Published on *The National Law Review* https://natlawreview.com

As the GDPR Compliance Date Looms, Risks and Budgets Grow in Tandem

Article By:

Daniel L. Farris

Jean Marie R. Pechette

As the May 2018 effective date of the General Data Protection Regulation's (GDPR) looms, U.S. companies have had to expand their investment in implementing measures to ensure compliance with the GDPR. According to a recent PwC Pulse Survey, 92% of respondents considered GDPR a "top priority" in 2017, with 77% of companies planning to allocate more than $1 million, and 68% saying their budget falls between $1 million and $10 million.

"No legislation rivals the potential global impact of the EU's General Data Protection Regulation," said Jay Cline, PwC's U.S. Privacy Leader. "The new law will usher in cascading privacy demands that will require a renewed focus on data privacy for U.S. companies that offer goods and services to EU citizens."

PwC's survey comes on the heels of December 2016 guidance from prominent GDPR analyst, Chiara Rustici, advising "businesses to ring fence 4 percent of 2016 global turnover and earmark it as budget for 2017 compliance." Rustici's budget advice was released too close in time to fully account for the EU's Article 29 Working Party GDPR guidance, which clarified certain key issues surrounding the ways in which EU Member States plan to enforce the sweeping data protection reform.

The costs and urgency of GDPR compliance may come as a shock to some companies. "American multinationals that have not taken significant steps to prepare for GDPR are already behind their peers," Cline said in PwC's report. Rustici gave similar advice in 2016: "There are no excuses for not having a GDPR budget in place before the end of 2016." Though there is still more than a year left for companies to attain compliance with the GDPR, and further guidance is expected from EU data protection regulators about how they intend to enforce the regulation in the coming year, PwC cautioned that companies should not wait to get up to speed.

For organizations wondering where to start – data mapping, developing data portability programs, hiring a Data Protection Officer, and obtaining the necessary budget – are perhaps the most important steps to take.

Need for Data Portability and Data Mapping

A key issue addressed by the Article 29 Working Party in the December 2016 guidance was the issue of “Data Portability,” which states that consumers must have access to their personal data in a manner that allows them to easily move the information to a different service provider. Data Portability works in tandem with other important GDPR concepts, like the Access Principle (individual’s right to know what personal data a company holds) and the “right to be forgotten” (individual’s right to request that personal data held by a company be eradicated). To accomplish these measures, Article 30 of GDPR practically obligates companies to develop comprehensive data maps to understand what data the company has, where it is stored, how it flows, with whom it is shared, and how it is used.

The Article 29 Working Party also highlighted the need for companies to start developing systems to respond to consumer requests for data under the data portability provision, including using technological means. "One of the ways in which a data controller can answer requests for data portability is by offering an appropriately secured and documented Application Programming Interface (API)," the Working Party advised. "This would enable individuals to make requests for their personal data via their own or third-party software or grant permission for others to so do on their behalf.” No matter how an organization attempts to tackle these issues, data mapping and data portability require significant undertakings by a company’s IT department.

Budgeting

"Securing a $1 million budget for data privacy has been more an exception than a rule for many American corporations," PwC wrote in its survey. "The GDPR's potential 4 percent fine of global revenues, however, has changed budget appetites for mitigating this GDPR risk." Because of the significant risk to multinational corporations and due to the pervasive nature of data in modern business operations, GDPR budgeting should be an enterprise-wide exercise (not merely legal, compliance, and/or IT). “[T]he budget is there to ensure that any interaction of EU-based individuals with a brand's real and digital estate follows the EU data protection principles,” says Rustici, and “that will mean product design, user experience, distribution and after sales support, HR, marketing, legal, risk and compliance, storage and security should all own a share of the corporate GDPR budget.”

A good GDPR budget may contain line items and funding allocation for some or all of the following:

- Budget for data inventory and mapping
- Budget for privacy and state-of-the-art safety by design
- Budget for solutions to enable data portability and the right to be forgotten
- Budget for internal training so employees can recognize GDPR personal data flows
- Budget for stress-testing GDPR resilience, information security, and audit
- Budget for coordination and compliance across the organization
- Budget for vendor management

- Budget to hire a GDPR architect, CISO, and/or DPO

Hire a Data Protection Officer

GDPR requires companies that process personal data “as a core activity” and/or monitor data subjects “on a large scale” to hire a Data Protection Officer (DPO). The DPO’s role is to serve as an independent monitor of corporate compliance. In its 2016 Guidance, however, the Article 29 Working Party suggested that EU Member States will look beyond the express language of GDPR when examining a company’s compliance. "Even when the GDPR does not specifically require the appointment of a DPO, organizations may sometimes find it useful to designate a DPO on a voluntary basis," the group said. "The Article 29 Data Protection Working Party encourages these voluntary efforts."

Whether data collection or processing is “large scale” or a “core activity” of a company will also be braodly interpreted. Factors such as the volume of data, the geographic breadth of data, and the importance of data to a company’s operations may all be relevant to the DPO requirement. Using healthcare as a reference, the Article 29 Working Party clarified by way of example: “the core activity of a hospital is to provide health care," the Working Party noted. "However, a hospital could not provide health care safely and effectively without processing health data, such as patients’ health records. Therefore, processing these data should be considered to be one of any hospital’s core activities and hospitals must therefore designate DPOs.” Companies operating in highly regulated industries – such as healthcare, financial services, and insurance, as well as consumer businesses, should anticipate the need for a DPO.

A DPO alone, however, may not be enough. A GDPR architect – that is, a good CISO, CIO, CTO, privacy lawyer, compliance officer, or all of the above – may also be required. “Think of a DPO as a ship's captain and of a GDPR architect as the naval engineer,” Rustici warns. “[T]o set sail to the seas you rely on a good captain, who can chart a course and avoid thirty-foot waves; but to build or make a ship sea-worthy, and ensure that it can withstand even thirty-foot waves, you first rely on a good naval engineer.”

Other Initiatives

Other top initiatives for U.S. multinationals in 2017 may include reviewing and revamping privacy policies, examining how the organization ensures consent for collecting/processing personal data of customers, and improving vendor management programs to ensure regulatory compliance and hardened information security. Many organizations are also considering data localization options, including moving data centers to Europe, while others are assessing the viability of moving operations out of Europe altogether.

National Law Review, Volume VII, Number 27