PRACTICE GROUP:
TECHNOLOGY

JUNE 19, 2018

KEEPING UP WITH GDPR AND US PRIVACY LAWS

Michael Edmonds | Vice President, Account Executive

Numerous headlines and articles warned of the impending GDPR regulations and the potential pitfalls facing companies with European Union resident data. With the May 25 implementation date in the rearview mirror, has much changed for technology companies less recognizable than Facebook or Google?

Many of the firms we speak with are still trying to understand the regulation and, more importantly, whether or not it has any direct impact on operations and the way they gather data. If a company collects personal data on people located in the EU or if a company is doing business in the EU, they are subject to the GDPR regulations. As we well know, data is king these days or, as Cloudera coined, "Data is the new bacon."

No shortage of firms have formed GDPR task forces that provide a road map to compliance. One could argue that, regardless of the direct impact, working to comply with the guidelines could prove wise and save time and resources in the future. Currently, the U.S. has numerous governmental entities playing a hand in regulating the use and protection of data, most commonly personally identifiable information (PII) or personal health information (PHI). Because of this, the task of interpreting U.S. rules around safeguarding this information may be more cumbersome and confusing than the GDPR rules, considering it is an all-encompassing law.

The right to privacy is not a new concept in the United States. Congress enacted the Privacy Act in 1974, which declared the right to privacy is a personal and fundamental right protected by the U.S. Constitution. While this act was specific to regulating government databases, it served as the foundation for future notification and security requirements on private entities collecting or processing personal data of employees, consumers, and other individuals.

Each state crafts unique guidelines and requirements in the event of a privacy breach. California has long been the poster child, and in 2003 was the first state to enact requirements for notifying individuals whose sensitive information was compromised. In the following years, 48 states, Washington D.C., and other U.S. jurisdictions have followed suit and developed notification and security requirements. Further complicating matters are the laws specific to a particular industry, such as financial services and healthcare.

continued >

The Federal Trade Commission has long served as the primary body overseeing consumer protection, and remains independent of the president's administration. Oddly enough though, the president designates the chair of the FTC and retains the ability to relieve the chair of their duties.

As risk management consultants, the sheer number of laws and entities overseeing data privacy is concerning on many levels. In my opinion, taking a similar approach to the EU and creating one body to oversee the issue would create significant efficiencies, collaboration, and peace of mind for business leaders and consumers alike. The majority of consumers enjoy the luxury and ease of utilizing the internet for shopping, sharing photos, administering finances, and so on, however consumers also need to be cautious and aware that the efficiency comes with significant exposure.

You may be asking yourself, "What is the point of all this? We all get that data security is important and there are ramifications for failing to properly care for the data you house." The point is to view the GDPR, and all that comes with it, as an opportunity to step back and take a fresh look at how you, individually or your organization, are protecting your data and that of your employees and customers.

> Too much is at stake to push this off on technology or information systems departments and trust they will get the job done.

More and more boards of directors are making a conscious effort to include this topic at every board meeting. We have presented to several boards already, and hope other clients or any company for that matter will follow suit. Too much is at stake to push this off on

technology or information systems departments and trust they will get the job done. This is not to suggest these teams don't play a vital role in data security, but the issue needs to be tackled from the board down and given proper attention and budget.

A CTO at a large firm once said, "I am doing the best I can with the budget I've been given." She was not making excuses or throwing anyone under the bus, yet it was clear that she felt more could be done with the proper resources. Human resources, I.T., finance, sales, essentially every department within an organization should collaborate and share ideas when crafting or refreshing incident response plans or business continuity plans. One of the biggest mistakes a company can make is not widely distributing the plans so that anyone in the organization can easily translate best practices in the event of a privacy issue.

From an insurance perspective, understanding the terms of your coverage and the fact that most policies were written prior to GDPR or other laws coming to life is key. If you currently have an insurance product to respond in the event of privacy breach, you should review the terms to verify that any security firm, forensic

firm, law firm, and the like is approved for use and outlined in incident response or continuity plans. Planning ahead and forging relationships with the carrier and all service providers requires an investment in time from a company and employees, however the investment will prove wise in the heat of a privacy incident. The last thing you want is to discover that invoices you receive from these providers are not eroding your deductible (i.e. will not be covered due to failing to obtain prior approval for use from the insurance carrier).

Several carriers now offer additional services for risk mitigation, such as penetration testing. In most cases, the carrier has negotiated rates with providers that are well below market. The potential negative fallout and hit to a hard earned reputation as a result of a breach is difficult to quantify, however many carriers now offer coverage for reputational damage and the financial impact resulting from the issue.

To summarize, time will tell how impactful GDPR is on middle market U.S. companies with limited exposure to citizens of the EU and their data. Common sense suggests the large, recognizable, multinational firms will be initial targets, especially when 4 percent of worldwide revenue could be at stake in the form of administrative fines for noncompliance with GDPR regulations. Most middle market firms in the U.S. likely could not absorb such a hit, and if so, it would have a material impact on future expansion or recruiting efforts in a competitive environment.

Of course, compliance does not happen overnight and without expense. Business leaders would be wise to weigh whether or not the status quo is enough to avoid potential fines, or if an investment must be made to bolster existing security, planning, and data collection and storage methods. Until the U.S. creates a single entity to oversee privacy security like GDPR, it would be prudent to talk with peers, contact an expert broker in risk management, and confirm your team comfortably understands what is and what is not covered from an insurance perspective.