GDPR – from challenge to opportunity

If anyone wanted to understand what the ins and outs of the new General Data Protection Regulation (GDPR) are, this couldn't be a better time to figure them out.

By Dr Paul Gonzi and Dr Antonio Ghio – Fenech & Fenech Advocates

Not only is the GDPR's day of reckoning literally around the corner, that being 25th May 2018, but the already very topical subject of data protection has just been catapulted to the forefront with a certain chilling panache.

The muddle of facts and allegations tied to the Cambridge Analytica (CA) and Facebook affair, an affair having intricate spin-offs tied to the controversies of Trump, Brexit and more (including one that is closer to home) are just ripe for the picking.

Let's face it, the ingredients have the makings of an outstanding thriller movie. Mass secret surveillance by companies and politicians alike. A Big Brother lurking in the shadows of innocent people's homes (circa 87 million of them, please note), covertly gathering and analysing their data, their preferences, their behaviour, their contacts, friends and foes, their likes, shares and emojis – absorbing millions of sets of data to learn what inspires them. In turn, they feed back personalised information using subliminal messages, convincing them to be something that they are not, to decide one way and not the other, all without them even knowing, let alone consenting to it; for instance: influencing them on whether they should buy the latest car, or vote for a particular candidate. That is the profiling and automated decision-making happening in today's technological world.

So how is this all relevant to GDPR?

Well, GDPR is intended to be the force against this sort of (alleged) abuse. It is the Version 2.0 of the data protection law in the EU. It raises the bar for those who process personal data, increases the rights of individuals whose data is processed and seriously ups the ante with tremendously pumped-up sanctions in case of breach, reaching €20 million or four per cent of global turnover, whichever the higher. To top that, it has a scope that extends beyond Europe's shores, supposedly impacting all those who process personal data belonging to persons in the EU, whether in China, India, North Korea or Timbuktu.

Take Facebook as a hypothetical example. Post 25th May, a breach by this global giant could potentially mean a whopping $1.6bn fine, four per cent of its circa $40bn worldwide turnover in 2017. And if all this weren't enough, GDPR contemplates other potential liabilities, including sanctions of a criminal nature and potential civil damages that any person (arguably those in the EU) who suffered a breach could claim.

But it doesn't stop there. The risk of getting GDPR compliance wrong will come with an obligation to report the breach to the authorities and possibly having to communicate it to all those individuals who may have been impacted. A marketing nightmare and a reputational disaster – a risk which is amplified by the fact that a breach under GDPR can also subsist in cases of inadvertent or negligent loss of personal data where there is no malicious intent.

On that note, it is reported that since the mid-March CA outburst, Facebook has lost approximately $100 billion in share value and counting. And who knows what the consequences would have been had this occurred post 25th May?

In the meantime, the data protection regulator in the UK (the ICO) has since raided CA's operations. Of course, Facebook and CA deny any wrongdoing, which is yet to be seen. So we must continue to watch this space. Yet, as we do watch and wait, we must nonetheless realise that GDPR is not a law designed just for the multi-billion corporations.

On the contrary, in the midst of all this hype, every small, medium and large organisation is expected to comply with the broad principles and rigorous rules imposed by the GDPR. Data protection must become the mantra, *by design* and *by default*, says the GDPR. There is no escaping it. The Article 29 Working Party (where all EU authorities get together to issue joint opinions that carry weight) have underscored the principle of equivalence; fines must be comparable across the EU and they are not to be used as a last resort!

Therefore, ignoring GDPR is an option, but a bad one.

Long story short, GDPR mandates protection of all data which directly or indirectly identifies a person: addresses, ID numbers, personal details, and location data – even an IP address can be personal data. Processing of personal data essentially means anything you can think of doing to it: sharing, storing, backing-up, deleting, losing it – literally anything.

Dr Antonio Ghio

And to process personal data lawfully, six principles must be complied with cumulatively, one of six grounds must be satisfied (and more in case of 'special categories' of data, such as biometric or health data). Principles of accountability, transparency, lawfulness and others translate into heaps of requirements, including information obligations, record-keeping, appointing a DPO, carrying out DPIAs, reporting breaches and handling data-subject rights.

And lo and behold, there are many such rights: the right to information, to access, to restriction, to rectification, to erasure, to portability, to object, to withdraw...

So where does one even start?

Well, first and foremost, an organisation must engage the right experts to facilitate the process. Next, absorb the basics of GDPR – learn to speak its language.

Dr Paul Gonzi

Then, it is time to figure out what personal data is being processed by whosoever within or beyond the organisation, for what purpose/s, using what means – essentially, a data mapping exercise.

Once that is done, it is time to analyse the legitimacy of that processing. Are the grounds for lawfulness being satisfied? Is there an overriding interest that prevails? Is there an exception to the rule? Should consent always be relied upon and if so, is it validly obtained? Is there automated decision-making? Is there a risk which requires a DPIA to be executed?

Following that, the organisation must weigh the risks of getting it wrong. Are the organisational and security measures sufficient to secure the data against accidental loss of data? Is the organisation prepared to defend against external malware attacks? Are the necessary protocols and procedures in place for an effective reaction to complaints, suspected breaches and data-subject requests? Have pseudonymisation and anonymisation mechanisms been contemplated? This requires a gap-analysis exercise designed to highlight room for improvement, flagged by priority. Only then can the organisation work towards filling in those gaps.

Several surveys show that there are still many organisations that are not even close to complying with the GDPR, which means they are exposed to significant risk – some more than others. Yet it is never too late, and getting the ball rolling towards compliance is better than having nothing to show. GDPR mandates *accountability* – record retention, with the ability to demonstrate compliance.

So, for those organisations that do not want to be part of the hype, or the guinea pig upon whom the fines are first tested, it is best to pull your socks up and get the ball rolling. After all, understanding what data you hold, how to streamline your processes and how to better exploit the data in a lawful way is, really, an opportunity worth investing in. You can convert this challenge into a long-term investment, conserving ongoing GDPR compliance as you move along.

As someone recently said, data is today's oil. So do this once, and do it properly. **cc**