GDPR Guide

The final countdown: are you ready for GDPR?
Effective 25 May 2018

exigent
an intelligent alternative

In just a few short months, organisations will face the biggest change in data protection laws for more than 20 years. The impact of The General Data Protection Regulation ("GDPR"), which comes into force on 25 May 2018, will be profound, and for those who have had the GDPR on their to-do lists for the past couple of years, it's time to make it a priority.

The reason for urgency is that implementing a GDPR strategy is complex and time-consuming, with multiple facets to be considered. Most importantly, unlike previous regulations, the GDPR will impose severe penalties for non-compliance. Regulators have unprecedented powers to enforce the laws and the repercussions for not treating personal data correctly are substantial. Organisations that fail to comply can receive fines of up to 4% of annual turnover or €20m, whichever is greater. Additionally, individuals have increased rights to express legal concerns and may be entitled to compensation if their data is treated incorrectly.

The new law

The regulations are designed to protect the processing, use and exchange of customer information, by governing how and where customer data should be stored, and how organisations must respond in the event of a data breach. There have been many high-profile breaches – from Bupa to Three Mobile to the now infamous Sony breaches – and this regulation brings greater consistency to how customers can expect their data to be treated in such events. Individuals will have the right to specific levels of data management. For example, the right to be informed on how their data is used, the right for their data to be transferred to a new provider, and the right to be forgotten. The regulations will have far-reaching consequences on how any global organisation that processes any personally identifiable information of EU residents deals with that data.

The new regulations supersede any previous data privacy laws and, agreed by the European Parliament and European Commission, they will be effective for citizens within all 28 member states. Brexit will have no impact on the GDPR.

For General Counsel ("GCs") and Data and Compliance Officers, the GDPR is more than just a huge headache. With so many elements to be considered, resources required and such stiff penalties, it's easy to see why so many organisations are so unprepared. According to a study from YouGov, just 29% of UK businesses are ready for the legislation. Yet more than half admit that redundancies, office closures or even going out of business would be on the cards if GDPR compliance fines were imposed on them.

Facing the challenge

The first challenge is understanding how, where and what impact the GDPR will have on the organisation.

1. Data controller or data processor?

First and foremost, companies need to figure out whether they are a data 'controller' or data 'processor'. The former controls the collection, uses and storage of data, the latter stores or processes data for the controller. Business partners and vendors must also be audited and reviewed to examine how they use and source data that could be connected to or used by the organisation.

2. Location, location, location

Where is your data and what data is relevant are two of the most dreaded questions when considering GDPR compliance. While organisations still wrangle over the US vs EU data centre/data privacy entanglements, the very notion of locating the right data, even just on your local servers, is a challenge. Then comes the question of exactly what data is relevant – just personal information, or specific contract terms applicable to individuals? Deleting or worse, keeping relevant data would fall foul of the law, but knowing what applies to your organisation and data is a GC minefield.

3. Developing a risk-based strategy

To misquote George Orwell, not all data is created equal. Some data presents more of a risk under GDPR than others and therefore deserves higher priority. Developing a risk-based strategy with the knowledge and understanding of the level of risk that each piece of data represents is a challenge in itself. Developing a risk-matrix can help prioritise the data according to its risk factor, and ensure compliance is not simply an expensive, data blanket-coverage exercise.

4. The technology conundrum

There is a plethora of technology available to help ease data woes, but knowing which technology is right for your company and your specific GDPR challenges is a long and laborious process. There simply isn't time to evaluate multiple systems and getting it wrong could cost valuable time in the race to compliance.

5. Allocate resources for compliance

The second, and perhaps biggest challenge, is locating resource. Arguably the reason so many organisations are unprepared and why GCs are stalling their approach, is the gargantuan level of resources needed to implement the changes required for compliance. Contracts must be located, adapted and clauses changed to ensure full compliance, teams motivated to update customer, supplier and partner terms and conditions, and systems and processes reworked to ensure all future contracts and clauses are revised. A mammoth task.

6. Compliance beyond the legal department

But the responsibility for GCs doesn't start and finish with the legal team. A third challenge is that they must ensure every business department that handles personal data is compliant. Teams from across the business are involved: sales and marketing, who use behavioural advertising and online tracking, to the finance department who use and store partner and vendor data, and most vitally the IT department which is at the core of protecting the data.

Simply knowing this and understanding the challenges is not enough. Now it is time for action; strategies must be implemented and tested, and board-level priority given to dedicating budget and resource to ensure compliance.

Where to start?

These challenges are not insurmountable. Every organisation will be impacted by the regulations in different ways, depending on a range of factors, such as the sector in which they operate, the nature and volume of personal data routinely processed and maturity of regulatory compliance within the current operating model. But, while a level of urgency is required, by working with the right partner, GCs and Data and Compliance Officers can ensure they achieve compliance, in time and on budget. At Exigent, we have already done the planning for you.

We have fully trained and qualified legal teams who have already helped many organisations navigate the GDPR compliance maze. Our legal teams can undertake a snapshot assessment of the impact of the new regime on the business so that any early steps can be taken to identify and implement the necessary changes.

At Exigent we conduct a four-point plan to help organisations achieve compliance:

1. Review

We will undertake a comprehensive review to benchmark the company's data protection policy and procedures against the requirements of the GDPR. We use technology-enabled solutions to perform a thorough analysis and assessment of your system architecture, existing policies and procedures. The assessment provides a data map illustrating the interaction of personal data across the company. A data map not only assists with compliance, but also contributes to improvement in operational efficiency of business processes, IT systems and intelligent use of data. Since the GDPR imposes stricter requirements for the processing of personal data, we recommend implementing a company-wide risk-based strategy. This is part of our technology-enabled solutions to identify, mitigate and manage GDPR associated risks to control and minimise potential impact. This risk-based strategy is a prerequisite of a 'privacy by design' approach.

2. Identify

We identify priority business areas where the GDPR will have the greatest impact to enable us to prioritise execution of the strategy. E-Discovery technology can help locate the right data, from personal details to contract terms and emails, to ensure you are processing and storing the right data. This process includes collecting and analysing data to prepare gap analysis and identifying any shortcomings in current processes. As part of the identification process, we will also work to pinpoint key stakeholders within the company to support the compliance programme.

3. Design

We design a strategy to rectify the shortcomings identified in our review process. This strategy will include processes to deal with revocation of consent and general client access requests, third party and customer contractual arrangements and creation of internal training and online testing material for compliance.

4. Execute

Exigent has the resources in-house to help implement the strategy, update contract templates and existing contracts to include processor language. We can also make recommendations for the update of security procedures that provide for breach notification. We formulate an Information Request List ("IRL") to determine the extent of the GDPR compliance and circulate this to third party processors. During and after execution, we will monitor guidance issued by the European Data Protection Board by checking for any legislative changes and impact.

Conclusion

The clock is ticking. We understand the challenges GCs face with GDPR and the urgency required to execute a strategy that ensures compliance by May 2018. Notably, the GDPR also represents an opportunity for organisations to get their business in order, re-evaluate processes, change workflows and ensure optimum resources where they are most required. As data breaches continue unabated, there will be increasing regulatory and public focus on what steps organisations are taking to prevent and protect the data in their care. Readying the business for this increased attention now will not only ensure fines and scrutiny are avoided, but that the organisation is proactively equipped for operation not just next year, but through 2019 and beyond.

To fast-track your GDPR implementation and navigate the regulatory changes contact Exigent now at http://www.exigent-group.com/contact/ or phone **+44 (0)207 578 9350**

exigent

+44 207 578 9350 | www.exigent-group.com/contact-us