Nutter uncommon law

INSIGHTS
NOVEMBER 2017

"Affected companies need to conduct a risk assessment, institute a data protection plan, implement measures to mitigate risk of data loss, and designate a Data Protection Officer."

GDPR Compliance: Think It Doesn't Apply to You? Think Again

Q: HOW BROADLY WILL THE EU GDPR LAW REACH? WHAT TYPES OF COMPANIES WILL BE AFFECTED?

SETH BERMAN: In addition to applying to companies in the EU, the GDPR applies to companies that lack a physical presence in the EU if those companies process personal data of EU residents. This actually applies to even more companies than it may at first seem, as the GDPR defines personal data to include not only the more typical identifying information such as name, address, or date of birth, but also less personal seeming details such as a user's web browsing history or IP address.

The GDPR includes provisions regulating how companies interact with EU citizens' data, what types of notice and consent companies need to obtain from users, the rights users have in their data (including a right to review it and, in most instances, erase it), special provisions for minors, and creates a reporting requirement in cases in which EU residents' personal data has been breached.

Q: WHAT HURDLES WILL BUSINESSES WHO NEED TO BECOME GDPR COMPLIANT HAVE TO OVERCOME?

SB: Companies should expect that compliance with GDPR will be a significant undertaking and should start taking steps now to meet these requirements.

In order to properly prepare for GDPR compliance, every company that touches European citizen data needs to conduct a risk assessment, institute a data protection plan, implement measures to mitigate risk of data loss, and designate a Data Protection Officer before the May 25, 2018 deadline.

Companies will need to audit the data they are currently holding and ensure that the permissions their EU customers granted clearly and accurately outline the intended use of their personal data. Of course, since GDPR applies only to the EU resident's data, companies can in theory decide to segregate their networks and businesses so that they treat EU data differently than non-EU data. In practice, however, this often proves quite tricky, and many companies may decide instead to try to abide by at least some parts of GDPR for all their users' data.

Q: DO COMPANIES FACE ANY CONSEQUENCES IF THEY AREN'T COMPLIANT?

SB: Yes. Failure to comply with the new law can result in penalties of up to 4 percent of global annual revenue or €20 million, whichever is greater. These are much larger penalties than have been traditionally applied in Europe for corporate compliance violations, and could rival or exceed the largest fines that have been paid by U.S. companies for corporate misconduct.

In addition, it is important to note that enforcement is country-specific, which means that each EU member state has its own data protection officers charged with enforcement of GDPR, such as the CNIL (La Commission Nationale de l'Informatique et des Libertes) in France or the LDI (Landesbeauftragte für Datenschutz und Informationsfreiheit) in Germany. The details of the legislation and how it is interpreted will likely vary from country to country—the GDPR sets the data protection floor, not the ceiling. It is also worth noting that regulators from multiple countries can impose penalties on a company for the same infraction so long as each of their citizens were impacted.

Seth P. Berman

PARTNER
Litigation Department
617.439.2338
sberman@nutter.com

Seth P. Berman leads Nutter's Privacy and Data Security practice group and is a partner in the firm's Litigation Department. Corporations and their boards engage Seth to address the legal, technical, and strategic aspects of data privacy and cybersecurity risk, and to prepare for and respond to data breaches, hacking and other cyber attacks. Seth teaches a Cyber Crime Law class at Harvard Law School.

PRESS CONTACT:
Heather Merton
Senior Communications Manager
617.439.2166
hmerton@nutter.com

Nutter is a top-tier, Boston-based law firm that provides legal counsel to industry-leading companies, early stage entrepreneurs, institutions, foundations, and families, across the country and around the world. The firm's lawyers are known for their client-centric approach and extensive experience in business and finance, intellectual property, litigation, real estate and land use, labor and employment, tax, and trusts and estates. Co-founded in 1879 by Louis D. Brandeis, who later became a renowned justice of the U.S. Supreme Court, Nutter is dedicated to helping companies prosper in today's fast-paced business environment.