ARE Privacy Law Alert: The GDPR Is Two Years Old: What You Need to Know

Author(s): Douglas A. Miro, David P. Goldberg, and Herbert Blassengale IV*

(June 11, 2020) On May 25, 2020, the European Union's General Data Protection Regulation (GDPR) celebrated its second anniversary. This law sets out the ground rules for data protection and privacy for people and companies living, working, or doing business in European Union (EU) countries. Because its reach goes far beyond EU member state borders, it is important to understand how the GDPR is now being interpreted and enforced.

Two years ago, many organizations were worried that the GDPR would fundamentally change the way they do business. There were early fears of crippling administrative costs and of large penalties for violations—especially because GDPR violations could lead to fines of 20 million euros or up to 4% of a company's annual revenue. However, following two years without significant punitive action for GDPR violations, especially in regard to American companies, the prevailing question now is whether these fears were warranted.

How the GDPR Is Being Enforced

Although the EU may not be home base to tech industry giants, it is one of the world's wealthiest markets. By stepping in early and decisively with the enactment in 2018 of the GDPR, the EU significantly boosted its regulatory presence in the high tech sphere, and effectively set the worldwide floor for data protection and privacy regulation.

Though the GDPR sets some strict standards regarding what is expected of businesses operating in the digital space, it also has had salutary effects. For instance, under the GDPR, employers are required to provide their staff with training on data protection and basic cyber security. This requirement encourages a more data-conscious and socially informed culture, and helps protect the privacy of millions of people worldwide.

Despite the generally smooth implementation of the GDPR, its enforcment has raised some unexpected issues. Under the GDPR, each EU member state has its own data regulation authority, which is charged with enforcing the GDPR within its borders. Because of this arrangement and a rule that directs complaints to the country where a company's European headquarters are based, Ireland's Data Protection Commission ("DPC") has become responsible for handling many technology giants, which are drawn to Ireland for its attractive tax incentive initiatives. With eight investigations into Facebook, three into Twitter, two into Apple, two into Whatsapp and two into Google, the DPC, a releatively small organization with a limited budget of only 16.9 million euros, risks being overextended.

On the other end of the spectrum, the United Kingdom has had roughly 22 thousand data breaches reported since the regulation was introduced. However, its Information Commission Office,the highest funded GDPR enforcement authority with a 61 million euro budget, has sought only one fine—a 275 pound fine against a London-based pharmacy for "careless storage."

This inequity of workload and allocation of resources among the EU's data protection authorities has led to a situation where there have been few significant punitive actions for GDPR violations. This fact is now gaining attention in the popular press, and we expect it may result in some adjustments in the future. We also expect that the DPC will be under increased pressure to complete its investigations, which may have significant results. Despite the challenges in GDPR enforcement, the potential for a consequential impact on business is still there.

While many non-European states are content to rely on the GDPR's de facto worldwide data protection and privacy scheme, perhaps unsurprisingly, the GDPR has inspired other states outside the EU to draft their own data privacy legislation.

For instance, India's Personal Data Protection Bill of 2019, which is similar to the GDPR but adds special governmental data access rights, regulates the sharing and processing of personal data in India. Brazil's Lei Geral de Proteção de Dados (LGPD) harmonizes more than 40 different statutes currently governing personal data in that country. Like the GDPR, the LGPD applies to any business or organization that processes personal data of people in Brazil, regardless of where that business or organization itself may be located, broadening the scope of those entities which must comply. How stringently such laws will be enforced, especially controversial clauses requiring governmental access rights, is yet to be seen.

Practical Effect

The imposition of fines may turn heads, but the requirement for companies to change their behavior may be the most effective outcome of the GDPR. And while there have only been two significant fines imposed on US companies under the GDPR thus far, the prospects for further action looms on the horizon.

Even though the GDPR is European, any company conducting business that may involve EU consumers must become more conscious of their data protection efforts, while simultaneously finding ways to best adapt and comply with the ever-changing digital landscape. With global digital integration making our world a smaller place every day, businesses must be vigilant in order to remain compliant with the ever-growing requirements of the international data protection regimes.

* Douglas A. Miro *is a partner,* David P. Goldberg *is an associate, and Herbert Blassengale IV is a law clerk at Amster, Rothstein & Ebenstein LLP. Their practice specializes in all aspects of intellectual property law, including privacy law. They can be reached at* dmiro@arelaw.com, dgoldberg@arelaw.com

, and hblassengale@arelaw.com*.*