# 2018 Brings New EU Privacy, Cyber Regime, But Some Laws Up in Air

*By George Lynch*

Game-changing new European Union privacy and cybersecurity laws take hold early in 2018, triggering the need for a wholesale shift for companies that transfer personal data outside the 28-nation bloc.

But an incomplete adoption of implementing legislation so far by member countries, and a surprising lack of harmonization among laws will leave companies scrambling to adjust. Billions of dollars in transatlantic trade flow between the EU and U.S. every day, making compliance, however demanding, essential for companies doing business in the EU.

The new regime brings a raft of changes. The potential for steep fines, along with a risk of private lawsuits, makes 2018 a much-anticipated year of reckoning for U.S. companies.

Of the two new laws, the General Data Protection Regulation (GDPR) is the more seismic. It covers privacy and data protection in the processing of EU citizens' personal data, and upends and replaces the EU's previous, 22 year-old privacy scheme. EU regulators will be empowered to impose fines of up to 20 million euros ($23.5 million) or 4 percent of a company's global revenue, whichever is higher.

At issue is the fact that the GDPR gives countries leeway in crafting their own national laws. Up to one-third of a country's provisions can stray from the text of the GDPR, including whether employers have access to employee criminal records and other types of employee data processed by employers.

Prospect of Compliance: 'Mind-Boggling'

"The prospect of having to comply with 20+ Member State laws in addition to the GDPR is mind-boggling," Wim Nauwelaerts, a data protection partner at Sidley Austin LLP in Brussels, told Bloomberg Law. "Divergences at the member state level will impact key decisions that practically every cross-border business is facing, such as 'do we have to appoint a [data protection officer] DPO,' and 'can we run background checks on new hires.'"

The variance in member states' GDPR implementation laws, enacted or under review, is wider than first anticipated, privacy attorneys told Bloomberg Law.

The resulting uncertainty clouds the ability of companies and attorneys advising them to properly prepare even for basic decisions, such as choosing the location for a company's data processing operations, Nauwelaerts said.

The second EU-wide standard, the Network and Information Security (NIS) Directive, is a new requirement that sets cybersecurity standards for operators of essential services and digital service providers, which include companies that provide EU citizens with search engines, cloud services, or online marketplaces, such as Amazon.com Inc.

## Fuller Picture to Emerge

The GDPR will take effect across the EU May 25, 2018, even though most of the 28 EU member countries aren't expected to enact implementing legislation until a few months before it is

effective. As of Dec. 5, only Germany and Austria had passed final GDPR laws.

The NIS Directive enters into force May 9, 2018, but directives require countries to adopt national laws to take effect. It's unclear whether countries will enact NIS laws in time for companies to get new compliance programs in place. So far, only two have: Germany and the Czech Republic.

In addition, a company covered by the GDPR and NIS could be responsible for fulfilling different compliance requirements and answering to different regulators.

**Risk of Noncompliance**

"Businesses that are active across the EU risk being noncompliant if they focus on the GDPR only," Nauwelaerts said.

Many companies covered by both the GDPR and NIS Directive will face layers of compliance from more than one regulator. For example, a company covered by both laws might have to answer to two sets of regulators and face different notification standards stemming from the same data breach, such as in the timing and content of notifications and differences in the regulators who must be notified of a cyberattack.

Also, the GDPR requires companies to report data breaches to the data protection authority in the country in which they process data. The NIS Directive requires companies to report cybersecurity incidents to a regulator to be designated by each member state, which varies by industry.
When it comes to setting up compliance programs, "not many companies are able to do NIS and GDPR at the same time," Jorg Hladjk, data protection of counsel at Jones Day LLP in Brussels, told Bloomberg Law.

**Companies: Show Your Work**

"Most regulators want to see you made a good faith effort to move the ship in the right direction even if you haven't completely complied to every obligation to the last degree," Ann LaFrance, a data protection partner at Squire Patton Boggs LLP in London, told Bloomberg Law.

Few companies will achieve full compliance before the GDPR and NIS Directive take effect, so they need to be prepared to defend their compliance programs—however imperfect—to regulators and consumers. Individual consumers are free under the GDPR system to file private lawsuits to recover damages for violations, such as a company using an individual's data without a valid legal basis.
"The bottom line is that the onus is on the companies to be compliant. They have to do their risk assessment and take responsibility," Rohan Massey, a partner at Ropes & Gray LLP in London and leader of the firm's privacy and cybersecurity practice in Europe, told Bloomberg Law.

Meticulous documentation by a company of the steps it has taken to comply and the reasoning behind those decisions will go a long way toward demonstrating its good faith effort at compliance, and could help mitigate the risk of formal enforcement actions by privacy regulators.

Demonstrating good faith compliance to regulators may also help companies prepare to defend against possible litigation, Tim Wybitul, data protection partner at Hogan Lovells LLP in Frankfurt, told Bloomberg Law. Because the GDPR is so complex, companies should be aware that it will be easy for attorneys representing consumers to point out compliance errors, he said.

Because the variations in national laws are still unknown, the best companies can do is to look for common denominators among the implementation laws as they are released and document good faith efforts to comply, Hladjk said.

“Companies need to have the ability to go back to regulators and say ‘This is why we made decisions, this is why we didn't go forward, this is why we are waiting, this is why our program isn't fully developed by May 25, but will be by a later date for these reasons,’” Massey said.