WEIGHTMANS LAW FIRM HAS ADOPTED INTERACTION TO DRIVE GROWTH AND ENSURE GDPR COMPLIANCE, WITH THE POTENTIAL FINES FOR NON-COMPLIANCE PROHIBITIVELY HIGH AT €20MILLION OR 4% OF ANNUAL GLOBAL TURNOVER

How LexisNexis Enterprise Solutions assists law firms with GDPR

Andrew Lilley

By Andrew Lilley, Product Director, LexisNexis Enterprise Solutions.

Software vendors have a responsibility to help customers comply with the GDPR. In fact, their role is clearly defined in the regulation – Article 25 – Data protection by design and by default. Vendors need to proactively consider how their technology could potentially be used in a negative context and put in place controls to reduce the risks to users.

At LexisNexis Enterprise Solutions we have devised a service – GDPR Readiness Review – to help our customers align the configuration of their implementation of our products with their GDPR processes. For users of our CRM solution, Lexis InterAction, we are delivering workshops at customer sites. These involve a collaborative review to help identify where the firm may need additional product support to comply with the regulation, identify the functionality that can help enable their compliance processes, determine areas of the solution that need reconfiguration, assist with process changes in the solution to support GDPR procedures, and highlight the data quality challenges that the firm must address. The firm is presented with a personalised report that highlights recommendations for change in InterAction providing red flags for critical areas, to ensure that InterAction is suitably configured to meet their GDPR process requirements.

Similarly, for our legal workflow and case management system, Lexis Visualfiles, a Consultant visits the customer site to help users understand how the solution can be tuned to reduce GDPR related risks and makes recommendations to activate functionality in the software that would support their compliance programme. From a product standpoint, we have added functionality like data obfuscation tools to our Visualfiles and SolCase solution stack. These tools help firms protect sensitive data from unauthorised access in their non-production environments.

Over the last year, we have developed a range of content in the form of blogs e-books from internal and external industry experts on the importance and implications of GDPR for the legal sector to help our customers, and the rest of the market, navigate and comply with this important regulation.

Why it's important that firms comply with GDPR

Complying with the GDPR isn't an option. It is a regulation, not a directive and must be taken seriously. The penalty of a breach is high – up to four percent of global annual revenue. Any organisation handling personal data of an EU-based individual and/or offering goods and services to EU countries must comply with the GDPR.

While the emphasis is entirely on complying with the GDPR to protect themselves from the wrath of the regulator, there are clear business benefits for organisations, such as security, streamlined processes for data protection, potentially limited intervention from the regulator and hence minimal disruption to business, customer trust and confidence, and clean data – which in today's environment is the lifeblood of any business. Good quality data is invaluable for targeted marketing and business decision-making; and can truly deliver a competitive advantage to organisations.

> "Organisations can have the best systems in the world, but if its employees don't have a full understanding of the compliance obligations and the impact of non-compliance with the regulation on the business then the risk will increase substantially."

Not only that, it is good business practice to only hold the data necessary and appropriate to your business and to give the individuals you interact with control of their personal data.

What companies need to do across the board to comply

Foremost, organisations must understand what data they hold, then categorise it into different groups such as employee, customer, financial, corporate, partner, supplier and so on. Thereafter, they must determine the nature of the data – i.e. whether it is personal, sensitive, etc.; who is responsible for its protection, what is the purpose of processing this data, how has the information been obtained, where this data is stored (i.e. corporate network, cloud, PCs, spreadsheets, CRM, etc.); and is it shared with third parties. This will help organisations quickly build up a picture of what they are holding and how to protect it. Thereafter, it's important to determine, how easily it can be accessed to comply with data portability, right to erasure and retention and deletion policies.

Of particular note is the sixth principle of the GDPR, which pertains to the protection of data. It requires data to be "processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."(A5.f)

To this end, it's important that organisations keep their data processing systems up-to-date with the latest software patches. This includes updating the underlying operating systems as well as all the software that is used on a daily basis (e.g. MS Outlook, Chrome, business applications, etc). The most important software to keep up to date is of course, the malware protection and security software installed on the computers and networks.

It's worth ensuring that the IT department has certificates such as ISO27001:2013, ISO27018:2014 and Cyber Essentials. These demonstrate that the organisation is doing everything it can to protect the data it holds.

Employee education is imperative here. Organisations can have the best systems in the world, but if its employees don't have a full understanding of the compliance obligations and the impact of non-compliance with the regulation on the business then the risk will increase substantially. Staff must be aware of the internal processes in terms of what data is subject to the GDPR, where it can be stored, how it can be used, the company's policy for data retention, and so on.

The wider significance of GDPR and data protection

Security breaches have now become common place and with the GDPR, the EU is holding organisations responsible for the personal data they hold. This is the most wide-ranging and comprehensive regulation yet and empowers the Information Commissioner's Office (ICO) to fine firms up to four percent of their global turnover. The burden on organisations is substantial, given that it is widely accepted today that a security breach is a matter of when, not if.

At the same time, it is good for us as individuals. The GDPR gives us rights related to how our data is managed by organisations. Under the GDPR, organisations are required to seek "consent" through a privacy notice, which is transparent, intelligible and easily accessible. They must also rectify correct data and even completely delete or remove information, should someone request it.

Tedious as it may be, the good thing about the GDPR is that it will ensure lawful processing of data and best practice.