organisations will need to provide these descriptions of their processing activities.

"It doesn't apply to public sector bodies"

Much has been made of the recent decision by the Irish Government to determine that public bodies and government departments will not be subject to the full force of the new fines and penalties available under the GDPR. The primary reason for this is that any such fine would simply require the payment of public funds from one department to another, on the 'wooden dollar merry-go-round'.

However, exemption from the full force of these penalties does not in any way exempt such organisations from the obligations of compliance with the Regulation and the DP Commissioner has made it very clear that other sanctions will still be available, even if the full monetary penalties are not going to be wielded. For example, the ODPC can issue prohibition or enforcement notices to shut down a particular programme or area of processing where substantial DP concerns arise.

"It doesn't apply to firms based outside the EU"

The scope of the GDPR has been quite clear and will include the activities of organisations based outside the EEA jurisdiction (the (for now) 28-member states of the EU plus Norway, Iceland and Liechtenstein), where they wish to do business within the EEA.

In such circumstances, the non-EEA organisation will require a formally recognised Nominated Representative established within the EEA, in order to protect their interests, as well as to be the primary point of contact for Data Subjects and the Data Commissioner in the event of an incident or DP concern.

"It's just another EU scare tactic"

The EEA has produced several iterations of the DP legislation over the years, namely in 1981, 1995 and 2002. All have been accepted, at varying speeds and levels of enthusiasm, by the Member States and each have tried to take account of both the commercial realities as well as the technological advances which were prevalent at the time.

The GDPR is no different, attempting as it does to harmonise the implementation and interpretation of DP principles across all 31 Member States on the same date, as well as taking account of the substantial advances in the way we process personal data since the last major draft of legislation in 1995.

BY
Hugh Jones

The objective is not to scare anyone or any organisation, into compliance. If anything, the objective of the GDPR is to provide adequate and appropriate levels of protection for our personal data, even where we often represent the biggest risk to our own privacy, through the manner in which we allow our information to be disclosed, acquired and distributed.

"I have loads of time to get compliant - May 25th is a target, not a deadline"

The final draft of the Regulation was published in April 2016, with the instruction for organisations to implement appropriate changes and protocols to prepare for its implementation in May 2018. This two years and 20 days was clearly marked as the 'lead time' during which organisations had opportunity to review their data quality, train their staff, modify their systems, upgrade their security measures and generally prepare for the 'brave new world' of organisational accountability (Principle Seven).

Many have done so, with varying degrees of effort and success. Nonetheless, from May 25th onwards, an organisation's DP compliance will be evaluated against the seven principles of the GDPR, not the eight rules of the preceding DP legislation.

There is no evidence of a 'stay of execution', a 'soft implementation' or a 'grace period' during which organisations can finally get around to taking the GDPR seriously – the past two years have been that preparation period.

"It's all about cyber security"

With all of the recent headlines in relation to hacks, malware and cyber terrorism, one might be mistaken in believing that the focus of the new Regulation will be on defending data against digital attack.

While digital communications and social media account for a massive volume of the data records we process on a daily basis, the GDPR nonetheless affords equal protection to paper (manual) records. And while the security, confidentiality and integrity of personal information is certainly one element of focus for the Regulation, this only accounts for one of the seven Principles.

Concerns for the fairness and transparency of processing, the accuracy and quality of the data, the duration for which it is held and the tangible evidence by which organisations can demonstrate their awareness and accountability of their obligations will all form part of the evaluation of compliance under the GDPR.

"The ODPC has no teeth and/or will never levy a € multi-million penalty"

On the one hand, we really don't want organisations to be motivated by their fear of the substantial new fines and penalties which are possible under the GDPR.

On the other hand, it would be extremely optimistic (or foolhardy) for any organisation to ignore their obligations solely on the basis that the Irish Courts have never levied a penalty that comes close to the 4% of global annual turnover or €20m (whichever is the greater).

We have already seen evidence in Italy of the appetite for a substantial penalty being imposed for breaches of DP legislation (a combined penalty of €11m against two firms for breaches of DP and Money-laundering regulations in 2016). We have also seen clear evidence that the Irish Commissioner has been ready to invoke those clauses within the legislation which make Directors individually liable for breaches which occur due to their 'negligence or connivance'.

Added to this, we must always remember that the structure of the new Regulation, with its built-in 'consistency mechanism', will allow Supervisory Authorities in other EEA jurisdictions to appeal against any decision by the Irish Commissioner or courts which they feel is too lenient or 'soft'.

There may be some gamblers out there who consider this a risk worth taking and ignore the GDPR on the basis that 'bad stuff happens to other people'. Time will tell whether or not this is a safe foundation on which to build your data management strategy.

"We're a Charity/Religious Institution/Sports club/self-employed/Medical Practice – we are exempt!"

As stated above, all organisations processing personal data will have obligations under the Regulation – while some derogations and exemptions apply, they are relatively few and far between and are quite isolated and limited in their scope.

Bottom line, the seven Principles will apply to all processing of personal data, from the point of acquisition, throughout the life cycle, to the point when the data is anonymised, deleted or removed from operational use (archived).

"The GDPR changes everything!"

Not so – if anything, the GDPR is a reinforcement of the key concepts which already existed under the DP Directive and the Electronic Communications Regulation – principles of privacy, fairness, transparency, data quality and integrity, timely removal and destruction of information, appropriate risk management, a commitment to security and organisational ownership of responsibilities and accountability.

Most of all, the GDPR will oblige organisations to appreciate the privilege of having access to personal data and understand the obligations which such access places on them. In turn, they will need to train their staff, implement appropriate policies and protocols and be able to demonstrate their commitment to and compliance with, the Regulation when called-upon by the Supervisory Authority to do so. No change there, then!!