Privacy Law Watch™

June 08, 2017

Bloomberg BNA

Data Protection

New EU Privacy Regime Fear, Loathing Driving Costs, Decisions

BNA Snapshot

- New EU privacy regime effective date fast approaching as companies seek compliance answers
- Lessons, insights from reviewing how data is stored, used, handled

By Joyce E. Cutler

Many companies have considered how to comply with the European Union's sweeping new privacy regime but haven't implemented their compliance planning, according to a new survey report released June 7. But the looming May 25, 2018, effective date of the EU's General Data Protection Regulation is pushing companies into what can be a costly compliance mode, privacy professionals told Bloomberg BNA.

Just 4 percent of companies are done with their GDPR compliance efforts, the survey report by privacy risk and compliance consulting company TrustArc, formerly known as TRUSTe, said. The May survey of 204 privacy professionals—92 percent of whom are based in the U.S.—found that 18 percent had a GDPR plan in place but hadn't begun implementation, and 61 percent haven't begun their implementation planning.

Companies have been focused on the GDPR's new massive fines of up to 20 million euros ($22.5 million) or 4 percent of a company's worldwide income but need to turn their attention to the new law's policy and technical privacy and data security requirements, privacy pros said.

“After initial hyperventilation due to the 4 percent potential fine,” companies should focus on a compliance path, Jim Koenig, global co-chair of Fenwick & West LLP's privacy & cybersecurity practice, told Bloomberg BNA June 6 on the sidelines of a TrustArc conference in San Francisco.

Companies can break the GDPR down into compliance effort primary buckets: making changes in user consent and other policies; developing new or enhanced processes, including for data breach notification; adopting privacy impact assessments and record keeping; and making decisions about whether to build or buy solutions, Koenig said.

Technology Drives Compliance Costs

The law requires technology and record-keeping changes to allow companies to document verifiable user consent to the use of personal data, Koenig said. The GDPR raises the new concept of digital accountability, “where privacy for the first time in a real way will have to be linked to actual data management and IT,” he said. “The GDPR signals the start of a sea change in privacy, where more and more IT and applications will be needed to support and to validate compliance,” Koenig said.

The TrustArc survey found 83 percent of companies expect GDPR compliance to be a six-figure expense; 65 percent expect to spend $100,000-$1 million on compliance, including for internal and external personnel, training, consulting, legal advice, technology, and tools; and 17 percent expect to spend more than $1 million.

Respondents to a recent Veritas Technologies LLP survey said they expect their organizations to spend over $1.4 million by May 2018 in order to achieve full compliance.

Unlike the Y2K scare, in which companies spent a substantial amount responding to a finite event—the rollover to the year 2000 that many warned would compromise computer programs that hadn't anticipated dates in the new millenium—complying

with the GDPR is more like complying with the federal Sarbanes-Oxley financial services law, Chris Babel, TrustArc CEO, said. That is, compliance spending on tools, technologies, and processes will be spread out over the business, and over a longer time, to maintain compliance, he said.

Ready or Not

Getting ready to comply with many of the GDPR requirements requires “a substantial lead time,” Lokke Moerel, privacy senior of counsel at Morrison & Foerster LLP in Berlin and a professor at University of Tilburg Law School, told Bloomberg BNA June 7. Ideally, companies would be “about halfway” through the implementation effort, she said.

Mauricio Paez, a privacy partner with Jones Day in New York, agreed. Companies that haven't already started implementing their GDPR compliance “are fairly late,” Paez told Bloomberg BNA June 6.

As for the 4 percent of survey respondent companies that said they were done with their GDPR compliance—they should reconsider, Babel told Bloomberg BNA June 6. The “only way you're done is you're not in Europe,” he said.

At the other end of the scale are companies that are just waking up to their GDPR compliance obligations. Companies that didn't realize they are covered have been “caught flat-footed, and they will need to scramble to bring their compliance programs up to speed,” Rebecca Eisner, a privacy partner, and **Lei Shen**, a senior associate, with Mayer Brown LLP in Chicago told Bloomberg BNA in a June 6 joint email.

David Moseley, GDPR solutions leader at Veritas, told Bloomberg BNA June 6 that when the GDPR was first announced, it was generally regarded by companies as an EU challenge. But “it doesn't matter if you're based in the EU or not, if your organization does business in the region processing data of an EU resident, the regulation applies to you,” Moseley said.

To contact the reporter on this story: Joyce E. Cutler in San Francisco at JCutler@bna.com

To contact the editor responsible for this story: Donald Aplin at daplin@bna.com

For More Information

The TrustArc survey report is available at http://src.bna.com/pAf.