CSO will be ready for new European breach disclosure rules, fines

The new European General Data Protection Regulation goes into effect next May, but a year might not be enough for firms to get ready

By Maria Korolov
Contributing Writer, CSO
MAY 24, 2017 5:00 AM PT

The new European General Data Protection Regulation goes into effect next May, with onerous notification requirements and high penalties, but a year might not be enough for firms to get ready.

Recent surveys show that most companies are not prepared for the regulations. According to a recent SailPoint survey, 80 percent see GDPR as a priority, but only 25 percent have an established plan. Gartner estimates that the majority of all companies affected by GDPR will still not be in compliance at the end of 2018.

The GDPR requirements are dramatic, said Benjamin Wright, U.S. attorney and senior instructor at Bethesda, Md.-based SANS Institute. He also wrote a white paper for SANS about GDPR earlier this year.

[Related: 4 places to find cybersecurity talent in your own organization]

The general idea behind the law isn't new, he said. Europe has long had a tradition of data protection.

"However, through the GDPR, the European Union has added a great deal of detail and greater enforcement and greater expectations for data protection," he said.

In addition, companies must have a Data Protection Officer, notify authorities without 72 hours of discovering a data breach, and delete private data of customers and employees on request.

All of these pose their own unique challenges.

ion Officer, for example, is a company employee, but answers to regulators.

"In the United States, this is a very very unusual idea," Wright said. "You hire someone and that someone has an obligation to be talking to a regulator and telling a regulator what the regulator wants to know."

If a company wants to replace its Data Protection Officer, or reprimand or demote them, there will be some obstacles in the way, he added.

"They can claim that they were retaliated against because they were doing their job of cooperating with the regulators," he said. "I my experience, it's a unique challenge in employee governance in Western countries."

Who is affected?

In general, any company that has users in Europe should comply with the new regulations, including online companies with no physical presence in the region. However, some aspects of the law vary based on size of company, types of data collected, where the data is kept, and other factors.

For example, not every company needs to have a Data Protection Officer, said Wright, only larger ones -- but it's not yet exactly clear what the size cut-off is.

Breach notification and penalties

The heart of the law is the breach notification requirements. US companies are already familiar with breach notification because most states have some form of it on their books.

However, GDPR goes a lot further.

Companies are required to report a breach within 72 hours of discovering it. That means that companies have just three days to determine the scope of a breach and whether any sensitive data was lost.

For example, the breach may have been limited to intellectual property, which is damaging to the [illegible] covered by GDPR.

"We're in a situation where organizations might report a GDPR breach just to be on the safe side," said Rashmi Knowles, CTO for EMEA at Bedford, Mass.-based RSA Security Inc..

And in addition to reporting to the relevant EU authorities, the company will also need to notify all the people who were affected, she said.

This is one of the hardest things that companies are having to deal with, she said.

Failing to comply can result in a fine of 20 million Euros or 4 percent of annual global revenues, whichever is higher.

"These fines are astronomical," said Dana Simberkoff, Chief Compliance and Risk Officer at Jersey City, NJ-based AvePoint Inc. "We haven't seen anything like this."

Companies that saw fines in the millions of dollars would have had to pay billions if the breaches occurred under GDPR, she said.

In a survey AvePoint conducted last year with the Center for Information Policy Leadership, the fines were the biggest concern for executives, she said.

LINK: https://www.informationpolicycentre.com/

Companies will need to take a very serious look at the data that they're collecting and how they're protecting it, monitoring it, and deleting it when it's no longer necessary.

"What we're advising people is to look at what information you're asking for, that you actually need it, and have a business purpose for why you're asking for this information," said Mark Taylor, managing consultant at Germany-based NTT Security. "And if you don't need it, don't ask for it, don't collect it -- that's the safest way to behave."

For some firms, that might mean using more outside vendors to do the heavy lifting, use specialized data management and protection companies for whom this is their main area of expertise, or try to have their business partners take on the work.

"I definitely think that companies will do everything they can to shift liability off of themselves onto others," Simberkoff said.

lot of cloud providers are already working on getting their services certified, she said. Using a bsolve the customer of responsibility, but if the provider has a solid platform then el confident putting their data there.

"Who's going to have a bigger security team, you or them?" she said. "It's a reasoned judgment that companies will make."

Many companies will also be looking for technologies that helps them evaluate the scope of their breaches, and vendors are already rolling out products.

CSPi, for example, offers appliances that track all access to sensitive data records.

"It's like a flight data recorder," said Gary Southwell, general manager of the high performance products group at Lowell, Mass.-based CSPI Inc.

That helps companies figure out which records have been breached, and do it in time to meet the 72-hour deadline, he said.

Or take, for example, the challenge of removing private employee data on request. Employees may be keeping all kinds of sensitive information in their corporate file shares, like copies of their tax returns, telephone finance agreements, children's college applications.

That stuff has been collecting on corporate servers for years, said Linda Sharp, associate general counsel at San Jose-based ZL Technologies.

"We have technology that allows us to go through and identify all those pieces of information and help them remove it," she said.

One type of service that would be very helpful, but is currently hard to find, is comprehensive cyber insurance.

Open-Xchange, a collaboration software company based in Germany, ran into just this problem.

"We supply systems for telcos and other companies that are heavily regulated," said company CEO Rafael Laguna. "And inside those systems is this data protected by GDPR. If we don't do our job properly and the data gets exposed, our customers get fined, and they are saying, 'You screwed up, you have to pay this.'"

Before GDPR, cyberinsurance coverage might have cost in the range of $5 million, he said. "Now it's in the range of $50 to $100 million."

nd it might not even be available.

ange five months to find the insurance it needed to cover the risks associated with mer, he said.

"It took five companies to handle the requirements, and it cost us a lot of money," he said.

But, eventually, as more companies look to buy cyberinsurance, the rates might come down, said Steve Conrad, managing director at Bothell, Wash.-based MediaPro Holdings, LLC.

"Anytime you have an insurance pool and you have more people paying into it, that distributes the cost," he said.

MediaPro provides online security training to employees, and some of its customers are in Europe.

The company has cyberinsurance in place, Conrad said.

"It's becoming more and more of a requirement to doing business," he said. "And, at the end of the day, if something bad happens, you want to be covered."

Data, data everywhere

To start getting ready for GDPR, companies must first take stock of what data they collect, and where they keep it.

That could be hard for large companies, with siloed controls and multiple systems, said Ken Krupa, CTO at San Carlos, Calif.-based database company MarkLogic Corp.

Then, companies need to be able to respond quickly to compliance-related requests from regulators.

Manual processes are no longer an option, he said.

It's not just online retailers who are affected. Take eSentire Inc., a managed security services provider based in Ontario, Canada.

"We have a data center in Ireland," said Eldon Sprickerhoff, the company's founder and chief security strategist.

That means that eSentire has information related to the employees who work there. And then there's the information it handles on behalf of its customers.

"We will be considered data processors under GDPR," he said.

helping its customers get up to speed on the law, the company is also reexamining s.

"We have a great idea of where data flow, we have a great idea of consent -- we've tightened up some of the language around that," he said. "But data subjects will also be able to request to be forgotten. How we work through some of the technical aspects can be significant -- there's a lot of data that could be considered personal data. We're trying to figure out what it means."

There are also a lot of edge cases that have to be worked out, he said, which should keep lawyers very happy for a long time.

Say, for example, a company is hacked by someone in Europe. Can you collect information about the hacker without their consent? The hacker, obviously, won't bother to comply with the regulations.

"There's asymmetric adherence to the law," he said. "This is one of those things that you discuss over bar stools with a couple of scotches."

Or take the case of international companies that have a single security operations center located outside of Europe.

"If a company's SOC is located in the U.S. and they are collecting data from offices in the EU, they can well be in violation of GDPR," said Israel Barak, CISO and incident response director at Boston-based Cybereason Inc. "Does it make sense, or even realistic, for most companies to potentially build 27 separate data collection and handling practices, for each of the 27 member counties? Probably not."

Next read this:

4 places to find cybersecurity talent in your own organization

---

Maria Korolov has been covering emerging technology and emerging markets for the past 20 years.

Follow

11 sure signs you've been hacked