NEAL GERBER EISENBERG

Publication

CLIENT SERVICES
Intellectual Property
Technology Transactions

02.09.18

Client Alert: GDPR May 25th Deadline Approaching – Businesses Globally Will Feel Impact

In less than four months, the General Data Protection Regulation (the "GDPR" or the "Regulation") will take effect in the European Union/European Economic Area, giving individuals in the EU/EEA greater control over their personal data and imposing a sweeping set of privacy and data protection rules on data controllers and data processors alike. Failure to comply with the Regulation's requirements could result in substantial fines of up to the greater of €20 million or 4% of a company's annual worldwide gross revenues. Although many American companies that do not have a physical presence in the EU/EEA may have been ignoring GDPR compliance based on the mistaken belief that the Regulation's burdens and obligations do not apply outside of the EU/EEA, they are doing so at their own peril.

A common misconception is that the Regulation only applies to EU/EEA-based corporations or multinational corporations with operations within the EU/EEA. However, the GDPR's broad reach applies to any company that is offering goods or services to individuals located within the EU/EEA or monitoring the behavior of individuals in the EU/EEA, even if the company is located outside of the European territory. All companies within the GDPR's ambit also must ensure that their data processors (i.e., vendors and other partners) process all personal data on the companies' behalf in accordance with the Regulation, and are fully liable for any damage

caused by their vendors' non-compliant processing. Unsurprisingly, companies are using indemnity and insurance clauses in data processing agreements with their vendors to contractually shift any damages caused by non-compliant processing activities back onto the non-compliant processors, even if those vendors are not located in the EU/EEA. As a result, many American organizations that do not have direct operations in the EU/EEA nevertheless will need to comply with the GDPR because they are receiving, storing, using, or otherwise processing personal data on behalf of customers or business partners that are subject to the Regulation and its penalties. Indeed, all companies with a direct or indirect connection to the EU/EEA – including business relationships with entities that are covered by the Regulation – should be assessing the potential implications of the GDPR for their businesses.

Compliance with the Regulation is a substantial undertaking that, for most organizations, necessitates a wide range of changes, including:

- Implementing "Privacy by Default" and "Privacy by Design";
- Maintaining appropriate data security;
- Notifying European data protection agencies and consumers of data breaches on an expedited basis;
- Taking responsibility for the security and processing of third-party vendors;
- Conducting "Data Protection Impact Assessments" on new processing activities;
- Instituting safeguards for cross-border transfers; and
- Recordkeeping sufficient to demonstrate compliance on demand.

Failure to comply with the Regulation's requirements carries significant risk. Most prominently, the GDPR empowers regulators to impose fines for non-compliance of up to the greater of €20 million or 4% of worldwide annual gross revenue. In addition to fines, regulators also may block non-compliant companies from accessing the EU/EEA marketplace through a variety of legal and technological methods. Even setting these potential penalties aside, simply being investigated for a potential GDPR violation will be costly, burdensome and disruptive, since during a pending investigation regulators have the authority to demand records demonstrating a company's compliance, impose temporary data processing bans, and suspend cross-border data flows.

The impending May 25, 2018 deadline means that there are only a few months left for companies to get their compliance programs in place before regulators begin enforcement. In light of the substantial regulatory penalties and serious contractual implications of non-compliance, any company that could be required to meet the Regulation's obligations should be assessing their current operations and implementing the necessary controls to ensure that they are processing personal data in a GDPR-compliant manner.