Just because you don't do business directly in the EU, that doesn't mean GDPR won't impact your business. Here's what you need to know about how the EU's privacy rules could impact your business operations.
GDPR

The European Union’s General Data Protection Regulation is about to turn privacy and compliance on its head throughout the world. Even if your company doesn’t deal directly with an EU country, you still might be required to comply. Evan Schuman investigates.

Starting in May 2018, enforcement will kick in on the European Union’s General Data Protection Regulation (GDPR), a move that could have a stronger privacy/security standardization effect than any technological effort has to date. A big part of the reason for that: Although GDPR technically applies only to customers based in EU countries, globalization efforts will make GDPR compliance the smart move – and perhaps essential – for global companies wherever they are located.

Even if a company has zero customers and zero employees based in EU countries, any global efforts – such as an outsourced customer support call center in an EU country, using the services of a company for supply chain services that already is compliant, or even purchasing parts from such a company – could force compliance. That is because the company partners you seek likely will be concerned of their GDPR-compliant data commingling with your non-GDPR-compliant systems, potentially making them non-compliant and subject to fines.

“Whether or not an entity is physically located in the EU, the GDPR seeks to address all entities who process personal data on EU residents,” says Bart Willemsen, a Netherlands-based Gartner director focusing on privacy issues. “Data residency concerns, adequate protection measures and increased attention for cross-border data transfer requirements are now C-level discussion material. And if they’re not, they should be.”

For many Fortune 1000 companies, avoiding anything touching any part of Europe is going to be increasingly difficult.

“Somehow you will end up dealing with EU countries,” says Jason Remillard, who was a vice president for security architecture and CISO for Deutsche Bank until May. He recently launched a data classification company called Classidocs in Raleigh, N.C. Remillard notes that a U.S. company that engages a shipping company based in Tokyo that does business with partners in Europe will find that the Japanese company will need to be compliant as well.

Want another reason? If your company wants to purchase cyber insurance and you want protection from GDPR penalties, you had better read your policy carefully.

You likely will find insurance contract language mimicking GDPR rules. In short, if you violate GDPR rules, the insurance carrier potentially could use that as the reason for denial of GDPR fine protection.

“With these heightened [cyber insurance] fines, think about the due diligence that will come from [making this purchase],” says Aaron Tantleff, a privacy and information security lawyer at Milwaukee-based Foley & Lardner LLP.

Kevin Kalinich, global practice leader, cyber/network risk for the London-based Aon, notes that for many Fortune 1000 companies, avoiding anything touching any part of Europe is going to be increasingly difficult.

73%
Percentage of respondents who said GDPR is the most significant change in globally privacy laws in the past 20 years.

– TRUSTe
Aon insurance company, agrees. “This is a big wakeup call for organizations all over the world to analyze whether GDPR applies. What do entities need to do to have a cyber impact analysis and a readiness analysis?” he asks.

Most of the GDPR specific requirements are non-controversial and look more like a privacy best practices white paper from a Fortune 1000 company from five years ago. What makes GDPR compliance much more challenging are stringent codification requirements, along with fines that can be as much as four percent of a company’s global revenue or €20 million ($21.3 million), whichever is higher.

Although the list of personally identifiable information (PII) content is extensive – including retention of a customer’s IP address – there is an exemption if a company can establish that the prohibited data is needed for a business function and needs to be retained for a specific amount of time. That is where the codification paperwork kicks in, Kalinich explains. Everything needs to be precisely documented. That means both a quantification of how the data is being handled and why. And the European regulators are going to insist on lots of proof behind that “why.”

This requires companies to try and quantify gap analysis, among many other things, attorney Tantleff says. “These things need to be documented and done correctly,” he stresses, whereas most U.S. companies today handle these data privacy issues in an “unofficial and informal way.”

“How is data being used?,” Tantleff asks. “Detail your predictive algorithms. [EU officials] significantly now have the right to understand them. That means companies may have to disclose their proprietary information, things that they have never had to disclose before. You may have to give a lot more information, without revealing your secret sauce.”

Francoise Gilbert, an attorney specializing in data privacy with Miami-based Greenberg Traurig, adds that the intent of the new GDPR pressure is to force company executives to question their colleagues – and then to question them again – about whether retaining this data is truly worth the hassle. The EU is hoping that companies will become compliant simply by choosing to reduce what data they choose to retain.

“The more data you keep, the more exposure you have,” Gilbert says. “If you have it, you can lose it. If you have it, someone – a customer, regulator, a litigant – may ask for it and then you have to give it. That’s one good reason for not having that stuff.”

Gilbert adds that the process is intended to be onerous. “I don’t think it’s magical. They’ll ask: ‘OK, show me why this is a business need. Where is the study? Where is the analysis that you made to draw that particular conclusion?’ You have that [business need] get out of jail free card, but how did you justify that? And where does it come from? You need to provide all sorts of written documentation.”

For those who are wondering if the UK’s Brexit vote will provide a GDPR escape for anyone solely doing their European business in the UK, it won’t – and for several reasons. First, even if the UK does ultimately exit the European Union – something that is not yet certain – it will not do so until years after GDPR enforcement kicks in. Therefore, the UK will have to comply with GDPR. Second, if the UK does ultimately leave the EU, it will have to write its own rules and UK analysts fully expect those rules to mimic GDPR phrasing to make life simple for UK businesses. Third, even if the UK does leave the EU and chooses
to write its own data privacy rules that differ from GDPR, UK companies conduct such an overwhelmingly high percentage of business with customers living in other EU countries that GDPR compliance would be essential.

Brexit is an irrelevance in GDPR consideration, says James Leaton Gray, the lead consultant on privacy for London-based Kemp Little Consulting Associates. “That’s because it has such massive implications elsewhere.”

Some have asked whether EU data rule penalties could even be enforced with companies based outside the EU. Those tracking this space say that even if enforcement might prove difficult, most global U.S. companies will have few practical alternatives to paying up. And with penalties as high as four percent of global revenues, that is going to grab the attention of a lot of CFOs.

“If a U.S. company has no EU presence, it is not going to be very easy for the regulators to get the money,” says Bojana Bellamy, president of the Centre for Information Policy Leadership, a global data security think tank with headquarters in the U.S., Belgium and the UK. But, she adds, because we live in such a globally connected world, the reputational damage and anxiety companies will face end up forcing payment.

Steve Durbin, the managing director of the UK-based Information Security Forum, says compliance will ultimately be the path of least resistance. “Until we’ve had someone who has tried to do it, it’s a ‘catch me if you can’ situation,” he says. “But then there’s the impact on brand and reputation. You would not want to be seen as an organization that ignored the legislation and, when caught, refused to comply.”

One of the more problematic GDPR requirements is to inform the EU of any data breach impacting privacy within 72 hours of company executives learning of the breach. Even though the “72 hours” reference is precise, it is potentially vague phrasing about when executives learn of a breach. Does that mean the first time the CIO is told, “Boss, something looks wrong here. We’re checking to see if we might have been breached?” Or does it mean when the CIO is told: “Our logs indicate no breach, but we’re seeing clues that the logs were tampered with.”

What about when the initial forensics report indicates a problem, given that the initial forensics reports are invariably wrong?

“There’s not much clarity about when that 72-hour clock actually starts,” says Will Jan, the vice president and practice leader for Outsell, a Boston-based research and advisory service.

Adds Remillard: “The moment of breach is subjective. I guess they could have been more prescriptive.”

“It’s very difficult to pinpoint the exact point of time that you know of a breach,” says Paul Lanois, a technology attorney in Paris who served as associate professor at the University of Cergy-Pontoise in France.

**Process versus procedures**

All things considered, it probably does not matter what point in time a company chooses to start the clock as long as it is consistent and can be justified to EU officials. The person who is going to interpret the point of breach recognition is the regulator, says Kemp Little’s Gray, referring to an investigative ruling by the European Data Protection Authority (DPA).

But Gray says there are various indicators. Clearly, if law enforcement alerts you that they have discovered your data on a suspect’s server or if it starts being found in fraud...
Percentage of respondents to a European poll who said they want to be asked permission to use their personal data every time it is collected.

– Dataiq and Autograph survey

75%

GDPR

5

Percentage of respondents to a European poll who said they want to be asked permission to use their personal data every time it is collected.

– Dataiq and Autograph survey

75%

GDPR

5
why you have many merchants who were PCI compliant and then had that compliance ripped away by Visa after a breach on the rationale that PCI rules are perfect so a breach must be proof of a PCI rule violation, he says. GDPR, on the other hand, is focused on the process. As long as a company is in strict compliance with the rules, a bad result is irrelevant.

“I am slightly nervous because I fear that you end up focusing so much on process that you sometimes forget principle,” Gray says. (GDPR) might lose sight of why it’s doing what it’s doing, he adds. “It becomes a very bureaucratic system.”

Cyberinsurance conundrum

Gray, who served as the BBC’s data protection officer for 10 years, says one good thing about GDPR is that it will likely deliver far more transparency. For U.S. firms, this means that “you can’t just bury it all in terms and conditions. That won’t be accepted by the DPAs. This is a real game-changer for some first movers.”

With penalties of either two or four percent for infractions (depending, in the DPA’s opinion, on the severity of the violation), there is likely to be a marked increase in the demand for cyber insurance that will cover GDPR violations, Aon’s Kalinich says. He points out that there are three categories of insurance policies: those that offer specific affirmative coverage; those that specifically exclude regulatory costs; and those policies that are “silent with respect to regulatory costs.”

Those all come with varying costs. Executives who sometimes like to gamble opt for the policies that are silent on protections, hoping that they can later talk the insurance company into paying, he says.

The four percent exposure, he adds, forces a very serious calculation. “They must do a cost-benefit analysis that will sacrifice the total cost of risk. It’s penny wise and dollar foolish. They go for the short-run, narrow, cost-benefit analysis instead of a macro one.”

In other words, they are going to weigh the cost of exposure versus the insurance cost of coverage. That number-crunching might convince some to forgo insurance and be extra careful to comply with every GDPR provision. Others might worry that they can indeed be completely compliant and they will try and buy the insurance.

But when the company is an $80 billion multinational, that will put the cost of covering a four percent violation at approximately $3.2 billion. Some underwriters are not going to allow that or they will price the premiums so high that the coverage might not make fiscal sense, Kalinich says. “Underwriting scrutiny is going to be in-depth.”

How the cyberinsurance conundrum plays out still is unclear. Do you buy cyberinsurance, only to be told later that your violation invalidates the policy and the company will not pay, or do you pay a potentially enormous amount of money to cover a potential threat?

This component of the GDPR might well become a major sticking point of its own in years to come. Only time – and a lot of litigation – will tell.