IAITAM: U.S. COMPANIES NEED TO GEAR UP NOW FOR NEW EU DATA PRIVACY REGULATIONS

Companies That Do Business in Europe Or With Europeans Face Major New Requirements; IT Asset Managers Need to Grasp Full Import of New Rules for Data Breach Disclosures, Designated "Data Protection Officers," And More.

WASHINGTON, D.C. & CANTON, OH.///April 28, 2016///Thousands of American companies that do business in Europe directly or online with European customers will need to start reckoning with data privacy regulations enacted this month by the European Union (EU) that are due to go into full effect in just two years, according to the International Association of Information Technology Asset Managers, Inc. (IAITAM).

IAITAM CEO Dr. Barbara Rembiesa said**: "These are sweeping changes to how personal and coprorate data is to be handled and they have far-reaching implications for many aspects of U.S. businesses, particularly in terms of how information security is addressed. The days are long past when U.S. businesses could worry only about complying with laws and rules in this country. Companies that fail to start planning now to deal with the General Data Protection Regulation (GDPR) requirements are going to be in for a real shock."**

IAITAM identified the top five impacts the new EU regulations will have on any organization:

1. ***Data breaches.*** "A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed" – The changes the GDPR makes to the definition of a data breach are significant. Simply stated, if an organization experiences a data breach, it must now be reported within 72 hours of the company becoming aware of the breach. Up until this point, a data breach typically is only announced in the U.S. when word of the breach is leaked to the public or media.

2. ***Data Protection Officer requirement.*** "The Controller or Processor shall designate a Data Protection Officer" – The EU has determined that an individual is necessary at each company doing business in Europe to ensure that data privacy and data control are maintained at a high standard. These Data Protection Officers (DPO) are to be "designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and ability to fulfill its tasks."

3. ***Consent of those providing data.*** "The data controller bears the burden of proof for the data subject's consent to the processing of their data for specified purposes. Any written request for consent must be presented in a manner which is clearly distinguishable from other matters. Consent will not serve as a legal basis for processing when there is a significant imbalance between the position of the data subject and the controller." – This aspect of the GDPR requires active acceptance of the terms and conditions by the end-user. Consequently, mere "use" by the end-user will no longer be sufficient acceptance of the terms and conditions.

4. ***Special handling of data related to Europeans.*** "Any transfer of personal data to a third country or to an international organization may only take place if, subject to the provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller or processor, including for onward transfers of personal data from the third country or an international organization to another third country or to another international organization" – This provision was created within the GDPR to specifically protect EU citizen's data once it's moved outside the EU. Any organization that is international in scope and handles personal information of EU citizens such as phone numbers, addresses or any other identifying information will be subject to the GDPR. Also, any organization that received the information "third-hand" will also be subject to the regulation.

5. ***Potential for hefty fines and court penalties.*** "For infringements of this Regulation, in particular for infringements which are not subject to administrative fines, Member States shall lay down the rules

on penalties applicable to such infringements and shall take all measures necessary to ensure that they are implemented. Such penalties shall be effective, proportionate and dissuasive." – An effective policy is an enforced policy. Subject to what would be referred to as a "tort" in the United States, an organization will be fined by the Member States to ensure that the damage to an individual is made whole in addition to penalties and fines meant to deter any additional infractions. This type of enforcement can become increasingly potent and result in monetary penalties reaching into the billions.

Rembiesa said: **"What is important to take away here is that any organization that processes or handles data from EU citizens must become familiar with this legislation and fully understand the impact it will have on daily business processes. Between the sweeping scope of the GDPR and the penalty structure, this is a piece of legislation that should be treated seriously and with an eye to what it will take ensure full compliance."**

IAITAM also recommended the following resources for those wishing to learn more:

The European Union General Data Protection Regulation Portal - http://www.eugdpr.org

The International Association of Privacy Professionals: Top 10 Operational Impacts of the GDPR - https://iapp.org/resources/article/top-10-operational-impacts-of-the-gdpr

Squire-Patton-Boggs: EU National Data Protection Regulators Raise Privacy Shield Concerns - http://www.iptechblog.com/2016/04/eu-national-data-protection-regulators-raise-privacy-shield-concerns/

ABOUT IAITAM

The International Association of Information Technology Asset Managers, Inc. (IAITAM) is the professional association for individuals and organizations involved in any aspect of IT Asset Management, Software Asset Management (SAM), Hardware Asset Management, Mobile Asset Management, IT Asset Disposition and the lifecycle processes supporting IT Asset Management in organizations of every size and industry across the globe. IAITAM certifications are the only IT Asset Management certifications that are recognized worldwide. For more information, visit www.iaitam.org, or the IAITAM mobile app on Google Play or the iTunes App Store.

MEDIA CONTACT: Alex Frank, (703) 276-3264 or afrank@hastingsgroup.com.