December 21, 2017

Is Your Company Prepared for the GDPR?

The European Union's new data privacy and security framework, the General Data Protection Regulation ("GDPR"), will take effect on May 25, 2018. Is your company prepared?

Promulgated in 2016 after years of negotiation, the GDPR represents a simultaneous broadening and tightening of already stringent requirements governing the handling of personal data of individuals located in the EU. Many companies engaged in significant business in Europe are already preparing to meet the GDPR's requirements. But the regulation's extraterritorial reach sweeps more broadly than some non-EU-based companies may realize, and the penalties for noncompliance can be severe — up to 4% of worldwide revenue. The following is a synopsis of key GDPR provisions, as well as takeaways that all organizations should consider, even those without a significant EU presence. Now is the time for companies that have not done so to assess whether any aspect of their business may be subject to the GDPR and make all necessary preparations.

Scope. The GDPR applies to "processing" (the collection, recording, storage, or other operation) of "personal data" of individuals located in the EU, defined to include any information relating to an identifiable person, such as a name, ID number, online identifier, or other identifying factor. The regulation will apply not only to data "controllers," the parties that determine the purposes and means of processing the data, but also to data "processors," the parties that perform that processing. Importantly, the GDPR is extraterritorial in scope, applicable to companies outside the EU where the processing relates to the offering of goods or services to EU individuals or the monitoring of EU individuals' behavior.

Compliance Requirements. The GDPR's requirements are extensive. To comply, companies that handle data of EU individuals, or "data subjects," must:

- Obtain express and specific consent for the processing of personal data, which consent must be demonstrable and subject to withdrawal, or ensure that another legal basis for processing applies;
- Provide specified information to the data subject regarding the data controller, the intended purposes in processing the subject's personal data, the subject's rights, and any data transfer outside the EU;
- Empower the data subject to demand erasure of personal data (the so-called "right to be forgotten"), correct inaccurate data, or restrict processing in certain circumstances (e.g., where accuracy is contested);

- Implement appropriate data security measures proportional to the associated risk, such as the use of data pseudonymization and encryption;
- Notify a supervisory authority of a data breach involving EU personal data within 72 hours and, in certain cases, notify affected data subjects;
- Designate a data protection officer in certain circumstances (e.g., where core activities require regular monitoring of data subjects), and a GDPR representative within the EU if the company is not established in the EU;
- Ensure that appropriate safeguards are implemented before any transfer of personal data outside the EU; and
- Satisfy other record-keeping and risk-assessment requirements.

Considerations. Companies not based in the EU should carefully consider the applicability of the GDPR to their activities, applying the following considerations:

- Companies should determine whether they control or process any personal data of EU individuals and whether the benefit of such activity outweighs the burden of GDPR compliance; and
- Companies involved in new business or M&A transactions that could bring them within the GDPR's scope should diligence counterparties' data privacy and cybersecurity compliance and risks and be prepared to comply with the regulation from the outset.

Cybersecurity and data privacy are critical risk areas for companies of most every profile, and risk oversight of these areas is an important board mandate. With cyber threats increasing in volume and intensity, even companies not subject to the GDPR may benefit from assessing how their compliance protocols stack up to the GDPR's strict and prescriptive requirements.

While certain features of the GDPR may appear overwrought when viewed from outside Brussels, protocols such as collecting data on an "as-needed" basis, employment of data encryption and pseudonymization, designation of a responsible data protection officer, and thorough recordkeeping should be viewed as best practices. Apart from reducing the risk of breach and associated liability, robust data security practices may ultimately prove to be a competitive advantage even where not legally mandated.

Marshall L. Miller
David M. Adlerstein
Jonathan Siegel