December 29, 2015

What US Companies Need to Know About New EU Data Protection Rules

By Doron S. Goldstein, Lisa Lowry and Matthew Baker*

On December 15, the European Commission put forward the General Data Protection Regulation (GDPR), which—subject to formal adoption by the European Parliament in 2016—will replace the 1995 Data Protection Directive, the existing basis for national data protection laws in the European Union. Historically, data protection authorities have expressed concern over "fragmentation in the way personal data protection is implemented across the union, legal uncertainty[,] and a widespread public perception that there are significant risks associated notably with online activity."[1] The GDPR is meant to address these concerns by increasing data protection and clarifying the rights of consumers with respect to their data.

> **Key Take-Away**
>
> Though there are no immediate action items, it is important for US-based companies operating in the European Union—beginning in 2016—to consider the GDPR's requirements as integral components to their privacy and data security planning to avoid complications during the transition to the new regulatory regime.

One critical feature of the GDPR is that it expands the scope of EU data privacy protection regulation to cover *all businesses* that control or process personal data related to the offering of goods and services or that monitor the behavior of individuals in the European Union, whether those companies are based in the European Union or elsewhere. The complex, 200-plus page rule package raises many questions for affected companies who will need to take advantage of the two-year implementation period to make substantial adjustments to comply with the GDPR. Among the top concerns are how potentially-significant conflicts with U.S. law will be resolved and how strictly the provisions of the GDPR will be enforced.

Below are key aspects of the GDPR that could affect businesses operating in the European Union:

Enforcement

- The GDPR establishes a centralized regulator for data processing activities within the European Union. Although not quite a "one-stop-shop," the single regulator is meant to streamline compliance for businesses.

[1] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (Jan. 25, 2012), available here.

* Matthew Baker, an associate in the Litigation and Dispute Resolution practice and candidate for admission to the California bar, contributed to this advisory.

For more information, please contact any of the following members of Katten's **Privacy, Data and Cybersecurity** practice.

Doron S. Goldstein
+1.212.940.8840
doron.goldstein@kattenlaw.com

Megan Hardiman
+1.312.902.5488
megan.hardiman@kattenlaw.com

Leonard A. Ferber
+1.312.902.5679
leonard.ferber@kattenlaw.com

Tanya L. Curtis
+1.312.902.5593
tanya.curtis@kattenlaw.com

Claudia Callaway
+1.202.625.3590
claudia.callaway@kattenlaw.com

- Businesses will face a greater range of potential fines for non-compliance under the new GDPR: administrative fines could be as high as 4 percent of the business's total world-wide revenue for the preceding year.
- Liability for data breaches under the GDPR will extend to third-party entities involved in processing data for the provision of specific services.

Restrictions on Businesses

- Companies that process sensitive data on a large scale or collect information on large numbers of consumers will be required to appoint a data protection officer.
- The GDPR will impose a risk-based requirement on companies that control data (and in certain circumstances those that process data as well) to carry out data protection impact assessments with "regard to the entire lifecycle management of personal data from collection to processing to deletion."
- The new regulations will tighten requirements for valid consent: "the data subject's consent" must be "freely given, specific, informed and unambiguous" and expressed affirmatively "either by a statement or by a clear affirmative action." The rules also set stricter standards for sensitive personal information, including information about race or national origin.
- Companies will be obligated to report data breaches to regulators within 72 hours of a breach, where feasible. Individuals affected by a data breach must be notified "without undue delay."

Consumer Rights

- The GDPR provides consumers with the "right to be forgotten and to erasure," i.e., the right to require that their data be deleted under certain circumstances, including "where the data are no longer necessary in relation to the purposes for which the data are collected or otherwise processed, where data subjects have withdrawn their consent for processing[,] or where they object to the processing of personal data concerning them."
- The GDPR provides a right to data portability for individuals to enable consumers to more easily transfer their personal data between services.
- The age of consent for children under the GDPR is raised to 16 years from 13 years: companies will not be permitted to collect data from children under 16 without parental consent.

Small and Medium-Sized Enterprises (SMEs)

- Smaller businesses may be able to take advantage of certain exceptions and cost-shifting benefits.

Key Points for US-Based Companies

As a result of these impending regulations, businesses should carefully evaluate changes to existing practices and, looking forward, establish a plan for easing into the new regulatory regime. US-based companies that collect personal information and that operate within the European Union should consider preparing for the GDRP's implementation by:

- Developing (or revising) a privacy program that collects and retains personal information only to the extent necessary (e.g., adhering as closely as possible to the European Union's "purpose limitation" requirements);
- Appointing a knowledgeable data protection officer or a chief privacy officer to oversee the company's privacy practices and ensure compliance with both domestic and international regulations;
- Reviewing (and possibly amending) contracts with third parties that process, control or maintain collected personal information to ensure proper safeguards and data breach reporting procedures; and
- Ensuring that there are updated and tested data breach response policies and programs to ensure timely notification to regulators and consumers in the event of a data breach.

Finally, businesses should look to the European Commission for additional guidance in the coming months. In its recent press release, the European Commission indicated that it "will work closely with Member State Data protection authorities to ensure a uniform application of the new rules" and, "[d]uring the two-year transition phase, the Commission will inform citizens about their rights and companies about their obligations."