advisory

THE REAL RISK OF GDPR NON-COMPLIANCE

American businesses, as a whole, are far behind their European counterparts in the extent of their compliance with GDPR, the European Union's General Data Protection Regulation. One of the most common reasons for this is also one of the most natural: it simply flies in the face of many Americans that their domestic activities might be governed by some European regulation. We did, after all, fight a war about a similar "taxation without representation" issue some 240 years ago. When GDPR's May 26, 2018 implementation date was first established, many American businesses questioned whether it would even be enforceable on this side of the Atlantic. However, the tens (if not more) of millions of dollars that are being invested in GDPR compliance by leading American companies gives a clear signal of how the smart money anticipates this question being answered.

There nonetheless remains much confusion about GDPR, including what are perhaps its two foundational questions: what does GDPR protect, and to whom does GDPR apply. As to the former, **GDPR protects "personal data:" data that, alone or in combination with other data, could be used to identify an individual.** For those vaguely familiar with HIPAA, the Health Insurance Portability and Accountability Act of 1996, think HIPAA – only across every conceivable category of personal information gathered or processed about any type of person: customer, employee, student, patient, survey respondent, website visitor, etc. For those intimately familiar with HIPAA who just read the previous sentence, feel free to pause until your pulse and blood pressure return to a normal range.

As to the latter foundational question, **GDPR applies to "data subjects" "in the [European] Union," "whatever their nationality or residence."** GDPR isn't limited to European citizens or European residents, as is often erroneously stated. If a person is in the European Union (which is presently interpreted to include the United Kingdom, despite the ongoing uncertainty known as Brexit) when their data is collected, that data is protected by GDPR. By the way, Europe's base population is 741 million, before even adding in the many additional millions of tourists, students, migrant workers, refugees, and so on roaming its hills and history-filled streets on any given day. That means that internet-based businesses that sell goods or services more than infrequently to European-based customers are subject to GDPR. It means that data collected by an American university on a student while she studies at the Prado in Madrid for a semester is subject to GDPR. It means that American hospitals that obtain data from patients or potential patients in Europe are subject to GDPR. And that includes even the internet "cookies" related to those potential European patients that the hospital's website collects.

However, even among those who recognize that GDPR does apply to American businesses, there remains a wide variety of both understanding and preparation. One of the primary reasons for this is entirely rational: of all the legal and regulatory risks haunting a business every day, a newly-enacted European privacy regime ranks pretty low on the Enterprise Risk Management matrix. Yes, business leaders are aware that the Supervisory Authorities enforcing GDPR can impose fines up to €20 million (about $24 million) or four percent of revenues, whichever is greater. Yes, this dwarfs HIPAA's $1.5 million fine structure; yes, it could put any mid-sized company out of business; and yes, it is reasonable to expect that United States courts will, fairly soon, start enforcing fines issued by GDPR Supervisory Authorities. But if you're a mid-sized biotech in Raleigh, or a data management platform in Boston, should you really lie awake at night in fear of a Notice of Violation from some Supervisory Authority in Germany? Probably not.

Private Right of Action Provision

Your much greater threat is the private right of action that GDPR creates. Unlike HIPAA, which has no private right of action, GDPR gives covered individuals the right to sue for "material and non-material damages." The non-material damages provision should not be taken lightly. From the rise of the National Socialists in the 1930s through the fall of Communism in the late 1980s, many Europeans suffered greatly as a result of the oppression made possible by the collection and misuse of their personal data. Judging from the public support of GDPR, they do not seem to be in the mood to tolerate misuse of their data today merely because the offending entity is now a corporation rather than the state. Thus, a business leader should expect the term "non-material damages" to be code for "whatever punishment a European court decides your business deserves."

Anyone who has been following global events is well aware that the Europeans are less than enamored of the United States at the moment. "Non-material damages" should be read to mean an amount that makes headlines, especially if an American company is involved.

Further, GDPR gives nonprofit organizations the right to stand in the shoes of affected individuals and sue on their behalf. This is not some theoretical risk: nonprofits are being organized now for this very purpose. While some, like the European Center for Digital Rights, founded by the Austrian lawyer Max Schrems renowned for his privacy battles with Facebook, may indeed have altruistic motives, not all will.

Many opportunistic lawyers, either acting through nonprofit groups or directly on behalf of affected individuals, will begin bringing suit for a much older and more reliable reason: making a buck. Or a Euro. Or as many of both as possible.

Further, the early targets of this opportunism will likely not be the marquee corporate names of Zurich, Paris and Rome, but rather those small and mid-sized firms whose GDPR compliance is less than complete. Further, the most attractive targets of opportunity may very well be American. The reason for this is simple. It is much easier for a European company to fight a GDPR action in its own jurisdiction. Similarly, the corporate titans of New York and Silicon Valley have the resources to fight GDPR lawsuits in European jurisdictions. They will defend lawsuits even when the cost of defense far exceeds the damages demanded, just to keep unfavorable legal precedent from being established in some low-profile jurisdiction in Moldova or Estonia that might later cost them dearly in London or Stockholm.

Thus, it may well be that the sweet spot of GDPR lawsuits will be small and mid-sized American businesses: those with deep enough pockets to pay out five- and low-six-digit nuisance awards, but who would not spend the money needed to defend such suits in a European jurisdiction. Unfortunately, this creates a viable business model for opportunistic lawyers on both sides of the Atlantic. Identify hospitals, colleges, biotechs, online vendors, nonprofit advocacy groups, and various other entities who collect or process the data of persons in Europe, send a demand for an accounting or amendment or deletion, and when it isn't responded to timely and properly, file suit in a remote province of Belarus. Once a judgment is obtained, forward it to the American law firm working as your business partner and have them enforce it.

Reading this for the first time, such a scenario may seem far-fetched. Then again, it was just a short time ago when it seemed equally far-fetched that some hacker from Eastern Europe would file a phony income tax return under your name and make off with a refund. Or that he might use your data to take out a second mortgage and wipe out all the equity in your home. Or that he might use ads on Facebook to influence an American presidential election.

GDPR presents a risk to any American business that collects or processes data on individuals in the European Union. And the businesses to which it ironically poses the greatest risk are those who are doing the least to prepare for it. The good news is that it is never too late to start.

Joel K. Goloskie

Senior Counsel

Joel K. Goloskie is Senior Counsel with Pannone Lopes Devereaux & O'Gara LLC and a member of the Health Care, Litigation, Cyber Law and Corporate & Business Teams. His experience ranges from compliance and HIPAA privacy matters to regulatory filings and approvals, contract drafting and management, and mergers and acquisitions. He has assisted health care clients as they dealt with compliance orders and deferred prosecution agreements, and has represented clients in both civil and criminal matters in federal court.

PANNONE LOPES DEVEREAUX & O'GARA LLC

counselors at law