Published on *The National Law Review* https://natlawreview.com

The EU's General Data Protection Regulation (GDPR)

Article By:

IMS Legal Strategies

The General Data Protection Regulation (a.k.a. the GDPR) is a regulation issued by the European Union (EU) that became effective as of May 25, 2018. It is intended to provide protection to citizens of the EU with regard to the processing and free movement of personal data.[1]

Because it is a regulation and not a directive, it is binding on all 28 EU member states. The GDPR requires that every company that offers products or services to EU residents within the various EU states comply with a strict set of data privacy and security measures.[2] Therefore, it extends beyond the EU to all companies who process and store personal data of EU citizens, whether such companies have locations in the EU or not.

The regulation is enforceable through the EU's Data Protection Authority, also known as the Supervisory Authority. As we shall see, the Regulation can and has also been enforced through local enforcement authorities of the member states.

The GDPR is voluminous, containing 11 Chapters and 99 "Articles." There are several noteworthy provisions of the Regulation, 3 of which are set forth below:

- First, Article 10 provides for criminal prosecution of individual D&O's for deliberate breaches. Therefore, corporate officers and members of corporate boards of directors can possibly be jailed.

- Second, Article 33(1) requires mandatory notification to the Supervisory Authority within 72 hours from when a company has become aware that a breach has occurred.

- Third, Article 83(5) provides penalties for violation of the regulations including fines of up to € 20 million, or 4% of the offending company's global annual revenues, whichever is higher.

In light of these regulatory provisions, U.S. corporations and their directors and officers must now keep track of whether they are compliant with the GDPR, as well as being compliant with their own domestic laws.

Notwithstanding the harsh measures imposed by this Regulation, and its extraterritorial applicability, as late as 6 months after the inception of the GDPR, many U.S. companies were either unaware of

its significance or failed to take prophylactic measures to avoid its impact. According to an article published in the Professional Liability Underwriting Society (PLUS) Journal, just weeks before the implementation of the GDPR, only 60% of U.S. companies had plans in place to respond to the demands of this regulation, of which 94% possessed customer data for citizens of the EU.[3] Moreover, of 1000 small business owners polled, over half of those questioned indicated that they were confused or "clueless" by the rules.[4]

However, the GDPR has already had a profound impact on U.S corporations and companies around the world. In fact, since the GDPR first went into effect, more than 42,000 complaints were filed against companies for breaches of the GDPR.[5] Since late 2018, and the beginning of 2019, there have been reports of penalties asserted against major data processing companies for violations of the GDPR. For example, on or about January 20, 2019, the French regulatory authority CNIL announced that it had levied a € 50 million (U.S. $57.2 million) fine against Google for "lack of transparency, inadequate information and lack of valid consent ads personalizations."[6] Previously, the Italian competition regulator fined Facebook € 10 million (U.S. $11.44 million) for misleading its own users over data practices.[7] Further, The Irish Data Protection Commission launched an investigation of Twitter, and The Dutch Authorities commissioned a General Data Protection impact assessment of Microsoft, concerning the use of Microsoft Office 2018.[8]

Although it appears that the European regulators are currently targeting the large multinational internet companies such as Google, Facebook, Twitter, and Microsoft, eventually the regulators will begin to look at smaller companies and companies that don't have locations in Europe. Therefore, it is prudent that such companies make conscientious efforts to ensure that they have proper and effective controls in place, particularly to ensure that they operate with the informed consent of their customer/client base.

As to the issue of directors and officers liability, it is unclear—but unlikely that fines assessed against directors and officers would be covered losses under a D&O policy. Local national and state laws would typically govern that issue. More significantly, director and officer liability may be triggered through the filing of derivative and securities class actions, where there are significant stock drops due to announced penalty payments. Derivative actions filed by corporate shareholders on behalf of the company to redress corporate losses, due to mismanagement, may be especially problematic if shareholders can establish that corporate boards should have been aware of the impact of the GDPR and failed to take reasonable remedial action in advance to avoid the regulatory fines. The issue of corporate and D&O liability arising out of the failure to protect data privacy of its customers will not be restricted to the European Union. In fact the California Consumer Privacy Act passed this past summer has protections that parallel the GDPR. California may be the first in a long line of states providing protection to its residents from corporations that fail to protect the process and free movement of personal data. Stay tuned, this may well be the start of a very bumpy ride for corporations and their D&O's.

_____

[1] Chapter 1, Article 1 GDPR

[2] Chapter 1, Article 3 GDPR

[3] "*Directors Beware: The EU's General Data Protection Regulation in Upon Us," 2018* PLUS Journal, 2nd Quarter, *By Keith Daniels, Jr.*

[4] “GDPR: Small business owners still ‘Clueless’ about data protection rules, study claims,” The (UK) Independent, reported in Advisen FPN. December 12, 2018.

[5] “The Impact of GDPR on D&O Liability Claims,” By Peter Wedge, presented at the Crowell & Moring 2019 D&O Symposium Event, “Directors and Officers Insurance An International Perspective,” February 5, 2019.

[6] “Google hit with GBP 44 m GDPR fine over ads,” CNR, by Chris Fox, January 21, 2019

[7] “Google fined record GBP 44 m by French data protection watchdog,” Guardian Web, reported in Advisen FPN, January 21, 2019

[8] “EU takes a stand on data protection with Google fine,” Business Insurance, by Gloria Gonzalez, Business, January 29, 2019

National Law Review, Volume IX, Number 67