How the European Union's Newly-Active GDPR May Affect Your North Carolina Business

BLOG | JUNE 18, 2018

Like me, you may have been the recipient of a recent onslaught of emails from businesses ranging from Amazon to Zillow notifying you of updates to their privacy policies. By and large, these updates have been prompted by the European Union's "General Data Protection Regulation," more commonly referred to as the GDPR, which was enacted in 2016 and became effective on May 25, 2018. GDPR represents the most comprehensive and exacting regulation of corporate handling of consumer personal data ever enacted by a governmental body. As evinced by the spate of updates you have no doubt received, GDPR will likely shape global business because of its strict requirements, harsh and potentially debilitating penalties, and ability to reach outside of continental Europe to enforce its protections.

While lengthy and complicated, GDPR essentially has two categories of major requirements for collecting and storing personal data. These requirements apply to all "data processors" – any entity, including businesses, non-profits, people, public authority, or agency that collects, stores, or otherwise works with individuals personal data. These categories are boiled down for simplicity, so do not take these summaries as a complete summation of a business' obligations under the GDPR.

Securing personal identifying data that you have collected from any breach.GDPR requires that businesses and other "processors" collecting personal data use appropriate technical and organizational measures to protect personal data from loss, alteration, and unauthorized disclosure or access. What is an "appropriate" measure depends upon the risks involved in the disclosure of the information – in other words, if the consequences to the end user are greater, "appropriate" security measures will involve greater protections. GDPR makes the business collecting the data accountable for any breach of data – including data you share with or receive from third parties. Businesses must notify authorities of a data breach within 72 hours and must notify users "without undue delay." Entities collecting personal data must also routinely assess the impact of a data breach or loss on people from whom it has collected data. Companies with large-scale or regular data collection operations and those that process personal data as a core corporate activity also must appoint a data protection officer to provide guidance on securing data and ensuring that GDPR requirements are met.

Overhauling privacy and data-collection policies. This is the prong that has received the most attention because it is public-facing. Under the new law, a business must state to its customers and users the specific types of personal data that it is collecting from them and the purposes for which the data is being collected. The reasons that a company may collect personal data are designated under the regulation, and companies are only allowed to collect data necessary to achieve the reasons they give for collecting it. You must receive explicit, affirmative consent from the user to collect the

data, and the consent must be revocable at any time in the same manner in which it was given. A company must put this information in a plain and understandable form – hidden policies stuffed full of legal jargon are no longer sufficient. Further, under GDPR users have numerous rights with the data that is collected from them, including the rights to access their data, delete data, and correct inaccurate personal information.

One important note is that GDPR defines "personal data" in a significantly broader manner than generally accepted in the United States. There is no catchall data protection law in the United States. Instead, there are piecemeal statutes that protect data in certain situations, such as the Health Insurance Portability and Accountability Act ("HIPAA"), which, among other things, establishes privacy rules for private persons' medical data. Generally, however, accepted United States standards protect "personally identifiable information," such as a person's social security number, birth date, driver's license number, and other sensitive personal information that can be used for identity theft.

GDPR, by contrast, protects a much broader scope of data. The regulation defines "personal data" as any information that could be used to identify a person. That definition provides much more protection to private citizens, protecting a business from collecting data such as their name, address, email address, photos, social media posts, IP address information, and more. If any information that a business collects might be used to identify an individual, that business must comply with GDPR's requirements.

GDPR allows people who have suffered "material or non-material damage" as a result of violations of the regulations to receive compensation from the organization that engaged in the violation. GDPR also authorizes fines and up to €20 million or 4% of global sales, whichever is greater.

GDPR allows people who have suffered "material or non-material damage" as a result of violations of the regulations to receive compensation from the organization that engaged in the violation (translation: customers may sue businesses who violate the regulations and receive compensation). As mentioned above, any organization involved in the violation is liable for the damage caused by its failure to adhere to the regulations; a business may only escape liability where it shows that it "is not in any way responsible for the damage." Thus, it is in any company's interest to ensure that its partners and entities in which it shares data are compliant with GDPR.

The real hammer that GDPR brings is administrative fines for violations of its strictures. GDPR authorizes fines of up to €20 million of 4% of global sales (not profits), whichever is *higher*. EU regulators have indicated that they plan to seek

the highest-available penalties that the law authorizes. Obviously, these types of fines have the potential to put some of the best-known worldwide companies into serious financial trouble.

How might this new regulation affect a small business primarily operating here in North Carolina?

In a variety of ways. First, the regulation applies extra-territorially, allowing EU residents doing business outside of Europe the same protections as they would in wholly intra-continental dealings. Thus, if one of your customers is an EU resident, you risk running afoul of European regulators if your data collection and protection policies fail to adhere to what is dictated by GDPR. While the full scope of GDPR's extraterritorial application has not been litigated, it uses very broad language in applying its rules to businesses with European customers.

Second, if you regularly work with businesses with a significant European footprint, your company may soon be asked to verify its compliance with GDPR in order to receive any type of personal data in order to limit the partner's liability risks. GDPR's enhanced penalties will make companies less willing to share data where there is doubt about the recipient's data protection policies and whether they comply with GDPR's rules.

Finally, and most relevantly, GDPR is likely the direction that the law is heading on this side of the Atlantic. You may have followed Facebook CEO Mark Zuckerberg's testimony before Congress in the wake of the Cambridge Analytica scandal with interest, but Facebook is hardly the first corporate giant facing a data breach issue. Even companies outside of the tech sector have been plagued by data breaches in recent years, including Equifax, Target, and Under Armour. While it may be years before an omnibus data protection bill passes both houses of Congress and is signed into law, Congress' demand for answers from Zuckerberg indicates that there is newfound interest in data protection among our lawmakers. As Americans elect younger and more tech-familiar lawmakers and data breach scandals continue to disrupt security, it is only a matter of time before some similar protections are enacted here.

About the Author

Robert D. Whitney is a member of Young Moore's litigation team. His practice focuses on business litigation, insurance coverage analysis, coverage disputes, and insurance bad faith litigation. He earned undergraduate degrees in Business Administration and Political Science from the University of North Carolina at Chapel Hill and is a *cum laude* graduate of Duke University School of Law. Robert is licensed to practice in North Carolina and California. Contact Robert at (919) 861-5072 or Robert.Whitney@youngmoorelaw.com.
