von Briesen
von Briesen & Roper, s.c. | Attorneys at Law

EU Strengthens Global Data Protection Regulations: Steps You Can Take Now to Ensure Compliance

Jan 08 2016

Posted By: Mark F. Foley

Practice Area: Information Technology, Data Privacy and Security

On December 17, 2015, European Union officials approved a new General Data Protection Regulation ("GDPR"). The GDPR will likely be signed into law in January 2016 and take effect early in 2018. The GDPR will replace the current EU Data Privacy Directive. The GDPR will create a consistent data protection standard throughout the European Union and set a higher global standard for personal data protection.

The GDPR applies to any company that does business with European customers or European employees, whether or not the company has physical operations in the EU.

Beware of Eight Figure Penalties
Compliance with the GDPR will be critical. EU data protection regulators will now have authority to issue penalties equal to **the greater of €10 million ($10.82 Million) or 2% of the entity's global gross revenue** for violations of record-keeping, security, breach notification, and privacy impact assessment obligations. Violations of obligations related to legal justification for processing, data subject rights, and cross-border data transfers may result in penalties of **the greater of €20 million ($21.65 Million) or 4% of the entity's global gross revenue**.

Other Key Provisions
In addition to significant penalties, the 200-page GDPR has several other provisions of importance to companies within its reach, such as:

1. **Expands Jurisdiction of EU Regulators.** Companies outside the EU are subject to the jurisdiction of the EU regulators just by collecting data concerning an EU citizen.
2. **Definition of Personal Data.** The definition of "personal data" expands to include information concerning an individual's physical, physiological, genetic, mental, economic, and/or cultural or social identity (e.g., location data, online identifiers, IP address, RFID codes, and social networking data).
3. **Companies without a Physical Presence in the EU Must Appoint an EU Based Representative.** Companies doing business with the EU or processing personal data about EU citizens without a presence in the EU **must** appoint an EU-based representative if they have either: (a) stable, non-occasional arrangements in the EU or (b) data processing activities related to offering goods or services in the EU or monitoring behavior of EU residents. The EU based representative is responsible for communicating with the EU regulatory authorities regarding the company's obligations under the GDPR and serves in a role akin to a registered agent.
4. **Increased Notice Requirements for Consumers.** A company utilizing Personal Data of EU citizens must provide the following upon request:
   (a) A detailed notice about the collection and use of their Personal Data, including the legal justification for the processing, the source of the data, and the retention period.
   (b) Copies of their Personal Data via an electronic request and response systems.
   (c) Transfer of data received directly from an EU citizen to another entity of that person's choice.
5. **Consent to Processing Personal Data.** When a company relies on individual consent as justification for data processing, that consent cannot be made conditional to performance of a contract or receipt of a service, unless the consent is actually necessary to the entity's performance.
6. **Breach Notification Standard.** A data processor must notify the data protection authority without undue delay and, where feasible, **within 72 hours** of becoming aware of a breach. The only exception is when a company can demonstrate the breach is unlikely to result in a risk to the individual. Risks include physical, material, or moral damage (e.g., discrimination, identity theft or fraud, financial loss, and damage to reputation).
7. **The Right to Be Forgotten.** A company must delete an EU citizen's Personal Data if it is no longer used for the original purpose or if the EU citizen revokes consent.
8. **Class Action Suits.** Class action suits by non-profit, public interest bodies are permitted. Individual complaints are still possible.
9. **Data Protection Officer.** Companies whose core business is large-scale processing of sensitive data or monitoring data must appoint a Data Protection Officer.

Steps to Take Now to Ensure Timely Compliance with the New Regulation.

1. **Evaluate.** Audit and assess existing data collection and processing procedures which relate to EU citizens, consent processes, and technical security measures, including use of privacy impact assessments.
2. **Contract Review.** Review existing and new contracts with vendors who handle or have access to Personal Data of EU citizens (whether consumers or employees) to make those vendors comply with applicable GDPR standards.
3. **Update.** Update internal and external policies and procedures addressing how Personal Data is processed, used, stored, and secured and how EU citizens may exercise their right to be forgotten, to withdraw consent, or to obtain information.
4. **Insurance.** Review insurance policies to assess coverage.
5. **Test.** Develop and test data breach response plans.
