Reinhart

Like it or Not – GDPR is Here

Effective May 25, 2018, American companies that collect, host or otherwise process the personal data of people located in the European Union (EU) will need to comply with the EU's new comprehensive data security and privacy law known as the General Data Protection Regulation (GDPR). The law not only reaches American companies with EU operations or employees but also many companies operating entirely outside of the EU. The GDPR's requirements vary significantly from data privacy obligations imposed by U.S. law and afford individuals certain rights related to their personal data.

If your company may be affected by GDPR and is not currently compliant, this article will both inform you on the applicability of the new regulation and suggest ways to move towards compliance.

POSTED:

May 25, 2018

RELATED SERVICES:

Data Privacy and Cybersecurity
https://www.reinhartlaw.com/services/data-privacy-and-cybersecurity

RELATED PEOPLE:

Martin J. McLaughlin
https://www.reinhartlaw.com/people/martin-mclaughlin

Who the GDPR Applies To

The GDPR applies in three instances:

1. Companies operating in the EU;
2. Companies that sell goods or services into the EU; and
3. Companies that monitor personal data of people located in the EU.

Processing means any operation performed on personal data, such as collecting, recording, storing, using, disseminating or deleting. It includes the collection of any identifying information of individuals located in the EU, such as logging IP addresses of website visitors or tracking cookies from their computers. Thus, a business can subject itself to the GDPR without any actual sales to EU residents if sufficient monitoring or marketing occurs.

Personal Data

The GDPR broadly defines "personal data" to include any information that can be used to directly or indirectly identify a person. Personal data can include someone's name, email address, bank information, a photo, financial account information, credit card number, medical information, social networking posts, and any other information that can be traced back to an individual. Personal data also includes technical information, such as IP addresses, cookies, or other

electronic identifiers that may be used to identify a person. In effect, the collection, processing, use, or storage of any information that contributes to identifying a person may trigger the obligations and liabilities of the GDPR.

GDPR Requirements

Companies falling within the purview of the GDPR must satisfy a lengthy list of requirements. For example, companies that collect or process personal data must provide individuals with specific notices and have a legitimate purpose or unambiguous consent prior to collecting personal data. The GDPR also requires companies to obtain explicit consent in certain situations, such as to collect sensitive data which can include information related to a person's health, race, religion, or political affiliation. The GDPR also requires companies transferring data from the EU to the United States to fall within enumerated safe harbors. Further, if a data breach occurs, the GDPR generally requires notification to the relevant authorities within 72 hours of the discovery thereof. As a practical matter, these specific consent, disclosure, and transfer requirements will require many companies to update, clarify and expand their existing information security procedures and privacy policies.

Five Steps to Become GDPR Compliant

If you believe your company may be affected by the GDPR and is not already compliant, speak with someone knowledgeable about the GDPR as soon as possible. For many companies, becoming compliant will require the active participation of personnel from several internal departments (e.g., IT, legal, HR, etc.), outside consultants and advisors.

Companies that are subject to the GDPR but who are not currently compliant, should take the following initial steps:

1. Determine what and how much EU data the company has and consider deleting unnecessary EU data;
2. Prioritize compliance tasks based on risk exposure;
3. Update the company's privacy policies to include necessary disclosures;
4. Send notice to any vendors that process EU personal data on the company's behalf informing them that they are subject to GDPR and the need to execute a data processing addendum; and

5. Determine the appropriate safe harbor for any transfer of data from the EU to the United States.

If you have any questions or concerns about GDPR, please contact Marty McLaughlin or another member of Reinhart's Data Privacy and Cybersecurity team at 414-298-1000.