Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

5 Common Myths About EU's New Data Protection Regime

By **Allison Grande**

Law360 (May 11, 2018, 6:52 PM EDT) -- The sweeping General Data Protection Regulation set to take effect in the European Union in just two weeks promises to revolutionize how companies around the globe handle personal data while imposing stiff penalties on those that don't comply. But attorneys say that although companies have had two years to get up to speed, several troubling myths still persist.

Even as the long-anticipated implementation deadline of May 25 closes in, attorneys say they are still fielding calls laced with misconceptions about the scope, reach and penalties behind the game-changing GDPR.

Under the new regime, companies that offer services to EU residents or process personal data within the bloc will face tighter restrictions on the way they use, share and protect personal information while contending with the prospect of penalties of up to €20 million or 4 percent of their annual worldwide revenue, whichever is higher.

Much has been written about the various obligations under the lengthy regulation since EU policymakers finalized it and gave businesses two years to comply in 2016, leading to a whirlwind of conflicting perceptions about which companies and types of data are covered by the law, how onerous the hefty fines and tight breach reporting window will really be, and what will actually happen after May 25.

"There's been so much put out there about the GDPR, and a lot of what we do is try to give better understanding to clients who hear a lot of different things about the regulation," said Debevoise & Plimpton LLP partner Jane Shvets, who is based in London.

Here, attorneys set the record straight on some of the top inaccurate assumptions they've heard from clients.

Those Outside the EU Can Rest Easy

As European lawmakers and member states were working to finalize the regulation, one of the most troubling aspects for many companies was the broad extraterroritorial reach of the regulation. Besides covering companies that have a physical presence in the EU, the law is designed to reach businesses beyond its borders as long as they are offering services to individuals within the bloc or are monitoring their behavior.

"The first question honestly that we get from companies is do we really have to comply, and the answer is usually yes," Baker Botts LLP special counsel Cynthia Cole, who is based in California, said.

Several attorneys said they are still fielding calls from clients asserting they don't have to comply with the regulation because they don't have a physical presence in the EU and therefore should fall outside regulators' purview. But aside from "a couple fringe cases," most companies have business operations that touch the EU in some way and therefore are caught up by the regulation's wide net, even if no one from the company has ever set foot in the bloc, Chicago-based Foley & Lardner LLP partner Aaron Tantleff said.

"Generally speaking, GDPR is extraterritorial and applies to companies all over, and while that may be concerning and frustrating to companies that don't think EU data protection authorities should be able to come after them, they still have to comply," Tantleff said.

Some companies have moved to eliminate or limit GDPR liability by closing themselves off from users in the EU completely, as email management service Unroll.me recently announced, or by ceasing the processing of non-EU resident's data within the bloc. Facebook most notably **took the latter step** last month, when it moved legal responsibility for the more than 1.5 billion users in places like Africa, Asia, Latin America and Australia who had signed service terms with its Irish subsidiary to the company's main headquarters in California.

However, moving data processing operations outside of Europe or leaving the EU market altogether may not be practical for most companies and could end up causing additional headaches, attorneys noted.

"Offering differential privacy and security where certain protections are offered in one location but not the other is dangerous territory," Tantleff said. "It has the potential to raise the ire of regulators, who may want to know why their citizens' data is being treated differently and their people are deemed to have less rights than those in the EU."

In getting ready for the regulation, attorneys are also encountering clients who are taking the completely opposite — and also not entirely accurate — view that the GDPR sweeps up anyone who holds any data about an EU citizen.

"From some of the commentary out there, you would think that anyone who has ever been to Europe is subject to the GDPR," Shvets said.

While the regulation's reach is broad, it is unlikely to apply to EU citizens while they are residing on U.S. soil or anywhere else in the world, attorneys say. For example, if a small bed and breakfast in Vermont that has no presence in Europe and isn't actively targeting EU tourists happens to be visited by guests from Europe, the establishment wouldn't be swept up by the GDPR just because they happen to hold data belonging to an EU citizen, Shvets noted.

"It's all about location," not citizenship, Shvets added. "If you're based in the EU, your data is protected, provided that the organization that processes it is subject to the GDPR. If you're an organization that's based in the EU, the regulation covers all data processing done in the context of the EU establishment, even for non-EU individuals."

Those Big Fines Are Automatic

The scramble to comply with the GDPR by May 25 has taken on added urgency in light of the significantly enhanced and eye-popping fining powers available to regulators, who now have the ability to levy penalties as high as €20 million or 4 percent of a company's annual worldwide revenue.

"The reason for the fines was to get everyone's attention, and I think that really worked," said Maarten Stassen, a Brussels-based senior counsel with Crowell & Moring LLP.

But just because regulators have the capability to hand down such fines doesn't mean a hefty penalty is automatic, attorneys say.

"A big myth we've been hearing is that if you breach the law, you're going to be fined 4 percent or €20 million, whichever is higher," said Venable LLP partner Shannon Yavorsky, who is based in San Francisco. "There's been a lot of fear mongering about very significant fines being imposed and people are really focused on them, but we're trying to talk clients off the cliff and reassure them that really significant fines are most likely going to be reserved for egregious breaches."

The big penalty numbers that dominate headlines are only the ceiling, not the required amount that regulators must impose for every infraction, attorneys noted. Under the GDPR, data protection authorities are instructed to take into account the nature, gravity and duration of the alleged violation and consider other ways to mitigate damages, and there's no reason to think that regulators won't take a more measured approach to enforcement, according to attorneys.

"It's true that fines can be big, but fines are just one tool in a large toolbox," said Tantleff.

The U.K.'s Information Commissioner's Office, which has been one of the most active data protection regulators in issuing guidance in the run-up to the GDPR, has indicated a preference for using the "carrot over the stick" and that fines would continue to be proportionate to the fines issued under the prior directive, Shvets said.

"If an alleged violation would have warranted a €50,000 fine under the prior directive, it's unlikely it would attract a €5 million fine under the GDPR just because maximum fines can be higher," she said. "The ICO is likely to keep its enforcement actions consistent with its prior approach."

When regulators do start to ask companies questions about potential noncompliance, attorneys recommend that they respond as transparently as possible and take steps to show that the company has been paying attention and doing work to comply with the regulation to the best of its ability.

"We think good faith will go a long way in terms of GDPR enforcement," said Jeremy Feigelson, co-chair of Debevoise's cybersecurity and data privacy practice.

Consent Is a Cure-All

Given that the regulation requires companies to be able to take steps such as furnishing copies of records or erasing data at individuals' request, companies will need to keep much more careful track of the data they hold on individuals and where it came from, attorneys noted.

"The GDPR is a compliance program," said Doron Goldstein, a Katten Muchin Rosenman LLP partner in

New York and co-head of the firm's privacy, data and cybersecurity practice. "It's not something where you can just change a privacy policy and it will work. You actually have to put programs in place and put real effort into doing that."

As part of those efforts, companies need to come up with an executable process for ensuring they have a lawful basis for processing all of the personal data that falls under the regulation's broad scope. Attorneys say that many clients are scrambling to obtain informed consent to fulfill this requirement, perpetuating **the common myth** that consent is the only legal way to process data under GDPR.

"People often want to rely on consent to process data, but consent can always be revoked," Cole said. "So it may be wise to consider the other ways under the GDPR to lawfully process personal information."

Under the GDPR, there are five other bases companies may rely on aside from consent in processing personal data. These include when processing of a consumer's data is necessary to carry out a contract or enter into an agreement with a data subject, to comply with a legal obligation, to protect the vital interests of a data subject or another person, to perform a task carried out in the public interest or in the exercise of an official authority vested in the data controller, and for the "legitimate interests" that are not outweighed by data subjects' rights.

Relying on the ability to process data such as home addresses to fulfill customers' orders and book hotel rooms is the most likely alternative to be used, although the other options may prove to be a more solid basis than consent given the circumstances, attorneys noted.

"A lot of people are struggling with the new enhanced requirement for consent and when it's valid, and don't realize there are other legal grounds," Stassen said.

In figuring out the basis for processing data, companies also need to ensure they are steering clear of the common misconception that the regulation only covers consumers' personal information, attorneys noted

"Customer data is usually the first thing companies think about when it comes to personal data," Yavorsky said. "They're often not thinking about things like employee data, other businesses' data and all the other buckets of personal data, including things like device identifiers and IP addresses that are swept up by the regulation."

Since the fines are so significant, companies would be wise to treat all the data they hold that could be used to identify a person — including hashed and pseudonymous data, which is frequently falsely assumed to fall outside the gamut of the regulation — in order to avoid running afoul of the law, Yavorsky said.

72-Hour Breach Reporting Window Is Unworkable

Along with the obligations designed to give users more control over the privacy and security of their data, the GDPR also establishes the first-ever breach reporting requirement for the bloc. Specifically, Article 33 of the regulation requires companies that hold consumer data to notify national supervisory authorities of data breaches "without undue delay and, where feasible, not later than 72 hours after having become aware of" the incident — a requirement that's sparking varying interpretations.

"There's definitely been confusion as to the timeline for that process," Goldstein said.

Some companies are being "very technical" about what it means to become aware of a breach, Cole noted, resulting in panic about how to comply with such a tight timeline. But the regulation appears to allow for some degree of reasonable discretion for companies to explore the impact of the breach, and businesses have the ability to go back and amend any disclosure, including to say that the incident turned out to be more or less significant than it had originally thought, according to attorneys.

The GDPR also separately requires companies that process personal data to notify the controller of that data "without undue delay" after becoming aware of a data breach, creating further uncertainty over how long the controller has to report the breach to the supervisory authority.

"A lot of controllers are saying that for breaches that involve processors, they don't even have 72 hours because the clock starts ticking when the processors become aware," Tantleff said. "But the time limit starts when the controller learns about the breach from the processor, and the time it takes the processor to notify the controller has no relevance."

Another common misconception around breach reporting is that companies won't be able to ever comply with the tight reporting window, given that it's far shorter than the timeline set by any of the 50 U.S. state breach reporting laws and it's hard to learn much about an incident in 72 hours.

But attorneys stressed that companies have already been successfully complying with the New York Department of Financial Services' recent groundbreaking data security regulations, which require notification within 72 hours, and that taking best practices common in the U.S. — such as conducting tabletop exercises and having draft notices ready to go — could play a big role in easing the time crunch.

"The 72-hour clock in GDPR is right in sync with the NY regulation enacted last year, and more companies are getting comfortable with the timetable operationally," Feigelson said. "Additionally, the GDPR allows for phased notification that gives companies an opportunity to come back and say more over time about what they've learned, so with that flexibility, 72 hours begins seeming less like a big deal and maybe more like the new normal."

Work Ends May 25

Companies may be feeling inclined to view the implementation deadline as a finish line and breathe a sigh of relief when it finally hits — but attorneys say not so fast.

"One myth is that GDPR compliance stops on May 25," said Jörg Hladjk, a Brussels-based attorney with Jones Day.

A primary driver behind the implementation of the regulation was to harmonize a patchwork of data protection laws that member states were allowed to enact under the previous directive. But while the regulation introduces much more uniformity, member states are still allowed to deviate from the GDPR when it comes to several important topics, such as the age that parental consent is necessary to collect data, the requirements for processing employment data and the ability to assess criminal penalties.

"Many companies think that they just have to comply with GDPR and they're set, but that's not so," Tantleff said.

Besides national laws implementing the GDPR, a first wave of enforcement activity by the data protection authorities will also require companies to continue to monitor how the regulation is being interpreted and making adjustments as necessary well after the implementation deadline has passed, Hladjk said.

Companies that may be feeling behind on their compliance efforts are likely to feel comforted by the opening to continue their work beyond May 25 — and should use the short time that remains to do what they can to show they're taking the new law seriously, attorneys say.

"It's understandable if companies are maybe feeling a bit nervous, even frantic, because the compliance deadline is almost here," Feigelson said. "But even if a company hasn't started yet, they're not necessarily in a terrible position. There's still a lot that can be done in the time that remains to begin getting companies into a compliance position and show good faith."

--Editing by Philip Shea and Breda Lund.
