THE EUROPEAN
SPRING 2018
www.the-european.eu

BITING REGULATION
Bell Temple ask if your company is ready for GDPR

BLOCKCHAIN MASTERS
Executive education goes big on tech

BEST FOR BUSINESS
Commerce meets culture in Frankfurt

FOCUSED ON FDI

Maria Teresa Uribe Gómez, CEO of Davivienda Corredores on why now is the time to invest in Colombia

UK £4.95,
Europe €5.00

IS YOUR BUSINESS READY FOR GDPR?

The imminent arrival of new EU data privacy laws means that businesses must be prepared or face tough penalties. **Katherine E. Kolnhofer**, lawyer at Bell Temple LLP explains how it works

Organisations that have not yet implemented compliance strategies to enable them to adhere to the rigorous standards that will have to be met when the General Data Protection Regulation (GDPR) comes into force on 25 May 2018, are running out of time.

The GDPR is in response to the vastly different digital landscape organisations are now operating in, one that was previously unforeseen. One where the rapidly escalating cybersecurity threats proliferating the globe are resulting in the corresponding need for governments to remodel their regulations aimed at protecting the personal data and privacy of its citizens. "However fast regulation moves, technology moves faster. Especially as far as data is concerned," said Elizabeth Denham, UK's Information Commissioner[1].

The GDPR will have wide-ranging implications for SMEs and larger-scale organisations, particularly those that did not prioritise data protection and skirted previous legislation. For some, it will be a step-up from their current data protection practices; for others, it will require a complete overhaul of their approach to the "processing" [2] of personal data.

Accountability and transparency are the hallmarks of the new and modernised regime. Consumers will have enhanced rights and control over the processing of their personal data, as organisations will be required to implement consent procedures that require informed and affirmative action by the consenter.

Gone are the days of pre-ticked boxes. To be compliant, consent will have to be "freely given, specific, informed and unambiguous indication of the data subject's wishes…"[3]. The Regulation also ensures it can as easily be withdrawn.

To reinforce accountability, both "controllers"[4] and "processors"[5] will have to engage in mandatory record-keeping of the processing of personal data and have such records available for inspection by the Supervisory Authority upon request. In other words, auditing and inspections should be expected.

The concept of privacy by design has been specifically incorporated into the GDPR, an approach that requires organisations to be proactive as opposed to reactive towards data protection. Article 25 of the GDPR mandates that organisations implement data minimisation measures, such as pseudonymisation. In high-risk circumstances, organisations will have to perform a data protection impact

"Consumers will have enhanced rights and control over the processing of their personal data"

assessment (DPIA) prior to processing the personal data. Depending on the outcome of the assessment the Supervisory Authority may need to be involved in ensuring that proper mitigation measures are in place.

The likelihood is that most organisations will suffer a breach at some point in time. In the case of a personal data breach which is likely to result in a risk to the rights and freedoms of an individual, notification to whom, how much and how soon is now specifically prescribed. As soon as a "controller" is aware of a personal data breach he/she must notify the supervisory authority without "undue delay" and where feasible, within 72 hours of becoming aware. In a high-risk situation, this could also include notification to the "data subject" without undue delay[6]. The priority is mitigating harm and further risk to the individual. ➤

Sharp enforcement

To further ensure buy-in by the business community, this regulation has teeth. Depending on the severity of the infringement, Article 83 imposes fines up to 4% of annual globe turnover or 20m euros, whichever is greater.

Certainly, while the "data protection by default" requirements are onerous and daunting to many enterprises, successful compliance will mitigate the risks of a breach and often costly consequences to consumers and the organisation. That's the whole point.

"The likelihood is that most organisations will suffer a breach at some point in time"

Organisations should consider engaging the appropriate experts, such as legal counsel and IT professionals to ensure compliance with the GDPR, including preparing an incident response plan. Cyber insurance is also a key component to ensuring resilience in the face of an attack. Often such insurance policies provide access to a data breach team, including legal counsel and forensic IT professionals to coach the organisation in its response and ensure regulatory compliance.

The global economy will only become increasingly reliant on technology and the IoT ecosystem, increasing the attack surface. While at the outset it may require a significant infusion of capital to bring an organisation into the GDPR zone of compliance, organisations should embrace the regulatory changes. The investment will pay-off. ■

ABOUT THE AUTHOR

Katherine E. Kolnhofer is a Partner at international law firm Bell Temple LLP. She leads the firm's Privacy, Cybersecurity and Technology Law Group.

Further information

kkolnhofer@belltemple.com

Footnotes: 1 ico. Information Commissioner's Office. https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/01/information-commissioner-talks-gdpr-and-accountability-in-latest-speech/. 2 Regulation (EU) 2016/679, General Data Protection Regulation ("GDPR"), Article 4 (2), 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. 3 GDPR, Article 4(11). 4 GDPR, Article 4(7), 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data… 5 GDPR, Article 4(8), 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. 6 GDPR, Articles 33 and 34.