PUBLICATION

Significant New EU Data Protection Privacy Framework Regulation Approved

Authors: Alisa L. Chestler
April 20, 2016

On April 14, 2016 the European Parliament approved the European Union General Data Protection Regulation (GDPR), which replaces the EU Data Protection Directive (95/46/EC), the privacy law originally established in 1995. The regulation should be published in the *EU Official Journal* in May, and would go into effect after a two-year transition period.

Organizations maintaining personal information on EU citizens should begin a process of understanding how this new law will affect them. The GDPR includes significant enforcement fines for non-compliance, stricter data subject consent requirements and data breach notification requirements to the EU. On the positive side, the GDPR will mean that the previous fragmented approach, which permitted differences in law between the 28 member countries, will be condensed into a single set of rules for organizations to manage. However, member state regulators will continue to play an important role with enforcement of the GDPR; thus, differences in interpretation and enforcement are likely to develop.

Significant changes include, among others:

1. As noted above, the stricter enforcement scheme can spell trouble for companies. Non-compliance permits regulators to levy financial sanctions of up to four percent of the annual global revenue of the company. Companies are required to notify the local authorities and individuals of data breaches.
2. Information governance responsibilities are clearly delineated in the regulations. For instance, companies will have increased responsibility for knowing what information they control and how they must safeguard it. Individuals will have the "right to be forgotten," which can present a complex set of issues for companies. They will also have the right to have better control over their personal data (e.g., clear and affirmative consent) and to be informed in clear and plain language regarding a company's privacy policies.
3. American companies that process any personal information or target EU residents by proposing goods or services will be subject to the GDPR.
4. Most companies will have to appoint a Data Protection Officer (DPO), especially if they process sensitive data. The DPO will report to the highest management level.
5. A privacy impact assessment (PIA) will be a mandatory prerequisite before processing personal data. This documentation will need to be robust, especially when the operations are likely to present higher privacy risks to individuals.
6. New rules provide special safeguards for children, including requiring parental consent in some circumstances. The age threshold for children (between 13 and 16) for these new safeguards will be established by the member states.

American companies with bricks and mortar operations in the EU and those that target EU consumers for sales of goods and services should begin to address the implications of the GDPR on corporate compliance. As part of this, companies should identify (i) what, if any, personal data is collected or processed on EU consumers; (ii) to what extent current privacy and information security policies will need to be updated or developed to address the requirements of the GDPR; (iii) what positions within the organization should have oversight and

responsibility for GDPR compliance; and (iv) a project plan and budgeting process for addressing GDPR compliance.

If you have any questions regarding this new regulation, please contact the author of this alert or any member of our Privacy and Information Security Group.