CURTAIN GOING UP ON GDPR

The preliminaries are done; GDPR goes into effect

May 25
GDPR: It’s showtime

Companies have had several years to prepare for GDPR yet many still are far from being fully compliant. With the launch deadline nearly upon us, Alan Earls reports on some final thoughts for corporate preparations.

Maybe it is just that people are reluctant to face up to bad news, like an ominous diagnosis from a physician. Or, perhaps it is the broad Atlantic Ocean, which seems like it ought to provide some insulation from the long arm of European law. Whatever the reason, most experts agree that companies on the North American side of the proverbial pond are too-often behind times in preparing for the consequences of the European Union’s General Data Protection Rules (GDPR), which sets a very high bar for privacy and data management.

This new regulation affects nearly every organization that does online business with citizens of the European Union, regardless of the citizens’ or the company’s geographic location. “If you process data of an EU citizen — even if your business is located outside of Europe or that individual is outside of Europe — you need to make sure you have systems in place to be GDPR compliant,” says Christopher Rence, chief information, security, and risk officer at Digital River, a Minnetonka, Minn.-based global ecommerce, payments and marketing services company.

The background, he notes, is that consumers globally are increasingly mindful of who is accessing, collecting, receiving, storing and otherwise processing their personal data. While some individual jurisdictions have tried to protect consumers with stricter regulations, no regulation anywhere in the world has attempted to compel so many companies, including those outside the borders of the body enacting the rules, to conform to a single compliance rule. In an effort to standardize emerging data protection requirements across Europe and improve trust in the rapidly expanding digital economy, the European Parliament and Council introduced GDPR.

Rence points out that GDPR sets strict rules for protecting the personal data of EU citizens and becomes enforceable starting on May 25, 2018. “GDPR gives individuals greater control over their data, and sets out a number of additional safeguards companies need to follow when processing consumer data,” says Rence. The regulation applies to all forms of processing including in the context of marketing, employment, information security, customer service, business-to-business sales and ecommerce.

Karen Schuler, consulting partner, national information governance practice leader at the Forensic Technology Services arm of BDO, a consulting firm in the Washington, D.C. area, notes that Article 34 of GDPR, requires “the controller” to notify data subjects without delay. “In talking with organizations about their readiness to respond and notify individuals of a data breach, we’ve discovered they have good

OUR EXPERTS: GDPR

Sara Hollan Chelette, co-chair of the cybersecurity litigation practice, Jackson Walker
Steven Durbin, managing director, Information Security Forum
Dan Frank, principal, Deloitte Risk and Financial Advisory Cyber Risk Services
Kevin Kish, privacy technical lead, Schellman & Company, Inc
Christopher Rence, chief information, security, and risk officer, Digital River
Karen Schuler, consulting partner, Forensic Technology Services arm of BDO

18% Survey respondents who said they understood what data their company has and where it lives

― Commvault
security controls in place, but many have not tested their incident response capabilities,” she says. Others have yet to implement the robust security awareness and annual training required by GDPR, she says.

For many U.S. companies, particularly those in highly regulated industries, many GDPR requirements might have already been fulfilled through their current data management and information security practices, says Schuler. However, even organizations with robust information governance programs must confirm that their current policies and protocols adequately address GDPR requirements and shore up any gaps.

Schuler says her organization has analyzed GDPR in comparison with other legal and technical frameworks to see where commonalities might help “jump start” an organization. Unfortunately, in comparing GDPR controls to ISO 27001, Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standards (PCI DSS), NIST Special Publication 800-53 and ISO 15489, BDO found little commonality. “Comparing ISO 27001 and PCI-DSS to GDPR, there are a mere 15 controls that overlap,” she says. On the other hand, “the foundation an ISO or NIST framework provides can be a good way to offset a complete overhaul of policies and procedures,” she adds.

“Many organizations are already wrestling with various challenges around critical information asset management; the GDPR’s standards for the handling of EU

Data protection by design and default

Enshrined in GDPR are two guiding principles: First, organizations are encouraged to build data protection from the inception of systems and processes rather than simply as an after-thought. Second, GDPR encourages systems and processes to be implemented in a fail-safe manner, so that at every step, risks of data loss are minimized, for example through storing data for the shortest time required to make use of it. Karen Schuler, consulting partner in the Forensic Technology Services arm of the security consultancy BDO, recommends focusing on eight crucial steps if you are still preparing for compliance:

1) **Determine** whether you are a controller or processor of EU personal data. Many companies fall into both categories, so it is critical to identify which business processes could require you to follow controller and processor guidelines.
2) **Make** sure you understand and document your business processes and the systems and data tied to those processes.
3) **Develop** a data register with the legally required elements.
4) **Review** your contracts with outside parties to ensure you include GDPR-relevant language, as outlined in Article 28.
5) **Review** your vendors to ensure they are taking steps to become GDPR compliant.
6) **Ensure** your policies and procedures are aligned with organizational needs, and that they address GDPR requirements, as well as any other U.S. regulatory requirements that might apply.
7) **Identify**, where applicable, a data protection officer. The data protection officer will serve as the organization’s liaison to the relevant supervisory authorities.
8) **Map** out ongoing requirements and develop a response plan for a request for information, so you will be ready if and when it happens.
residents’ personal data add another layer of complexity,” says Steven Durbin, managing director of the Information Security Forum, a London-based, independent, not-for-profit organization focused on cyber, information security and risk management. Not surprisingly, he notes, businesses are encountering many difficulties as they prepare for the May deadline. First and foremost is the widespread lack of awareness among internal stakeholders.

“Addressing the obligations will likely cause compliance and data management costs to increase; in many cases, it will be necessary to pull resources and attention away from other important efforts in order to ensure that required processes and plans are implemented in time,” Durbin says.

**Data processor or data controller: the difference matters**

According to the EU’s GDPR website, under the regulation, a data controller “determines the purposes for which and the means by which personal data is processed.” Typically, that means a company and its employees. On the other hand, a data processor, typically a third party, “processes personal data only on behalf of the controller.” Each role has its own requirements and those roles can change depending on circumstances.

Schuler says controllers need to maintain a register that includes the type of processing activity as it pertains to each business process, the purpose of processing and contact information identifying the individual responsible for controlling the information. Also required is a description of categories of data subjects and categories of personal data, who will receive this personal data, transfers of personal data, time limits for erasure for each category of data, and a description of organizational security measures.

For processors, the task is a little less onerous, she notes. “Their register should include a list of process activities carried out on behalf of the controller and should identify contact information, data protection officers, categories of processing, transfers of personal data, and a general description of the organization’s security measures.”

The regulations also define “a joint controller” — a situation with its own complexities. Additional information about GDPR is available from the EU’s official site.

**Implementing GDPR**

When trying to turn plans and promises into GDPR compliance, try being realistic. “Across the board, senior leadership seems to understand that compliance with GDPR is mandatory and that they must do whatever is necessary to comply...but some organizations believe they are closer to compliance than they really are,” says Schuler. Organizations do not realize how extensive the requirements are and assume they do not need to put forward much effort to become compliant, she says. A readiness assessment and gap analysis can be one way for companies to prioritize remediation efforts.

But it has to start at the top, according to
Assigning specific responsibility for GDPR can also help. “At the Information Security Forum, we believe that a data protection officer (DPO) should be designated to act as a focal point for ongoing data protection activities,” he says. Furthermore, an organization’s governance functions, including information security, legal, records management and audit should be familiar with the requirements of the GDPR and have the necessary people, processes and technical capabilities in place to achieve compliance.

Amplifying the discussion about roles and responsibilities, Daniel P. Frank, principal with Deloitte Risk and Financial Advisory Cyber Risk Services in the Chicago area, says it is important to get past the idea that GDPR is just a problem to be handled by the privacy or security function. “The reality is that to comply with GDPR it ‘takes a village’ and virtually every business function, and every individual, plays a role,” Frank says.

For example, legal departments must interpret GDPR requirements and provide sound counsel on the business activities that fall under GDPR purview, he notes. Internal audit plays an important role in assessing GDPR readiness, while IT departments will be on the front lines of GDPR capabilities such as “privacy by design” and data protection impact assessments. Procurement departments, working with legal, play a role in assessing third-party contractual clauses. And, he notes, continuous monitoring of compliance and risk requires the steady vigilance and guidance of compliance and risk functions.

As with other amorphous business challenges that don’t go directly to the bottom line, motivation and communication are important. Organizational campaigns and general awareness training programs are a great way to generate buzz on GDPR and to prime staff on its wide-ranging requirements, notes Kevin Kish, privacy technical lead at Schellman & Company, Inc., a security and privacy compliance assessor. Longer term, your organization’s first line of defense is the people who interact with customers. So, Kish says, it makes sense to build a tactical, role-based training plan with department privacy leads to address how specific business units should handle data in their possession.

Consider what happens if a customer service representative receives a data subject access request [under Article 15-22] from a client in which the client is requesting that their personal data be sent to a competing company, says Kish. “If the request isn’t resolved properly, the client has lawful grounds to submit a complaint to their supervisory authority (e.g. regulatory authority),” he says. One place to start is to develop metrics to track things like response time to a customer inquiry, to measure the success of your privacy strategy,” Kish says. Because the GDPR definition of personal data is far broader than the definition of personally identifiable information or personal information that U.S. companies might be familiar with, it is wise to start your preparation by creating a data map or data

---

52% Percentage of survey respondents who say that their organization is either not concerned about GDPR or are unaware of its relevance for their business

– HyTrust
inventory, says Sara Hollan Chelette, co-chair of the cybersecurity litigation practice at Jackson Walker in Dallas.

GDPR specifically defines personal data as any information relating to an identified or identifiable natural person. A person can be identified by a name, identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of the person, she says.

That’s a very broad scope, so an organization needs to know what personal data it collects, how it collects the data, where the data travels, where the data resides, who has access to the data, how the data is used, and how long the data is stored.

“Preparing a data map or inventory is a crucial step,” she says.

The process must then continue with a review of customer communications, disclosures, privacy policies and justification for processing personal data, she explains. Entities must have procedures to comply with the rights of data subjects such as reviews for accuracy, the right to be forgotten, or requests to transfer information. Clarity must also be ensured about consent — when it is given and when it is withdrawn, she says.

Size matters too. A data protection officer is required if the controller’s or processor’s core activities consist of regular and systematic monitoring of data subjects on a large scale. And, of course, GDPR is strict regarding data transfers to any country deemed to have less-than-adequate data protections, the U.S. being a prime example.

Fasten Your Seatbelts

“While GDPR is more stringent than any data privacy regulation we have in the U.S., in our view, it’s just a matter of time until U.S. regulators play catch up,” says Schuler. “GDPR is just a kick in the pants for organizations that have put information governance on the back burner,” she adds.

The million-dollar question: If we attempt to comply with GDPR requirements, will we be viewed in a better light should a data breach occur? “The simple answer is — we will see,” says Schuler. In a reasonable world, “it would make sense” that if you make a good faith effort to comply, your fines would be lower as a result, especially in a world where a data breach and human error are certainties, she says. But no one will know until after May 25, 2018.

“No organization that operates on a global footprint of suppliers can afford not to prepare for changes that will result from new GDPR compliance rules,” says Durbin. GDPR is putting data protection practices at the forefront of business agendas worldwide and for most organizations, the coming weeks will be a critical time for their data protection regimes as they determine the applicability of GDPR and the controls and capabilities they will need to manage their compliance and risk obligations, Durbin says.

“The good news is that, in the long run, organizations will benefit from the uniformity introduced by the reform,” says Durbin.

For more information about ebooks from SC Media, please contact Stephen Lawton, special projects editor, at stephen.lawton@haymarketmedia.com.

If your company is interested in sponsoring an ebook, please contact David Steifman, VP, publisher, at 646-638-6008, or via email at david.steifman@haymarketmedia.com.

39%

Percentage of UK-based SME survey respondents who said they had yet to start planning for GDPR in January 2018

– The Data Compliance Doctors
RSA offers Business-Driven Security™ solutions that uniquely link business context with security incidents to help organizations manage risk and protect what matters most. RSA solutions are designed to effectively detect and respond to advanced attacks; manage user identities and access; and, reduce business risk, fraud, and cybercrime. RSA protects millions of users around the world, and helps 90% of the Fortune 500 companies thrive in an uncertain, high risk world.

Learn more at rsa.com.
The General Data Protection Regulation (GDPR), the European Union's new data protection law, represents a major evolution in global data security and privacy practices. Visit rsa.com/gdpr for information to help you navigate GDPR preparation.