FTI CONSULTING

**GDPR COUNTDOWN**

# May 2018: The starting point, not the finish line

**Companies around the globe are impacted by the landmark EU legislation, the General Data Protection Regulation (GDPR) which comes into force on May 25, 2018. While there is tremendous focus on the steep fines, the risks associated with reputational damage due to the inappropriate management of personal data is much greater. Trust is the fuel behind the digital economy. Done right, GDPR will help companies to strengthen trust and transparency with its clients.**

## Cost of a data breach

**£120m**

**-1.8%**

*A firm listed on the FTSE 100 becomes worse off by roughly £120 million in the wake of a breach, while share prices fall by an average of 1.8 per cent.*[1]

Over 140 million Americans and UK residents were impacted as a result of the Equifax data breach in September 2017. Under the GDPR, the potential fine of 4% of global annual turnover would have meant about a $63 million USD fine. The event also resulted in the resignation of the CEO, CIO and CISO and subsequent criminal investigations for insider trading. The case for evolving data privacy and security from being a CIO/CISO technical issue to becoming a company wide and board room priority is clear.

The GDPR modernises and replaces the existing EU Data Protection Directive (95/46/EC), adopted in 1995. Under the GDPR, individuals across Europe will have enhanced rights, including the right to have their data deleted, as well as rights around data portability. The bar has also been raised around consent, which will need to be unambiguous, freely given, and an affirmative action.

One of the aims of the GDPR is to give control of personal data back to the individual, while simultaneously promoting greater corporate accountability and transparency. There is now increasing demand from consumers worldwide that organisations take stronger measures to secure and protect their personal data.

> *According to the International Association of Privacy Professionals (IAPP) at least 75,000 new data protection officers (DPOs) will be needed worldwide in response to this EU law.*[3]

According to a survey by the Information Commissioner's Office (ICO)[2] only one in four UK adults trust businesses with their data. This piece of legislation is already generating a lot of debate and discourse across the UK, Europe and beyond, at the c-suite and boardroom levels of many businesses. This is because of the potential for significant penalties and brand damage.

More importantly data protection issues are fast becoming reputation issues. Investors have started punishing companies for poor security; listed companies have lost millions of pounds with share prices dropping in the wake of data breaches. According to a study by Oxford Economics a firm listed on the FTSE 100 becomes worse off by roughly £120 million in the wake of a breach, while share prices fall by an average of 1.8 per cent.[1]

The legislation is complex and far-reaching, laying out specific mandates for any company doing business in Europe involving the personal data of consumers in 28 EU member states plus Norway, Liechtenstein and Iceland. This will also include the UK, which is likely to maintain compatible data protection laws to enable free data flows post-Brexit.

## Information governance as a journey

Managing data compliance, risk and security is unlikely to be a simple issue to resolve. Compliance for the GDPR and better information governance is a journey for many corporations - one that involves ownership of aligning complex rules & obligations with the data itself.

Corporations are now taking stock of their data assets. There is greater realisation that many businesses sit at the centre of a complex ecosystem of information. This raises questions about data protection regulation throughout their data landscape, such as why and how they collect and process the personal data they do, the answers to which lay at the very core of their business.

Additionally, holding on to data for longer than you are legally allowed creates a multitude of issues beyond the GDPR. Corporations are now taking the opportunity to get rid of personal data they no longer need or use.

For many corporations, there are still as many – to use a phrase coined by former U.S. Secretary of Defence, Donald Rumsfeld – 'unknown unknowns' as there are 'known unknowns' when it comes to the GDPR with respect to the data they hold. Companies will need to take a risk-based approach, but also develop a strategy for dealing and mitigating the risk associated with these unknowns.

The scale of the task is not to be underestimated. According to the International Association of Privacy Professionals (IAPP) at least 75,000 new data protection officers (DPOs) will be needed worldwide in response to this EU law.[3]

## Holistic approach needed

All companies handling the personal data of EU citizens will be accountable for complying with the GDPR, including data processors. Prior to this new regulation, data processors were only responsible for following data controller's instructions. Everyone along the data supply chain will now need to take a proactive role in the identification, management, security and governance of personal data.

This EU legislation will have a systemic effect on how we handle information relating to an individual. Companies will need to have clearly defined procedures and systems in place when a data breach occurs, and the company will need to notify supervisory authorities within 72 hours, and in some cases, also notify the impacted individuals without 'undue delay'.

## GDPR Considerations

- **Data inventorying** also has the net effect of forcing an organisation to understand its core business processes, **why** they do **what** they do, and **where** they could be simplifying or eliminating unnecessary collection/steps and consequently reducing risks.
- The GDPR is not a box-ticking exercise; it is about a whole **cultural shift** within an organisation, well beyond 25 May 2018.
- The legislation has **extraterritorial reach**, which means any company around the globe, including those based in the US, that interact with EU personal data will be required to comply.
- **Personal data** under the GDPR is broader than Personally Identifiable Information (PII) and includes any information which directly or **indirectly** identifies an individual.
- **GDPR** it just one regulation. **NIS** cyber directive, Payment Service Directive **(PSD2)** and other regulatory requirements need to be considered in a broader framework for how and why data is collected and protected through its life.
- **Data protection** and **information governance** is everyone's issue, not just that of the IT department.

Compliance therefore needs a holistic and integrated approach. This involves many stakeholders, processes and technology, all of which need to talk to one another. IT, privacy, marketing, legal, business and security professionals and the board must get involved and take a proactive approach.

Executives must act less in silos and realise everyone has a vested interest to make data compliance work. There is also a recognised disconnect in businesses, between the requirements of data whether it be legal, regulatory or business value and how it is being managed, in reality.

Those companies who have brought the right stakeholders together to address data compliance regulations have reaped the benefits of a collaborative approach, working through the issues as a team.

> *When it comes to compliance, you need to ask the right questions about how and why you have the data you do, align it with the rules around it so that you can use it lawfully.*

## Restraints and constraints with the GDPR

Many organisations have budget constraints when it comes to governing data and allocating resources for a large piece of legislation such as the GDPR. Budgets also vary greatly depending on the scope of compliance activities and also existing investments made in data privacy, security and information governance.

Some organisations are seeing this legislation as an opportunity to get board level support and funding towards critical digital transformation and data management initiatives. The GDPR enables companies to take a client-first approach, re-engaging with their clients, employees and other business associates about their preferences, personalisation and security, based on transparency and openness.

One of the other intents of the GDPR is to streamline and provide greater consistency in the enforcement of EU data protection regulation. Companies will still need to pay attention to applicable local data protection legislation which minimally apply the GDPR and may adopt even more stringent requirements. There are still a number of areas in the GDPR that leaves it up to member states to adopt their own national rules, such as those regarding the processing of personal data in an employment context.

The GDPR is just one of many regulations governing the privacy and security of customer data being implemented across the globe. The ePrivacy Regulation (EPR) and the NIS cyber directive are also upcoming legislation that need to be considered in the overall design of a GDPR compliance framework.

Many corporations are also considering the implications of moving data to the cloud. Some cloud-based service providers have enhanced retention, security and privacy controls built in. However, even with these controls in place, it is up to the company to ensure they understand the location of their cloud providers and where they host their data. It is crucial that the required organisational and technical controls are applied, and the appropriate provisions are declared in any applicable contracts to enforce these new obligations.

The role of the authorities such as the ICO which will implement the GDPR in the UK is also a factor when it comes to compliance. Dealing with the potential volume of inquiries may be an issue for the ICO. The amount of resources needed to investigate some cases could be vast. Some highly regulated industries such as financial services and pharma may have started compliance efforts early and therefore have an advantage over other industries such as retail and manufacturing who may have less maturity or budget in managing/protecting its personal data and may be particularly vulnerable to GDPR related threats.

Many firms are working on completing their assessments and are beginning their remediation efforts in order to comply with the 25th of May 2018 deadline. With limited time and resources, companies need to prioritise their compliance actions.

Focus on clients and customer personal data first and those areas of highest risk and impact in the event of breach. Understand the role of technology as an enabler, not the solution to GDPR compliance. Finally, if you do nothing else, bring awareness to your organisation about the GDPR and take some steps towards compliance. Doing nothing is the highest risk choice that you can make.

**RESOURCES:**
1. The Cyber-Value Connection, www.cgi-group.co.uk, 2017
2. Consumers taking action over mistrust of organisations handling personal data , www.ico.org.uk, 15 June 2016
3. Study: GDPR's global reach to require at least 75,000 DPOs worldwide, www.iapp.org, 9 Nov 2016

## Lessons to be learnt

1 **Know your Approach:** Consider your risk profile, company size and industry to shape how you approach GDPR compliance. One size does NOT fit all.

2 **Cultivate Awareness:** Your executive stakeholders and board need to understand the specific risks and costs, and how it impacts your organisation.

3 **Process First, Technology as an Enabler:** Don't believe the hype, technology alone will not make you magically compliant. Get to know your business processes first, follow the data, and augment with technology where it is cost-effective. Technology without process context or purpose could result in wasted budget, resources, and organisational fatigue.

Sonia Cheng
Senior Director
Information Governance & Compliance Services
+44 (0)20 3727 1783
sonia.cheng@fticonsulting.com

Paul Prior
Managing Director
Performance Analytics
+353 879665296
paul.prior@fticonsulting.ie

FTI CONSULTING™

EXPERTS WITH IMPACT