Changes in GDPR

Several major changes to the GDPR from the prior directive may have global impacts, as the regulation applies to an organization processing personal data for any data subject residing in the EU, regardless of where the organization is located and whether the data processing occurs in the EU. The GDPR further defines how personal data should be protected and handled, how consent for personal data is granted and withdrawn, and financial penalties for organizations that do not meet the requirements or provide notification of data breaches.

Data subjects will be able to request details from the data controller around what personal data is held, how and why it is being used, and a copy of the data itself, along with having the “right to be forgotten” where the data subject can withdraw consent for their data to be processed and request it be erased permanently (GDPR Key Changes).

This grants individuals more rights and control of their own personal data and will bring transparency to how their personal data is being used. People have become very reliant on technology throughout all aspects of their lives, and provide a large amount of personal information to organizations both directly and indirectly. It is important that these organizations are making a strong effort to protect the myriad personal data they have collected from data subjects.

Organizations affected by the GDPR need to assess their data risk, create a plan to protect personal data and may even need to appoint a data protection officer if they are:

- public authorities
- organizations that engage in large scale systematic monitoring
- organizations that engage in large scale processing of sensitive personal data” (GDPR FAQs)

This regulation provides a set of definitions and requirements that organizations must meet, which will help standardize personal data protection, though it does leave the definition of what would be considered reasonable data protection up to an organization to define. The GDPR has heavy penalties for organizations that do not comply with the regulation, such as 4% of annual global turnover or €20 Million, whichever is higher, for the most severe infractions with regards to not having consent for data processing or meeting basic data privacy standards, while lesser infractions such as not having “their records in order (article 28), not notifying the supervising authority and data subject about a breach or not conducting impact assessment” would result in a 2% fine (GDPR FAQs). The GDPR applies to both data controllers and data processors, so it is important for organizations to be aware of what the regulation requires, how it may apply to their organization, and its penalties for non-compliance, whether they are processing personal data themselves or sending it to a third party for processing.