No DPO? Uh Oh…

By: Tighe Burke and Marty Coover

THE KEY ROLE MOST COMPANIES HAVE NO IDEA THEY ARE MISSING

If you think your company is safe from General Data Protection Regulation sanctions because it's located in the U.S.—think again.

The GDPR, enacted in May 2018, requires businesses operating in the European Union to, among other things, institute a data protection officer (DPO) to confirm certain preventative actions have been taken.

No matter where a business is headquartered—Europe, the U.S., or elsewhere—if the organization processes data from just one European Union citizen, the EU expects it to fulfill GDPR requirements, or potentially face hefty fines of up to €20 million or 4 percent of the company's annual global revenue.

Individuals can also claim compensation if a company has infringed on their GDPR-specified rights, causing them to suffer material damages such as financial or reputational loss; and companies that aren't GDPR-compatible may find they have to pay out of pocket for the expense. Insurance will only cover civil GDPR fines if an organization can prove it earnestly tried to be compliant, according to an Aon/DLA Piper report.

Still not sure if your organization needs a DPO—or how to find one? The following information can help.

WHO HAS A DPO?

More than half (52 percent) of U.S. companies were expected to be subject to GDPR, according to a survey conducted before the legislation took effect.

With the threat of data breaches becoming increasingly expensive, a number of U.S.-based organizations that aren't subject to the EU mandate are also adopting some of its stipulations—including voluntarily appointing a data protection officer.

DPO activity in the U.S. has yet to echo the role's implementation in the EU; however, Alexis Kirkman, corporate counsel and data protection officer at cloud-based email provider SendGrid, expects the position to become more prominent.

"We have not seen many DPOs in the U.S. market, with the exception of large organizations," Kirkman says. "Given the laws are going to change here—that's inevitable—and so many other countries are enacting laws, it's going to become an essential role."

So, What's the Big Deal?

Along with GDPR considerations, U.S. businesses can face other data management concerns, including recent privacy-related legislation a number of states have passed that touches on elements such as on vendor relationships, according to David Stauss, a partner specializing in privacy and data security matters at the more-than-700-attorney law firm Husch Blackwell.

A dedicated privacy professional can help organizations that operate in multiple areas track new regulations to ensure all conditions have been met.

"The U.S. is slowly moving toward dealing with privacy," Stauss says. "Now, in the absence of federal privacy legislation, you see states like California implementing their own privacy laws—which only makes the patchwork of the landscape more difficult."

California's Consumer Privacy Act of 2018 grants citizens the right to receive information about all data a business has collected about them, twice a year, at no charge, and refuse the sale of their information. Ohio also passed data protection-related legislation in 2018.

In Colorado, where Stauss resides, new data security legislation requiring entities and third-party service providers they work with to maintain reasonable security measures to protect Colorado residents' personally identifiable information in paper and electronic documents took effect in September.

Recent U.S. Privacy-Related Legislation

In 2018, a number of U.S. states passed legislation to address privacy concerns—including:

- California—The state's Consumer Privacy Act of 2018 grants citizens the right to receive information about all data a business has collected about them, twice a year, at no charge, and refuse the sale of their information.
- Ohio—The state senate passed legislation to provide a legal safe harbor to covered entities that implement a specified cybersecurity program.
- Colorado—New data security legislation requiring entities and third-party service providers they work with to maintain reasonable security measures to protect Colorado residents' personally identifiable information took effect in September.

B2B partner relationships can be another incentive for companies to strengthen privacy efforts by establishing a data privacy officer position, according to Rita Heimes, research director and in-house data protection officer for the International Association of Privacy Professionals. IAPP's governance report found 25 percent of companies shifted their supply chain processors due to GDPR.

"Let's say you use a company to host a customer relationship management database or workforce information that's used for payroll—you'd want it to have [practices] built into its systems to be compatible with GDPR [if it's] placing data for Europeans," Heimes says. "Having someone in-house at a processor whose job it is to understand GDPR is really important to controllers who sign up for that service."

Now I Know What It Is, But Who Do I Hire?

Some organizations employ one person who is solely dedicated to data privacy efforts; at others various members of a department may handle privacy-related work, or an employee performing another role may oversee it.

Kirkman, for example, divides her time between corporate counsel and data protection duties, spending about 30 percent of her time on legal work, and the remaining 70 percent analyzing how

employee, customer, and other types of data are treated and ensuring new products incorporate data privacy principles.

In Europe, whether a data privacy officer is housed inside or outside of the company, the role is generally viewed as being independent of the organization, according to Stauss.

U.S. companies, on the other hand, are more likely to have an in-house privacy professional, according to Heimes.

"That may just be culturally how U.S. companies structure themselves," she says. "They like to have a role deeply embedded in the legal or compliance department so they can walk across the hall and talk to folks."

Regardless of where they come from or where they sit, U.S. DPOs often possess some of the following skills:

- **Compliance and other oversight experience**: DPO professionals need to confirm certain protocols have been met; so previously having worked directly with or in a compliance department may be helpful. Due to the various steps involved in creating a comprehensive privacy program, project management is also a component of the job, according to Kirkman.

- **Technological know-how**: Although more privacy professionals hail from the legal sector than any other industry, tech fields rank second and third; 12 percent of privacy professionals held an information security position before assuming their current role, and 11 percent worked in IT.

  "You're going to need people, or a person, who can speak to how servers are configured and where they're located," says Erik Dullea, a partner at 700-plus-attorney law firm Husch Blackwell. "But they also need to understand information governance and data management—to have a sense of what data is being collected, retained, and for how long."

- **Operating cross-functionally**: In addition to being comfortable reporting directly to the board, to ensure data protection efforts are comprehensive, privacy professionals need to be able to work across business units and pull people together, according to Heimes.

"You cannot solve problems with one office," she says. "You have to work with IT, marketing, everybody—a whole program has to be instituted; it's not series of questions you ask someone."

WHAT'S THE CATCH?

When your organization comes to the conclusion it will benefit from hiring a DPO, finding one may not be easy—for a number of reasons, which include:

The DPO Role is Fairly New: The occupation itself didn't exist 10 years ago; according to IAPP nearly nine in 10 professionals have come into the field from another discipline, making the pool of qualified candidates somewhat small.

"Everyone wants someone who already has privacy experience—when we see ads come through IAPP, they all want 3-5 years as a minimum," Heimes says. "It's rare to find people with that kind of experience. Those people already have jobs, so there is definitely a skills gap right now, in terms of what companies are looking to hire."

The Hiring Process May Have to Center on Nontraditional Candidates: With no one discipline offering an ideal amount of preparation, employers often have to adopt a creative approach to examining the experience and skills candidates possess.

The Person You Hire May Need Some Guidance and Training: IAPP's recommendation to companies looking for DPO candidates, given the challenges involved, has been to consider either promoting someone internally who has a very solid technology background, understands the business, and is willing to learn about privacy and GDPR, or hiring someone from another discipline, Heimes says.

"The role is not so complicated you couldn't figure it out coming from an adjacent profession," she says. "There has to be appetite for hiring people who have the inherent skill set of legal analysis and communication skills."

Until a more defined DPO career trajectory becomes clear, companies will likely need to vet candidates from a variety of disciplines and potentially wildly different backgrounds to determine the best fit for their organization's privacy needs.

"It's new enough that the mousetrap may not have been built yet," Dullea says. "The role can mean you need to subscribe to new software patches, but there's a legal component, as well. It's more than just determining the cost of buying new servers and firewalls—it's really going to be a combination of strategy and risk management for the enterprise."

While the data protection officer role may be fairly new, in today's business environment, it's becoming increasingly clear that taking a proactive approach to data security is a strategic and necessary business decision.

Prospective customers or clients may not be basing today's decisions on whether or not a company has a DPO just yet. However, businesses know a widely publicized data privacy issue can affect their bottom line—which could prompt them to improve their privacy protection efforts in the future, according to Kirkman.

"Aside from the financial and legal consequences, [a breach] also has a huge PR consequence," she says. "It can have a devastating effect on your reputation. Someone who runs a business has consumers—and employees—who are becoming more aware of how their data has been used."

CONTACT INFORMATION

Tighe Burke, Partner, Cybersecurity and Technology, Jobplex

tburke@jobplex.com

Tighe Burke is a Partner in the firm's Denver office. He is currently responsible for leading recruiting, business development, search execution, client management, and candidate assessment for high potential, next-gen leaders. Tighe has deep experience working with growth-stage companies to identify their future functional leaders across the enterprise software, cybersecurity, and broader technology landscape. Having previously spent time in the company's Chicago headquarters and many years in San Francisco, his experience is truly from a national perspective. In the Bay Area, he developed valuable domain expertise executing searches on behalf of various enterprise software and other technology-based organizations. He is also a frequent speaker at various security conferences on building and retaining top-performing security teams.

Martin Coover, Partner at Jobplex

mcoover@jobplex.com

Currently in his seventh year with DHR and Jobplex, Martin specializes in the placement of executives in sales, marketing, operations, and technology functions, with a passion for software, advanced technology, industrial, and healthcare services organizations and a breadth of experience working with private equity and venture capital-backed companies. Martin serves as Partner out of the firm's Denver office.

About Jobplex

Established in 1996, Jobplex leads the recruiting industry in offering diversified search services for your company's next generation executive leader. Our customized search offerings and performance-based fee structure provide solutions from a Single Search to Project Recruitment. For more information on Jobplex, visit www.jobplex.com.