Data Is An Asset: It Deserves Protection; It Offers Opportunity

The challenges faced by organisations as a result of the new European Union data protection framework, the General Data Protection Regulation (GDPR), are undoubtedly huge. However, while many of the headlines have so far focussed on the increase in penalties as a consequence of the GDPR and the issues associated with complying with the new legislation, much less attention has been given to other aspects of the change and the opportunities it presents for proactive organisations to enhance their data capabilities and grow their business.

MODERN DATA PROTECTION LEGISLATION IS OVERDUE

There is now less than one year to go until the most significant change to data protection law in Europe in 20 years. On 25 May 2018, the current two-year implementation period will conclude and the GDPR will finally become directly applicable in all EU Member States.

New data protection legislation is certainly overdue. European Directive 95/46/EC, from which the current Data Protection Act 1998 (DPA) derives and which the GDPR replaces, preceded the Internet boom and birth of social media.[1] The world has come a long way since 1995: global internet traffic has increased from 33 gigabytes per month in 1995[2] to one trillion gigabytes in 2016,[3] while global e-commerce sales have grown from US$500 million[4] per year in 1995 to US$2 trillion in 2016.[5]

Data privacy and the right of individuals to choose and control how their data is used and accessed have not kept pace with technological advancement and the digital economy, however. With a loss in consumer trust as to how organisations use their personal data, there has been an impact on the profitability of the Internet. It is estimated that ad blockers cost companies GBP22 billion per year worldwide,[6] as a consequence of consumers preferring incognito browsing over an incessant online assault on their identity and data.

The GDPR provides companies with the opportunity to regain customers' trust and leverage technology to grow their businesses. However, this can only be done if companies move away from viewing the GDPR as a compliance-driven, tick-box exercise, and embrace it as a means to improve data management strategies in such a way that drives their business forward.

THE GDPR: THE CHANGES

The GDPR introduces:

- Enhanced rights for individuals (for example, the right to object to profiling, right of data portability, and the enhanced right to erasure).
- More onerous obligations on organisations processing personal data (including transparency of processing, accountability framework, and mandatory data breach notification requirements).
- Increased enforcement powers.
- More stringent consent requirements.
- Direct obligations for data processors, as well as for data controllers.
- A territorial reach that extends beyond the EU to companies offering goods or services (even for free) to EU citizens or where companies monitor the behaviour of EU citizens.

THE GDPR: THE PENALTIES

Much of the media attention given to the GDPR has so far been in relation to the increase in potential penalties, which could rise to as much as €20,000,000 or 4% of total annual global turnover, whichever is greater, for breach of a data subject's rights and freedoms.

However, the GDPR allows data protection authorities to take into account mitigating factors when deciding whether to impose a fine and the level it should assume. These mitigating factors include the intentional or negligent character of the infringement and the degree of responsibility of the controller or processor, taking into account technical and organisational measures implemented by them to safeguard the personal data processed. The importance of companies embracing the concept of accountability and understanding and mitigating the risks they face can not be over emphasised.

Protecting data held is an imperative for all companies to de-risk themselves of damage to their reputation and commercial consequences.

SEEING THE OPPORTUNITY IN CHANGE

While some organisations will consider compliance with the GDPR to be a costly and disruptive undertaking, it actually presents a great opportunity.

Forward-thinking organisations will look at this in a whole new light. They will be willing to embrace the challenge to develop their technology, as well as their information management and cyber-security systems.

For too long, many organisations have captured swathes of data without proper protocols surrounding its processing, storage, and sharing or any real understanding of its relevance and value to their business. While developments such as this, will require time and money, the value to be derived from gaining customers' trust and improved data management could be market-leading and may go some way to offsetting this.

GENERAL DATA PROTECTION REGULATION: SAVING BUSINESSES MONEY

The European Commission has projected that working within the framework of the GDPR may even reduce costs for businesses by as much as €2.3 billion a year[8].

IMPROVING CYBER SECURITY AND ESTABLISHING A RISK CULTURE

It has been estimated that cybercrime cost the global economy more than US$450 billion in 2016.[9] The GDPR and the requirements contained within it, should go some way towards reducing this figure by enhancing cyber security levels and therefore reducing the potential for data loss, operational disruption, physical damage, and also reputational and brand damage.

Organisations' levels of understanding around cyber risk continue to increase, partly due to a series of recent high-profile cyber incidents around the world, including the recent WannaCry ransomware attack that impacted as many as 40 hospitals in the UK. However, there is still a long way to go for many in order to map and quantify their cyber exposure and establish the cultural change required throughout their organisations.

Under the GDPR, where the processing is carried out by a public body or where, for private companies, "the core activities of the controller or the processor consist of processing operations which (by virtue of their nature, their scope, and/or their purposes) require regular and systematic monitoring of data subjects on a large scale, or the core activities of the controller or the processor consist of processing on a large scale of special categories of data", there will be an additional requirement to appoint a Data Protection Officer (DPO). The DPO's role will be to independently supervise compliance with the GDPR and advise staff who deal with personal data. It is envisaged that the requirement that DPOs will report into the highest management level of their companies, will go a long way toward creating a cyber risk culture. It may even improve board-level ownership of cyber risk within these organisations.

BREXIT WILL NOT AFFECT THE IMPLEMENTATION OF THE GDPR IN THE UK

The UK Government has already stated that the country's decision to leave the European Union – which could be finalised by December 2018 at the earliest[10] – will not affect the implementation of the GDPR in the UK.

Consequently, there would be at least six months where UK data controllers would have to abide by all the provisions of the GDPR.

However, the Government has indicated that, in order to achieve its goal of free data flows with the EU post-Brexit, the UK will replace the DPA with legislation that mirrors the GDPR[11].

CONSENT: A NEW RELATIONSHIP WITH THE CONSUMER

The GDPR aims to provide EU citizens with greater control over the use of their personal data. Central to this is consent. The threshold for consent under the GDPR is higher than under the existing legislation. To meet the new consent requirements, consent needs to be freely given, specific, informed, unambiguous, and businesses must be able to demonstrate these elements when relying on consent for processing. Special categories of personal data such as health information require explicit consent. Where an organisation relies on consent to process an individual's personal data, the individual will have the right to withdraw that consent at any time, together with a right to obtain and port their personal data for their own purposes across different service providers ("data portability") and an enhanced right of erasure (the "right to be forgotten"), should they wish to do so.

Consent must be a positive indication of agreement that personal data can be used in the specific manner and for the specific purposes set out by the controller. A pre-ticked box will not be valid consent. Consent requires engagement. And it is that type of engagement that enables businesses to better understand the needs and desires of their customers and develop a relationship based on trust and transparency.

Consent requires engagement. And it is that type of engagement that enables businesses to better understand the needs and desires of their customers and develop a relationship based on trust and transparency.

While ensuring compliance with the GDPR will no doubt cost time and money for some organisations, it presents a great opportunity for many to enhance their data capabilities and grow their business.

For more information please contact:

Ireland representative:

BREEGE LYNN
+353 87259 0129
breege.lynn@marsh.com

CONCLUSION

Much of the focus afforded to the GDPR has so far been in relation to the increase in potential fines and the resources required by businesses to ensure compliance with this new legislation. Yet while ensuring compliance with the GDPR will no doubt cost time and money for some organisations, it presents a great opportunity for many to enhance their data capabilities and grow their business.

The GDPR will provide an impetus to improve data security and controls around the use of personal information. In turn, it presents an opportunity for organisations to better understand their data and how it may be used to add value to their business. Most importantly of all, however, it is hoped that the actions required of organisations to comply with GDPR will go a long way toward helping to repair the recent breakdown in trust between consumers and organisations in terms of how personal data is used. This will enable businesses to take greater advantage of the data-driven economy.

1 For example, Google was founded in 1998, while Facebook was launched in 2004.

2 Cisco. "The History and Future of Internet Traffic", available at https://blogs.cisco.com/sp/the-history-and-future-of-internet-traffic, accessed 1 June 2017.

3 Cisco. *The Zettabyte Era – Trends and Analysis*, available at http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/vni-hyperconnectivity-wp.html, accessed 1 June 2017.

4 L. Southern, R. Schwartz, and S. Veeramachaneni. *E-Commerce: A Global Perspective*, available at https://www.scheller.gatech.edu/centers-initiatives/ciber/projects/workingpaper/1999/99_00-23.pdf, accessed 1 June 2017.

5 eMarketer. "Double-digit growth will continue through 2020, when sales will top $4 trillion", available at https://www.emarketer.com/Article/Worldwide-Retail-Ecommerce-Sales-Will-Reach-1915-Trillion-This-Year/1014369, accessed 1 June 2017.

6 Marketing Land. "Ad-Blocking Report: Nearly 200 Million Users, $22 Billion In Lost Ad Revenue", available at http://marketingland.com/ad-blocking-report-nearly-200-million-users-22-billion-in-lost-ad-revenue-138051, accessed 1 June 2017.

7 UK Information Commissioner's Office. "GDPR and accountability", available at https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/01/gdpr-and-accountability/, accessed 1 June 2017.

8 European Commission. "Agreement on Commission's EU data protection reform will boost Digital Single Market", available at http://europa.eu/rapid/press-release_IP-15-6321_en.htm, accessed 1 June 2017.

9 Hiscox. *The Hiscox Cyber Readiness Report 2017*, available at https://www.hiscox.co.uk/cyber-readiness-report/docs/cyber-readiness-report-2017.pdf, accessed 1 June 2017.

10 Bloomberg. "U.K.'s New Brexit Czar Sees December 2018 as Likely Leaving Date", available at https://www.bloomberg.com/news/articles/2016-07-13/david-davis-named-brexit-czar-in-u-k-prime-minister-may-s-team, accessed 1 June 2017.

11 Computerweekly.com. "UK should pursue EU data protection adequacy post-Brexit, says ICO," available at http://www.computerweekly.com/news/450414506/UK-should-pursue-EU-data-protection-adequacy-post-Brexit-says-ICO, accessed 1 June 2017.