Data, Data, Everywhere! In Data We Trust!

"Historically, privacy was almost implicit, because it was hard to find and gather information. But in the digital world, whether it's digital cameras or satellites or just what you click on, we need to have more explicit rules - not just for governments but for private companies." – Bill Gates

On May 25, 2018, a new data protection regulation entitled General Data Protection Regulation ("GDPR"), Regulation (EU) 2016/689, will come into force in the European Union ("EU") and its 28 Member States. The GDPR provides significant new data privacy protections for individuals ("data subjects"), with corresponding requirements that must be implemented by organizations, regardless of location, that control or process the personal data of individuals located in the EU.

What are the Requirements of the GDPR?

The GDPR applies to the collection and processing of personal data in connection with an automated process or part of a manual filing system (both direct and indirect personal data, including: name, location, and online identifier). Under the regulations, an organization needs a lawful basis to process personal data and is required to satisfy additional requirements to process "special data" which, among other categories, includes: race; ethnic origin; religion; politics; and sexual orientation.

The GDPR imposes far reaching requirements on "data controllers" (organizations that determine the purpose and means of processing personal data) and "data processors" (third parties who process data on behalf of controllers) within the EU, as well as organizations located outside the EU if the organizations: (1) offer goods and services to persons in the EU; or (2) monitor behavior of individuals in the EU. Mere website accessibility by persons in the EU is likely insufficient to establish intent to offer goods and services to persons in the EU or its individual Member States.

To ensure compliance with the GDPR, organizations must, *inter alia*, institute appropriate technical and organizational measures to implement data protection principles. In addition, organizations should appoint a data protection officer ("DPO"), such as an employee or external consultant who has "expert knowledge of data protection law and practices" that must "directly report to the highest management level" and implement policies consistent with the GDPR for: (1) processing personal data; (2) deleting data when there is no longer a need for it; (3) document retention; (4) responding to data breaches; (5) disclosing personal data; (6) training employees about privacy; (7) maintaining an up-to-date privacy policy and terms and conditions; (8) reviewing of encryption software; and (9) performing regular compliance policy reviews and/or audits.

Data controllers are required to have a written contract with data processors to ensure organizational and technical compliance with the GDPR. The GDPR sets forth what needs to be included in these agreements. The GDPR also provides detailed

restrictions on the cross-border transfer of personal data, which will have significant implications insofar as United States civil litigation discovery requests are concerned.

The GDPR also requires data controllers to self-report security breaches to regulators within 72 hours of the subject breach with some exceptions.

How to Avoid GDPR Liability

To avoid GDPR liability, organizations should, among other things, establish and implement policies and procedures regarding their protection and handling of the data of individuals that they control/obtain, conduct staff training, hire DPOs, and establish breach response protocols. These measures can help identify, prevent, and reduce regulatory and/or legal liability. Companies should review all contracts with business partners to ensure compliance with the GDPR and review insurance policies to make sure that GDPR-related coverage is in place. In addition, organizations should keep records of GDPR organizational and technical measures that have been implemented. This will be useful in the event of an audit by a supervisory authority.

Given the complexity of the GDPR, any company that controls, processes, or collects data from individuals located in the EU should consult with experienced counsel to ensure that all of its data collection, use and sharing policies and procedures are compliant with the new regulations.