THE REVIEW OF
SECURITIES & COMMODITIES REGULATION
AN ANALYSIS OF CURRENT LAWS AND REGULATIONS AFFECTING THE SECURITIES AND FUTURES INDUSTRIES

Vol. 51 No. 14 August 15, 2018

EU GENERAL DATA PROTECTION REGULATION: IS THE U.S. FUNDS INDUSTRY READY?

Businesses in the U.S. funds industry that target European investors are now subject to the GDPR. The regulation can apply even if the fund's structure is located outside the EU and personal data are stored outside the EU. The author discusses GDPR's coverage and requirements, and lays out a series of "next steps" for businesses to address compliance.

By Gretchen Scott *

May 25, 2018, was GDPR day. After two years of preparation, the EU General Data Protection Regulation 2016/679[1] ("GDPR") is now enforceable across the member states of the European Union. The GDPR governs the processing of personal data by controllers and processors established in the European Union and, in recognition of the cross-border nature of data flows in the age of borderless business and technology, also applies to controllers and processors based outside the EU in certain circumstances. It has introduced enhanced obligations on controllers and new obligations on processors, whilst establishing new rights for individuals with respect to their personal data.

Every business within the funds industry ecosystem that targets European investors or handles personal data of European investors – including fund vehicles, investment managers, general partners, transfer agents, trustees, custodians, depositaries, and administrators – needs to appreciate the impact of the GDPR on their respective businesses.

The GDPR introduces a competition-like sanction regime with potential fines for violation of core data protection requirements (including processing without valid consent, breach of individuals' rights, or unlawful data transfers) of up to the higher of 20 million euros or 4% of global annual revenues, or up to the higher of 10 million euros or 2% of global annual revenues for violations regarding notification of data breaches, data processor terms, and other requirements.[2] The data protection authorities have been keen to emphasize that fines are not the only enforcement weapon available to them in their arsenal; however, fines are likely to remain the most practical enforcement option for the authorities when dealing with a non-compliant U.S.-based business. Data subjects are more aware than ever of their individual rights. Moreover, the GDPR introduces the right for non-profit organizations to bring claims on

[1] General Data Protection Regulation (EU) 2016/679 (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG). (references hereinafter to articles are to the GDPR).

[2] Article 83.

* *GRETCHEN SCOTT is a partner at Goodwin in London and is a member of their Privacy and Cybersecurity team. Her e-mail address is gscott@goodwinlaw.com.*