

INVESTMENT MANAGEMENT AND PRIVACY & CYBERSECURITY UPDATE



THIS UPDATE IS PART OF A SERIES from a working group of investment management and privacy & cybersecurity attorneys. We look forward to sharing more insights on privacy & cybersecurity trends and developments of concern to the investment management industry.

GDPR AND THE FUNDS INDUSTRY

WITH THE PUBLICITY surrounding the May 25, 2018 implementation of the European Union's (EU's) General Data Protection Regulation (GDPR), many United States-based registered funds and advisers are continuing to ask whether and how the GDPR will apply to them. Investors and clients are also asking about GDPR compliance. GDPR is a comprehensive data protection regime governing the "processing" of personal data, including collecting, storing, using, or performing any operation on the personal data. For funds or advisers that are established in Europe—for example, if they have European subsidiaries or if an adviser has an office or an affiliate in the EU—the GDPR will apply to the processing activities of those establishments as well as the processing activities (if any) of the US-based fund or adviser insofar as they are linked to the activities of those establishments. Even for funds and advisers that do not have subsidiaries or establishments in Europe, though, the GDPR could still apply in some circumstances. With the potential for significant fines, funds and advisers should carefully review their operations to determine whether the GDPR applies to their activities.

ONE OF THE EXPRESS AIMS of the GDPR is to broaden the territorial scope of the European privacy regime. Processing activities of even non-EU-established funds and advisers are covered if the fund or adviser (1) offers goods and services to individuals in the EU or (2) monitors the behavior of EU-located individuals. It is important to note that the citizenship of the data subject does not matter—the GDPR will apply even if the subject is not European, provided the above criteria

are met. At the same time, the GDPR only applies to processing data of a "natural person." Data relating to institutional investors is not covered (though information relating to their employees or individual plan participants may be).

FOR FUNDS AND ADVISERS without an establishment in the EU, the "offering goods or services" prong is the most likely to apply based on the offering of investment opportunities to EU investors or offering advisory services to EU clients. Even if the fund or adviser has *some* European investors or clients, however, that fact alone may not be sufficient to bring GDPR into scope. The fund or adviser must "offer" its goods or services (i.e., investment opportunities) in a way that suggests it "envisaged" (i.e., anticipated) providing such goods or services specifically to individuals in the EU. In other words, the fund or adviser must target investors in the EU in some way, rather than, in the case of a fund, offering its investments passively to the general public, or, in the case of an adviser, accepting an EU-located individual as a client after being contacted by such individual. Since most US-registered funds do not actively solicit European investors, they are likely to fall outside of the GDPR's scope on the "offering goods or services" prong. Likewise, an adviser may have some EU clients without necessarily having the GDPR apply. Additionally, if the fund or adviser could be viewed as targeting only *institutional* investors or clients that are EU-located, it remains an open question whether such activities would fall within the GDPR's scope, as the law anticipates offering goods or services to "data subjects," i.e., actual people.

A USEFUL COMPARISON is web-retailing, which is discussed in the GDPR's recitals. In that context, the recitals explain, the mere fact that users from the EU *could* access and thus purchase from a website does not trigger the application of the GDPR. For GDPR to apply, the website must be somehow directed towards EU individuals, for instance, through the use of a local language, by allowing users to pay in Euros, or by featuring profiles of EU users. For the

funds industry, many activities could likewise be deemed to target EU investors in a way that “envisages” offering goods or services to them. Such activities could include conducting roadshows in the EU, periodically meeting with EU-based investors, or using promotional materials that are obviously directed at European investors such as by translating them into French or German or by featuring profiles of Europeans. It is important to note that GDPR’s scope provisions are highly fact-specific, and so any single factor may not be dispositive. In evaluating whether they are covered, funds and advisers may wish to leverage any review they have conducted under the Alternative Investment Fund Managers Directive’s reverse solicitation exception, which requires an assessment of similar, though not identical, factors.

THE SECOND PRIMARY way that the GDPR may apply to funds and advisers without EU establishments is if they are “monitoring” the behavior of an individual in the EU, typically, but not always, online. Only “natural persons” are protected, so tracking a company’s performance would not be covered. However, unlike with the “offering goods and services” prong, the fund or adviser does not need to target EU individuals specifically. If any EU individual is monitored, those activities would be within the GDPR’s scope whether or not that was the fund or adviser’s intent. “Monitoring” the behavior of a subject means more than simply collecting data, though. The data must be collected in order to track the individual, in particular, if the tracking is done to create a profile used to predict future behavior. Funds and advisers that access data that includes personal information about EU residents should assess whether such activities could constitute monitoring within the meaning of GDPR. For example, to the extent that US-registered funds begin engaging in direct lending or similar activities to EU-resident individuals, this may be an example of a situation where a fund or its service provider’s activities in connection

with those loans could give rise to monitoring subject to the GDPR. Similarly, a robo-adviser that collects data of EU-resident clients also might be viewed as engaging in monitoring activities subject to the GDPR. With respect to both of the prongs discussed, regulators will likely take an expansive view of the GDPR’s application.

EVEN IF THE FUND OR ADVISER does not offer goods or services or monitor the behavior of individuals in the EU, it may still need to comply with the GDPR based on other relationships. If an adviser’s parent company is established in the EU, for example, the adviser may have compliance obligations due to that affiliation. An adviser who has “access persons” located in the EU who are required to provide information to the adviser for code of ethics compliance purposes could find that this activity is subject to the GDPR. European investors or clients may also ask the fund or adviser to comply with certain GDPR provisions. Institutional investors established in the EU that share personal data for anti-money laundering or other purposes may require funds or advisers to enter into standard contractual clauses to legitimize the data transfer under GDPR’s international transfer provisions. Other investors may take a conservative approach regarding the GDPR’s territorial scope and seek to impose compliance whether or not the fund or adviser believes that it fits within the GDPR’s scope. In responding to these requests, firms should evaluate what data they are likely to collect and the burden of any compliance program.

GDPR CAME INTO EFFECT on May 25, 2018. Given the burden of GDPR compliance, many US-registered funds and advisers without obvious EU connections have taken a wait and see approach to determining whether they are potentially within GDPR’s scope. For those entities, we recommend actively monitoring enforcement for insight on how the GDPR is applied to the funds industry in practice.

CONTACTS



Paulita Pike
Partner, Chicago
Investment Management
paulita.pike@ropesgray.com
+1 312 845 1212



Elizabeth Reza
Partner, Boston
Investment Management
elizabeth.reza@ropesgray.com
+1 617 951 7919



Heather Sussman
Partner, Boston
Privacy & Cybersecurity
heather.sussman@ropesgray.com
+1 617 951 7125



Kevin Angle
Counsel, Boston
Privacy & Cybersecurity
kevin.angle@ropesgray.com
+1 617 951 7428