General Data Protection Regulation (GDPR)

The European Union (EU) General Data Protection Regulation (GDPR) is a regulation designed to strengthen data privacy laws across Europe. The GDPR gives EU citizens and residents control over their personal data. The regulation applies to any organization (data controller) that collects or process data from EU residents. It also covers organization that processes data on behalf of a data controller.

The regulation was debated over four years and approved by the EU Parliament on April 14, 2016. The regulation goes into enforcement on May 25, 2018. Organizations found in non-compliance may face heavy fines up to €20 million or up to 4% of the annual worldwide income (Article 83, Paragraph 5 & 6).

Data must be collected and processed legally, and the subject must give consent by optioning in. The law also gives the subject the right to withdraw consent. Only a minor’s parent or guardian can give consent for a minor.

The regulation gives data subject the right of access, right to be forgotten and right to transfer.

Right of access is covered under Article 15. This article gives the data subject the right to get access to their personal data and information upon request. The data controller must provide the type of data, a copy of the actual data, data processing details, how the data was acquired, if the data was shared, purpose of data collection and whom the data is shared with.

Right to be forgotten is covered under Article 17. This article gives the data subject the right to request erasure of personal data.

Data portability is covered under Article 20. Data subject have the right to transfer personal data from one electronic processing system to and into another. Both data that is being 'provided' by the data subject and data being 'observed' are covered under this article. Data controller must provide data to the data subject in a structured and standard electronic format.

During the meeting we discussed the following implications:

* Enforcement and Penalties: data controller that violate GDPR can be liable for huge penalties.
* Data Protection office: data controller must assign data protection duties to Data Protection Office (DPO).
* Consent: data controller has the burden to prove that the data subject consented freely to data collection and processing.
* Right to be forgotten: data controller must erase data without undue delay.
* Data breach notification: data controller is required to notify “supervisory authority” within 72 hours of becoming aware of any data breach. One thing to note is that the data subject must be notified.
* Scope: this regulation applies to the processing of personal data to even organization outside of EU.

A take away is that GDPR will have major impact in the US. I suspect GDPR will have a strong implication in a company competitiveness and the overall global economy.