BRACEWELL

INSIGHTS

EU Data Privacy Law Countdown – Who's Ready?

May 14, 2018

On May 25, 2018, the European Union's data privacy regime is getting an upgrade (the General Data Protection Regulation, or GDPR) to improve individual protections. It will also, however, raise various new operations concerns. The organizations that plan ahead for life under the new regime will be best positioned to identify errors, make adjustments and ultimately have a better GDPR compliance record going forward. Private funds based outside the EU should take heed because the GDPR likely will apply to some portion of your data, too.

At its most basic, the GDPR governs the protection of processing and moving of personal data associated with natural persons in the EU (such as investors, customer, or employees). Perhaps the biggest change implemented by the GDPR is that it can apply equally to non-EU companies with no direct operations in the EU. As a result, non-EU companies that offer products or services to natural persons in the EU are expected (by the Independent Supervisory Authorities identified by the GDPR) to develop a GDPR compliance program. Other key new components required by the GDPR include explicit data breach notification requirements and steep penalties associated with non-compliance. In the event of a data breach, companies are required to notify their designated Independent Supervisory Authority within 72 hours. For U.S.-based funds, this obligation could be in addition to other relevant state and federal notice requirements.

The GDPR also more thoroughly addresses the mechanics and realities of modern data processing, use and storage (expanding the earlier EU Data Protection Directive). The GDPR covers matters related to the types of personal data being collected, uses of the data, the location of data processing, underlying basis for processing, and modifications to the data; all of which must be addressed as part of any GDPR program. The need for a transfer mechanism to transfer personal data from the EU to a third country is still required and the GDPR expands upon the options available that ensure an adequate level of protection. Any compliance program requires appropriate technical and organizational measures to ensure data privacy protection.

For U.S.-based private funds that are adjusting their data privacy programs to meet GDPR requirements, there is considerable guidance available to aid GDPR compliance integration into a pre-existing compliance program. Companies adopting GDPR should emphasize, within their organizations, the expectation of individual responsibility for compliance, throughout all levels

of the company. For example, senior leaders should be educated about new GDPR-based privacy expectations and should be encouraged to speak out in favor of compliance. Companies should also assess what ongoing steps can be taken to demonstrate a commitment to compliance with GDPR, including documenting and tracking any remediation efforts that are required, if shortcomings are discovered. Finally, the GDPR compliance or audit function should be subject to review and adjustment.

For funds that are still developing their GDPR compliance programs, it could be worthwhile to prioritize key areas to address before May 25, to minimize high-level risks. Funds should also examine budget projections and expectations for GDPR-related technology and compliance expenses that could increase in the years ahead.