Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Scope Of EU Privacy Law Has Companies Scrambling To Comply

By **Allison Grande**

Law360, New York (April 20, 2016, 4:19 PM ET) -- European policymakers recently cleared the way for sweeping data protection measures to take effect in 2018, a move that should inspire companies to immediately take stock of the data they hold and the privacy practices they employ in order to boost their chances of avoiding significantly enhanced regulatory penalties.

After more than four years of negotiations, the European Parliament last week **became the final political body** to give its backing to the proposed general data protection regulation, or GDPR, which will replace the current patchwork data protection framework with a uniform regime that tightens restrictions on the use and flow of data while empowering national privacy regulators to levy fines of up to either 4 percent of a company's annual global revenue or €20 million ($22.2 million).

While the regulation won't take effect for another two years, attorneys say that the breadth of the new regulation — coupled with the significantly ramped up consequences for noncompliance — requires that multinationals start taking steps now to get ready for 2018.

"Companies need to sit down and consider how they're going to be affected by this and how they're going to up their game to make sure that they comply with the increased requirements of the GDPR," said Timothy Toohey, a Greenberg Glusker Fields Claman & Machtinger LLP partner.

Given that the regulation greatly expands multinational companies' obligations when it comes to collecting, storing, transferring and using personal data, most businesses will need to set up new procedures and policies for interacting with their EU customers — a process that will require a large investment of both time and resources.

"Two years may seem like a long time, but there are a lot of things that companies will need to do to make sure they're compliant," Squire Patton Boggs LLP partner Gretchen Ramos said.

One of the first steps that companies will need to take is to familiarize themselves with the text of the GDPR, which spans nearly 300 pages, and to confirm that they are indeed swept up by the regulation. While companies could avoid the existing directive's pull by physically staying out of the EU, the regulation is much broader in that it applies to any business that offers its services to consumers who reside in the bloc.

Once they have a firm grasp on their obligations, companies should turn to the task of taking an inventory and mapping out the data they hold, so that they can start the process of figuring out how to comply with provisions such as the enhanced consent requirement and the obligations to erase and transfer data at users' request, attorneys say.

"There's no point in knowing one without the other," Fenwick & West LLP attorney Jonathan Millard said. "If you're an expert on the GDPR but don't know where your data is, that's not going to matter, and if on the other hand you're hot on your data but don't know about the GDPR, that's not going to be helpful either."

The data mapping exercise is particularly important in light of several changes teed up by the regulation that will require companies to revamp the way that they interact with consumers and obtain permission to use their data, according to attorneys.

Europeans' attitude toward U.S. privacy protections has changed dramatically since the European Commission **first floated** the data protection overhaul in January 2012, with developments such as the leak of information about U.S. intelligence-gathering activities by Edward Snowden and the **recent invalidation of** the trans-Atlantic safe harbor data transfer regime making many in the EU increasingly skeptical of the ability of U.S. entities to adequately protect their data.

"The tensions were there in 2012, but now they're coming up to the surface, and whether they like it or not, companies have been caught up in these issues," Toohey said.

This shift has led to the tightening of certain mechanisms during the life span of the GDPR, including those involving the consent required for obtaining and processing data and the rights that EU citizens have to control what happens to their data after they've handed it over to a business.

The new regulation includes not only a stronger consent mechanism that requires data use requests to be specific and clear, but it also embraces the newly developed rights of data erasure and data portability.

In order to be successful in complying with these changes, businesses will need to make a significant investment in data management, attorneys say.

"Companies are going to need to have a system in place so that they know what data they have and what it is," Ramos said. "It may seem like a simple thing, but it’s not always so simple depending on how systems are set up."

Many businesses — especially large operations that hold vast troves of consumer data that they use for a variety of purposes, from advertising to profiling — will likely need a big chunk of the upcoming two-year transition period to establish and thoroughly test such a system, according to attorneys.

"Any time that organizations make a change that involves data management components, there's always the possibility that there will be problems or imperfections," said Jim Koenig, who is of counsel in the privacy and cybersecurity practice at Paul Hastings LLP. "That's why companies have two years to make sure that the technology is tested and seamless and works well for their organization."

Delivering on such changes will also require general counsel and others responsible for compliance to work on their boards of directors to secure both buy-in as well as expanded budgets, attorneys noted.

"It's a corporate risk if the business is not in compliance, and that risk is going to be huge come 2018," Ramos said.

The heightened risk profile primarily stems from the chance for fines that promise to be much greater than anything that companies saw under the old regime.

"Europe doesn't have a history of strong enforcement and penalties, but the [new fines under the regulation] ... are going to get the attention of senior management," Koenig said. "When the first enforcement action with a heavy fine is announced, that will be a shot across the bow of European and global companies everywhere that Europe has gone from being behind the curve in terms of levying fines and penalties to now being able to impose significant financial consequences."

Besides having the opportunity to get their systems and board members up to speed, the two-year implementation period will also give companies a window to clear up questions and uncertainties they may have about the regulation, attorneys noted.

While the point of the regulation is to unify the current patchwork of member state data protection laws, the new regime does raise significant concerns about issues including how unified an approach regulators will take to enforcement and how countries will deal with the dozens of implementing acts that will allow them to set their own rules when it comes to topics such as the age required for parental consent when it comes to the collection of children's data, attorneys say.

"To some extent, U.S. companies welcome the GDPR because they feel that it offers greater harmonization, but there are national differences and differences between the various national data protection authorities that are not going to go away," said Paul Schwartz, special counsel at Paul Hastings and a professor at the University of California, Berkeley, School of Law.

Companies over the next two years will also be looking to regulators for additional guidance on how to meet their new obligation to report data breaches within 72 hours of their discovery. While U.S. companies have ample experience with breach notification under their long-standing duties under a patchwork of state laws, they still need clarity about what their notice to EU officials must contain and what exactly will trigger a report in order to allow them to develop procedures to meet their strict new responsibilities, attorneys say.

"Having breach response plans in place will be critical because, like in the U.S., if a company doesn't have procedures in place so that it knows what to do if there is an incident, that's where it can get itself into trouble," Ramos said.

With the Parliament's approval of the regulation last week, and the European Council's backing of the reform efforts the week before, the regulation now moves into its final phase of being prepared for publication in the Federal Register. Once it's been out for 20 days, the two-year implementation clock will begin ticking, setting off what promises to be a very eventful 24 months for multinationals.

"While this step [of the regulation gaining approval] was expected, it heralds the largest transformation in European privacy regulation in two decades," said David Turetsky, Akin Gump Strauss Hauer & Feld LLP's cybersecurity, privacy and data protection practice co-leader. "[And] the path for many companies to become ready begins now."

--Editing by Jeremy Barker and Katherine Rautenberg.