GDPR-Compliant by May 25, 2018 – Are You Ready?

The European Union’s General Data Protection Regulation (GDPR or regulation) was adopted in 2016 and becomes effective May 25, 2018. This regulation is the EU’s attempt to provide better data security and privacy protection for EU citizens and to allow them greater control over their personal data.

This regulation will affect any association or organization that collects or processes personal data of an EU citizen, who is residing in the EU, regardless of the location of the association or where the personal data is stored. The full GDPR text may be viewed at: https://gdpr-info.eu/

“Personal data” means any information relating to an identified or identifiable natural person (“data subject”); an identifiable person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, online identifier (e.g., email address) or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

An association that owns or manages personal data of EU citizens residing in the EU is defined by the GDPR as the Data Controller. A vendor that the Data Controller utilizes to process or store the Controller’s personal data is generally defined as a Data Processor.

Under the GDPR, Data Controllers are responsible for, and must be able to demonstrate compliance with the principles relating to the processing of personal data. Data Processors are responsible for implementing technical and organizational measures that allow Data Controllers to comply with the regulation.

According to the regulation, the Data Controller must select Data Processors who can provide “sufficient guarantees” that the GDPR requirements will be met. In addition, there must be a written contract between the parties that contains minimum criteria specified in the regulation.
Data Controllers and Data Processors are required to understand and follow the requirements of the regulation. In brief, the major requirements include:

- EU citizens residing in the EU (“EU citizens/residents”) must consent to the storage and use their personal data. This requires the affirmative action by the individual to give consent. For example, pre-checked opt-outs are not compliant.

- Individuals who are EU citizens/residents and EU authorities must be notified within 72 hours of discovering a security breach impacting the personal data of such individuals.

- EU citizens/residents must be able to receive copies of their digital personal data when requested, as well as a description of where they are stored, their use, and the opportunity to correct them.

- EU citizens/residents have the right to have their personal data deleted and not used or shared.

- GDPR requires that organizations have data privacy controls and security built into products and systems. It is expected that this requires the use of commercial best practices for data security.

The maximum fine for infringements is the greater of 20 million Euros or 4 percent of the offender’s worldwide turnover (sales) for the prior financial year.

An informative GDPR handbook prepared by White & Case can be viewed at: https://www.whitecase.com/publications/article/gdpr-handbook-unlocking-eu-general-data-protection-regulation