Long Island BusinessNEWS
OCTOBER 5-11, 2018 | OUR 65TH YEAR | NO. 40 | $2.00 | LIBN.COM

EU's data protection regulation could impact LI firms

By THOMAS TELESCA and NICOLE DELLA RAGIONE

The European Union's new General Data Protection Regulation, which took effect in May, aims to protect the personal data of EU citizens, but it may very well impact Long Island businesses with grave consequences. We highlight some of the compliance issues here, and issues that should cause companies concern.

Many may not expect a regulation from the EU to affect a local business. However, the GDPR has an extraterritorial scope – meaning it applies to companies not established and/or physically operating within the EU. A business can come within the reach of the GDPR regardless of its size if it handles personal data belonging to EU citizens. A marketing firm, for example, which collects information on EU citizens, or any company that sells products to the EU, targets EU citizens for sales via the internet or otherwise, or which accepts the Euro as a form of currency may need to comply with the GDPR. Why is this important to U.S. businesses? There can be dire consequences for failing to comply.

A company could be fined up to 4 percent of its annual global turnover or €20 million, whichever amount is greater. To understand the gravity of the GDPR's potential fines, look to Facebook's recent Cambridge Analytica breach, which occurred prior to the implementation of the GDPR. Facebook was fined €500,000 (approximately $586,000). However, if the GDPR had been in effect, it could have faced a $1.9 billion fine.

The GDPR brings new compliance problems for businesses. Importantly, personal data under the GDPR has a broader scope than many U.S. businesses are accustomed to protecting. In addition to names, addresses, social security numbers, and financial information, the GDPR now considers information as seemingly innocuous or insignificant as eye color, weight, religious and political opinions to be deserving of protection. Geo-tracking data, or cookies, also come under greater scrutiny. This will require companies with nearly any connection to the EU to work with their IT departments and legal counsel to assess their data and if they are adequately protecting personal data to meet GDPR requirements.

Together with assessing their data and data security, companies must determine if they have a lawful reason for collecting and processing the personal data in the first place. Companies must update or create a privacy policy that aligns with GDPR requirements. Under the GDPR, there are six lawful reasons for collecting and processing personal data. Companies must ensure that their collection and use of the data complies with one of those lawful purposes, such as consent or to perform contract. Not an easy task, considering how this is an entirely new way of viewing data.

Additionally, data breach reporting requirements are different from those in the United States. Once a company becomes aware of a breach, it must notify a GDPR supervisory authority within 72 hours. This tight timeline may be difficult for companies to meet, and increasing the difficulty of reporting, there is little guidance on which supervisory authority a U.S. company should make its report.

The GDPR also gives EU citizens new rights, such as the "Right to be Forgotten," which will apply in the United States. One can revoke consent for a company to process their personal information, and can request that a company delete them from every data system within the company with limited exceptions. If a company does not understand its IT systems and where it stores an individual's data, complying with this request could be burdensome, or even impossible.

With the severe consequences that may result from a failure to comply with the GDPR, any Long Island business is well advised to assess its GDPR compliance.

Telesca and Della Ragione are attorneys with Ruskin Moscou Faltischek.