General Data Protection Regulation
"GDPR"
Effective May 25, 2018

The European Union (EU) adopted the GDPR with the purpose to regulate organization's management of data with a primary focus on protections of personal information stored and processed by businesses. This outline provides the highlights of the regulation.

1. GDPR is adopted by the European Economic Area (EEA) which includes the EU* plus Iceland, Liechtenstein, Norway and Switzerland.

2. It applies to any company doing business in, offering goods or services to, or employing, Data Subjects in the EEA. The liability for failure to follow the regulations is massive fines of up to 4% of global revenue or 20 million Euros, whichever is larger. In May 2017 Facebook was fined $122 million under the GDPR's predecessor. Potential liability could be in range of $1.6 billion.

3. Persons must be provided the option of Opt In or Opt Out – the choice can be withdrawn at any time.

4. Persons are granted the right to access their data, and obtain a copy of their data, in an interchangeable format. (Formatting is underdevelopment by Microsoft, Facebook, Google and Twitter)

5. Persons have the right to "be forgotten" – this applies to third parties who may also have access to the data.

6. All data processes going forward must be designed with the concept of "Privacy by Design". This is a new approach to system design requiring businesses to adopt specific design processes that check-point and document the privacy protections at each step.

7. Data breaches must be reported to EEA authorities within 72 hours of the suspected breach.

8. Personal data includes:
   a. Personally Identifiable Information (PII - similar to the US privacy regulations) – Name, birthdate, drivers license, passport, address, social security number. <u>New is a person's IP address(es)</u>
   b. Sensitive personal data, including:
      i. Racial or ethnic origin
      ii. Political opinions
      iii. Religious or philosophical beliefs
      iv. Trade union membership
      v. Genetic or biometric data
      vi. Health
      vii. Sex life or sexual orientation

9. Principles of the GDPR – data must be:
   a. Processed lawfully, fairly and transparently
   b. Collected for specified, explicit and legitimate purposes
   c. Use limited to the purpose it was collected
   d. Accurate and, if needed, kept up to date
   e. Kept only for as long as needed for the purpose collected

f. Processed with appropriate security including Confidentiality, Integrity and Availability

10. Tasks for business:
    a. Businesses must appoint someone to assume the responsibilities of a Data Privacy Officer (DPO).
    b. Conduct a GDPR Readiness Assessment
    c. Update website privacy notices
    d. Complete data inventory
    e. Train all Users
    f. Adopt Privacy by Design
    g. Implement a Secure Software Development Lifecycle (SSDL)
    h. Test for security throughout all components of a system, including third party suppliers
    i. Prepare to respond to inquiries from authorities

11. Restricts the transfer of data outside the EEA unless:
    a. Authorities are convinced that other countries have adequate safeguards in place

The bottom line is that any business doing business in and out of the EEA must comply with the GDPR. Risk Management, Legal Counsel, Information Systems and Security professionals should be engaged to design, fund and oversee the operations of Information Management for their businesses, clients and suppliers operating in the EEA. All steps should documented with the expectation that authorities will request with little notice.

*EU countries - Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the UK.