LAST-MINUTE GDPR COMPLIANCE

It's too late to do GDPR compliance right for the May 2018 launch, but not too late to start.

ebook

An SC Media publication

Sponsored by

HID®

GDPR triage

If you haven't started preparing for GDPR, you have serious problems. With 90 days to go until implementation, you don't have time to do it right. We triage the major concerns to help you start your compliance program. Evan Schuman reports.

With the deadline for the European Union's General Data Protection Regulation (GDPR) now barely 90 days away, many CISOs are panicking. They know full well that a proper GDPR compliance program for a U.S. Fortune 1000 company can take two to three years, depending on how close they initially were to being compliant. Most European companies started out much closer to GDPR compliance as the new regulation significantly overlaps with EU rules that have been around for many years.

In the U.S., though, anxiety is the more likely state-of-mind, but it does not have to be. First off, GDPR regulators will have their hands full with European companies as the deadline passes. If those regulators opt to make an example of a U.S. company, they are most likely to focus on the well-known, low-hanging fruits such as Google, Facebook and Amazon. That said, it is not clear how much time that buys. Also, if a U.S. company is hit by a major breach, it might instantly rise to the top of the GDPR regulators' inspection list.

What to do then? SC Media asked a variety of GDPR experts what they recommend a U.S. organization do if that company has done next-to-nothing on GDPR compliance and has only 90 days left to the GDPR launch.

The good news is that there are several triage suggestions that can help. The bad news is that the experts more frequently disagree with each other rather than agree on what those suggestions should be. Those disagreements stem from the fact that GDPR has not happened yet and that there are no EU judicial decisions on which to base an interpretation. That means that there is no certainty about which provisions will be examined first, what the regulators consider to be most important and how lenient GDPR regulators will be about compliance gaps.

Privacy policy

One suggestion that almost all of the GDPR experts agreed with is to start with a GDPR-friendly reworking of a company's privacy policy. Why? Because it is a publicly-viewable document and is therefore quite likely the very first item to be inspected. Also, GDPR is all about privacy, not data security. If the privacy policy is wholly consistent with GDPR, there is a chance the regulators might move on to the next company. If that privacy policy is seriously lacking from a GDPR perspective, that could suggest to regulators "If these people aren't even promising the right things in its privacy policy, what are the chances that they are doing the right things everywhere else?" Hence, a bad privacy policy might be inviting GDPR regulators to look far more

OUR EXPERTS: GDPR

Darren Abernathy, senior global privacy manager and attorney, TrustArc

Kendall Burman, data privacy attorney, former associate White House counsel and former deputy general counsel for the U.S. Department of Commerce during the Obama administration

Chris Lippert, GDPR technical lead, Schellman & Company

Everett L. Monroe, privacy attorney, Hanson Bridgett

Hyoun Park, founder and CEO, Amalgam Insights

Paul Sonntag, product director for healthcare and privacy, Coalfire

Salvatore Stolfo, professor, Columbia University; CTO, Allure Security Technologies

Benjamin Wright, private practice attorney

GDPR

>240K

A 2014 data breach compromised the personal information of more than 247,000 Department of Homeland Security employees and other people connected with the DHS

– NextGov

closely. (Hint: You really do not want that.)

"The first thing I'd do is update my privacy policies on my web site. It's public. It's out there. It's being viewed," says Dallas-based attorney Benjamin Wright. "You want to clean that (privacy policy) up as it will be the first thing they'll likely look at."

Paul Sonntag, product director for healthcare and privacy, Coalfire

Wright adds that the privacy policy investment also plays to a psychological concern, with his argument that regulators will likely think "If you're doing that right, you're probably doing other things right as well."

Paul Sonntag, a product director for healthcare and privacy at cybersecurity consulting firm Coalfire, also says that "the privacy policy is a really good place to start as it's the means by which the organization establishes management intent."

Salvatore Stolfo, a Columbia University professor of computer science and artificial intelligence, concurs. "It's a very wise thing to do and to do it quickly." In addition to his nearly 40 years at Columbia, Stolfo last year became a co-founder and CTO of the Waltham, Mass.-based document security firm Allure Security Technology.

Former Aberdeen Group analyst, now founder and CEO of the analyst firm Amalgam Insights, Hyoun Park says the "privacy policy has to come first as it's the public version of your GDPR position. The privacy policy definitely has to match the expectations" of regulators.

Although the agreement that the privacy policy should be one of the first items dealt was widespread, it was not universal. The argument to not do the privacy policy first focuses on how bad it would look if your privacy policy gets ahead of what your systems actually do. Beyond GDPR, a company promising more than it can deliver could also get into trouble with the U.S. Federal Trade Commission, which tends to take disconnects between public promises and actual deliveries most seriously.

Wright argues, for example, that a publicly-announced data breach easily obliterates any good will earned with a well-phrased privacy policy. "What is much more likely to trigger a massive fine is a data breach. The reason is that the amount of injury to (EU) citizens is much greater under a data breach compared to failure to write the proper words into a privacy policy," Wright says.

Darren Abernathy, an attorney who serves as the senior global privacy manager with privacy compliance consulting firm TrustArc, says that he would discourage a company from making the privacy policy first on its triaged GDPR to-do list. "Certainly the privacy policy is low-hanging fruit and it's the most visible thing that (regulators) will see," Abernathy says. "But handle the data first so you can deliver."

Data Flow Mapping

Abernathy also breaks with the group in suggesting a strategy for data flow mapping. To many, data flow mapping is a long process that can barely be started in 90 days. Hence, many suggest leaving it off of the 90-day triage list. But Abernathy argues that not only should data flow mapping be managed in those 90 days, but it needs to be started before the privacy policy is written.

"To have (the privacy policy) be fully accurate, you need that data map," Abernathy says. CISOs need to create "company-wide data flow mapping and inventorying to know precisely what data is collected, from whom/where it originates—such as the EU—with whom it is shared, its nature, sensitivity and how it should be classified for storage and deletion,"

10%

At the end of 2017, only about 10% of federal agencies had met a Homeland Security deadline to properly configure the email security standard DMARC

– ValiMail

Abernathy says. (Editor's Note: Abernathy concedes that technically "inventorying" is not a word, but perhaps it should be.)

Abernathy recommends that the first GDPR triage move is to assemble representatives from all germane parts of the company including legal, engineering, marketing, procurement and the like, so that a "privacy champion" can be identified for each company unit and the mapping process can begin. "From my perspective, so much emanates from mapping. There are so many data touch points and you have to start with knowing what you collect and store. You may find that the EU data isn't that much."

The reason for the large size of the company team is so that all company data interactions can be identified and analyzed through a GDPR lens. It is critical to determine, Abernathy says, "based on a review of all data flows, contracts, and vendor/partner relationships, all of the areas where the company is a data controller versus a processor, as differing obligations may apply."

Kendall Burman, data privacy attorney

It is also important, Abernathy continues, to "clarify the legal basis under the GDPR for each purpose of personal data processing and, where data subject consent is the basis, having a scalable method for recording the date/time of each consent and the ability to withdraw consent. If, for instance, after this it becomes clear to the company that it does not act as a data controller for any EU-originating personal data, then in consultation with its legal counsel it may be able to de-prioritize" some of that data.

Another specialist arguing for data-mapping to come first is Chris Lippert, the GDPR technical lead for Schellman & Company, a security/privacy compliance assessor.

"Without a data mapping inventory being performed and updated on a real-time basis, companies won't be able to understand what data is captured on individuals and what security, privacy and compliance risks are involved therein," Lippert says. "It aids in laying the ground work for all present and future privacy considerations. That is definitely the first place to start. Companies very often have asset inventories, but don't often think of personal data captured or data in general as an asset" so the asset inventory might not be as useful as some CISOs might expect.

Data privacy attorney Kendall Burman, who served as associate White House counsel as well as deputy general counsel for the U.S. Department of Commerce during the Obama administration, agrees that data mapping needs to be an early move. "As an initial step, organizations should perform an assessment of their data processing activities, including mapping their data, in order to develop a plan for compliance that is tailored to the elements of their processing that present issues under the GDPR," Burman says. "Ignorance of one's data processing activities will be no excuse."

Analyst Park does not think a data-mapping effort for a Fortune 1000 company would get far enough in 90 days to justify placing it on the triage list. When a company has opted to ignore the imminent GDPR for years and is finally starting to focus on it 90 days before it kicks in, Park says, "you have to make bad choices at this point, quite frankly. This amounts to papering over minimum standards to have a veneer of compliance."

"The most important intermediate step is to create two sets of rapid response teams, internal (groups that can) run down quick data, who can know where data goes," Park says. "You don't have time to map it all out. You just need to have the ability to find it and make

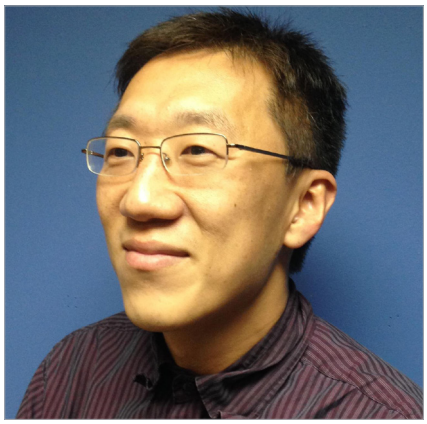
$2.8B

The global SMS firewall market is expected to grow from $1.7B to $2.8B by 2022

– ResearchandMarkets.com

fixes on the fly. There's going to be a lot of retroactive GDPRing (sic) that needs to occur."

One of the many ambiguous elements of GDPR is the extent to which data collected prior to May 2018 can be seen as grandfathered in, immune from GDPR scrutiny. "In terms of corporate responsibility, the full aspect of GDPR scope only applies to data that comes in after May 2018," Park says, quickly adding that a breach could instantly bring all of that old data back into GDPR scope. "After May, if you have a breach, you are dealing with the GDPR rules. Period."



Hyoun Park, founder and CEO, Amalgam Insights

Hence, it is not safe to ignore older data, but if something has to slide through during this emergency triage effort, it is a consideration.

"Any data brought in prior to May does have to be protected," Park says, but "there will have to be some sort of slack put in because GDPR rules are not set in stone from a technical perspective. The standards are still wishy washy, to be honest," he continues. "The parts that I would put off for later are around the ability to erase data and the ability to port data. I can always put people on it" later if individuals request to be forgotten.

Data Protection Officer

Another controversial element of GDPR triage is whether a data protection officer (DPO) needs to be appointed right away. Although there is a widespread belief that GDPR requires the appointment of a DPO, GDPR actually only requires it under specific circumstances. That said, most of the GDPR experts agree that there are few, if any, Fortune 1000 companies in the U.S. who would not need to appoint a DPO for GDPR compliance.

Here is what the GDPR says about whether a DPO is needed: "DPOs must be appointed in the case of: (a) public authorities, (b) organizations that engage in large scale systematic monitoring, or (c) organizations that engage in large scale processing of sensitive personal data. If your organization doesn't fall into one of these categories, then you do not need to appoint a DPO."

It is hard to look at even a routine customer relationship management (CRM) effort from the likes of a major department store as not engaging in large-scale processing of sensitive data, as well as large scale systematic monitoring. Without case law to specify what does and does not comply, it is wise to simply appoint a DPO. But given that nothing in the land of GDPR is simple, let us consider the implications of that DPO appointment.

The DPO typically must report to the board of directors directly and be an independent voice. That independence requirement makes it risky to simply slap the DPO title onto an existing employee, such as the chief technology officer or chief privacy officer. Doing so would raise conflict of interest issues if, for example, that CTO reports to the CIO and the CIO is pushing a data plan in concert with marketing. How can that CTO make an independent analysis if his or her direct supervisor — the one who controls their bonuses, raises and layoff recommendations — has taken a position that the DPO thinks it contrary to GDPR rules?

"The data protection officer is the new data unicorn — someone who is data-savvy, compliance focused, and public facing. It's usually hard enough to find one of those three," Park says. "The DPO role is no joke and many companies are going to mess this up by simply picking a security or GRC (governance, risk and compliance) manager who is not ready to face investor and public scrutiny."

24%

Percentage of businesses that treat preventing, preparing for and responding to risk as a strategic business priority

– 2017 Travelers Risk Index

What is arguably the most problematic aspect of the DPO appointment is that the role comes with GDPR protections against a company trying to retaliate against the DPO by firing that person or terminating their contractor agreement. That makes that person difficult, but not impossible, to fire, which is a key reason to think twice before bestowing that title on an employee who had been considered an at-will employee.

Everett L. Monroe, privacy attorney, Hanson Bridgett

In theory, that DPO could be terminated if the board concludes that the employee is a rotten DPO, in that they do not understand GDPR well. Other than that, terminating the DPO could prove quite problematic.

Everett L. Monroe, a privacy attorney with the Hanson Bridgett law firm, argues that while slapping the DPO title onto an existing employee "is certainly not brilliant," it can, in fact, work out. "Having them have other duties is not necessarily bad, but you have to make sure that they don't conflict," Monroe says.

One analogy is the role of the investor relations (IR) officer. In some companies, the CEOs and board members tend to respect — and fear — the IR officer's recommendations as they are seen as being Securities and Exchange Commission (SEC) experts. Ignore the IR recommendation and you might soon be facing an SEC investigator. In the same way that IR is viewed as representing the SEC, a DPO will be seen as representing GDPR; cross them at your own risk.

Monroe argues that a DPO needs to have two distinct areas of expertise: GDPR and your company. And it is the company expertise — knowing everything that your firm does, why and how — that is the best argument for making the DPO a fulltime employee of your company rather than a contractor or outsourced party. One might consider outsourcing the role to a law firm or consulting company and, Monroe says, "If (the company is) small enough, outsourcing may make sense."

Another DPO challenge is finding someone with the appropriate privacy expertise. "Are there suitable candidates who have the proper credentials?" asks Columbia's Stolfo, noting that every GDPR-compliant organization outside of Europe is likely right now trying to find and hire one. "In an ideal world, (hiring someone from the outside to fill the DPO role) sounds like the proper solution. I just don't think it's realistic. I don't know that there (exists) a sufficient number with the proper credentials. (Also,) are they sufficiently embedded into the company?"

Stolfo also urges companies to add third-party evaluation to their 90-day GDPR triage effort. "My greatest fear is the third-party problem," he says, adding that the responsibility for whatever privacy efforts are done by your third-party partners and supply chain" are now all on your head.

"You now have the problem of whether they are in compliance. You cannot hide behind that contract to protect yourself," Stolfo says. "Contract law now in the United States is irrelevant. You're inheriting the liability no matter what." ■

For more information about ebooks from SC Media, *please contact Stephen Lawton, special projects editor, at stephen.lawton@haymarketmedia.com.*

If your company is interested in sponsoring an ebook, please contact David Steifman, VP, publisher, at 646-638-6008, or via email at david.steifman@haymarketmedia.com.

18%

Percentage of small business owners who think they are at risk for a cyberattack

– Insureon