Enough of the Noise: Let's Embrace GDPR

There is, and has been, a lot of noise around the European Union's General Data Protection Regulation (GDPR) that comes into force in May of this year. Much of this has involved scare mongering with the prospect of large fines brought to the fore, primarily by organisations looking to promote their magic pill to solve the compliance challenge in one hit. Unfortunately, no such thing exists. GDPR is predominantly solved through first understanding where the biggest risk and gaps lie, then addressing those through the implementation of processes and procedures, documented to demonstrate compliance, and finally reinforcing through specific technologies.

The unfortunate consequence of this becomes a level of fatigue and scepticism around the subject which is extremely unhelpful because GDPR, in its essence, is a change for good. The UK Information Commissioner's Office (ICO) website is an independent and superb source of analysis and advice on the subject and should be reviewed by any business looking to understand the regulations. The ICO will act as the Supervisory Authority for the UK and is therefore the body that will audit companies for compliance.

GDPR: How it benefits you

So, why is GDPR a change for good? Our world is becoming increasingly digitalised and our identity often represented by ones and zeros. Nowadays, we can bank, shop and work without leaving the house. When we do venture out, we can jump in a taxi without any money in our pocket, potentially to stay in somebody else's house with a pre-agreement conducted online all because our identity is validated on someone else's server. Everyone is drilled to protect their own online and physical critical security details, such as bank card PIN numbers, passwords and credit card information. As part of our daily lives, we are frequently requested to hand this information over to a 3rd party and blindly assume that they are taking as much care of our information as we do.

GDPR aims to ensure that this is no longer an assumption, but fact. The information referenced earlier falls under the definition of personal data and would require protection under GDPR. However, the regulations are wider than just a framework definition for data protection and address areas around the collection of that data, bestowing new rights upon consumers including decisions on how their data is handled. For example, you have the right that your data is collected only with your explicit consent, you have the right to request any and all data a company holds on you is permanently deleted (your right to be "forgotten") or for it to be provided to you in a portable format. No longer will you have to scrutinise every form you complete to determine if you have already been opted in to further marketing – are you opted in by default, do you need to check or uncheck a box to opt out or to opt in? Currently there is no consistency around how these requests are presented to you. Under GDPR, your data can only be collected with your explicit consent and, when deciding whether to opt in or out, a clear description of how that data will be processed and used will be provided. For the man and the woman on the street, this is all positive. The companies that consume our data are now required, under GDPR, to take a responsible attitude to the collection, storage and processing of that data. The regulations adopt a pro-active stance to data protection in that they allow for organisations to be audited to check they are in compliance and, in the event they are not, will apply and monitor remedial action. This is another step forward as currently we only tend to discover a company's lax data protection strategy at the point our data has been breached, which is far too late.

If you have suffered as a victim of a data breach, a best-case scenario is that you will need to cancel credit cards with the worst case requiring you to reclaim your identity. Anything that is put in place with the sole mission to avoid this type of situation should be welcomed.

Taking a Step Toward GDPR Compliance

As a business, there will undoubtedly be some effort required to ensure compliance with the regulations. If a strong data protection policy is already in place, it could just be a tweak. For others, it may involve a bit more work. A simple step towards GDPR compliance and its challenges is to ensure that every business is aware of GDPR and what it entails. Apricorn's survey, conducted by Vanson Bourne, uncovered the fact that 24 per cent of surveyed companies were not aware of GDPR or its implications, whilst 17 per cent of those who were aware had no plan for compliance.

However, GDPR provides an opportunity for businesses to clean up their house, and to really understand what data they hold, whether it is all necessary, how it is processed and to re-confirm their relationship with their customers and partners. The first, and most important piece of work is to analyse all personal data that is collected, stored and processed and to understand where it is located and who has access to it. All data deemed irrelevant to the business should be deleted and the remainder tested in support of the new rights individuals will have under GDPR – has the subject explicitly consented to the collection of their data, are you able to delete it or provide it in portable format on request? Once the data is understood and the processes around it documented, the next step would be to protect it both at rest and on the move in order to defend against any potential breaches.

GDPR is non-specific in terms of prescribed technologies. However, Article 32 does go a step further, requiring "the pseudonymisation and encryption of personal data". This would seem an obvious requirement, but there are still frequent examples of the use of unencrypted media at the centre of a breach played out in the media. The recent discovery of Her Majesty the Queen's security details on an unencrypted USB stick outside Heathrow airport is a case in point. Furthermore, Article 34 notes that, in the event of a breach; if the data at risk is encrypted, the requirement to contact each data subject affected is no longer mandated, thereby avoiding the resultant administrative costs. Therefore, it would appear prudent to apply encryption to all personal data within corporate systems and even more so on any media that is used to take the data outside of the business.

Spread the Word

Finally, once a business has these 2 pieces of the puzzle in place, an employee education and awareness program must be put in place. As home based and mobile workforce numbers continue to grow, so does the number of locations and devices on which corporate data is carried. Each employee has the responsibility to ensure that they follow corporate data protection policy and to understand their role in ensuring any personal data they carry remains safe at all times. The aforementioned survey found that 48 per cent of the surveyed companies said employees are their biggest security risk, and as many as 44 per cent expect that employees will lose data and expose their organisation to the risk of a data breach. Therefore, this should be an area of focus – not only to equip the workforce with easy to use tools that support the data protection policy but to ensure everyone understands the policy and is aware of their obligations under it.

We are headed to a perfect storm where business will be legally required to implement data protection best practice and audited against that, individuals will become more aware of their rights, take more ownership of their data and expect companies to be doing everything GDPR mandates.

Everyone should embrace GDPR regardless of whether they are a citizen or a multi-national conglomerate. To the citizen – this is your data, you have every right to expect it to be treated responsibly and with your permission. To the businesses – it is time to take your obligations seriously. GDPR is an opportunity for both sides of the data exchange relationship to get their house in order. It's about time, wouldn't you agree?