GDPR: ARE YOU READY FOR NEW REGS?

Data Privacy Alert
January 22, 2018

The most significant change in data privacy regulation in more than two decades will go into effect on May 25, 2018. The EU General Data Protection Regulation ("GDPR" or "Regs") not only requires compliance by EU organizations but it requires that any non-EU organization that offers goods or services to, or monitors the behavior of, EU "data subjects" (i.e., EU residents), comply with the Regs as well, or face significant penalties. Thus, it is imperative to understand the extent of your organization's handling of, or nexus with, the personal data of EU residents. To be clear, certification under the E.U.-U.S. Privacy Shield does not constitute compliance with the GDPR.

Under the GDPR "personal data" is defined broadly, and includes at least the following: an individual's name, photo, email address, bank information, online identification, identification number, location data, social media information, medical information, computer IP address, and other things.

Assuming you are a covered entity, it is important to know that under the GDPR, failure to comply may result in fines of up to 4% of your organization's annual global turnover or approximately $24.5 Million, whichever is greater. Penalties may be imposed for a variety of non-compliance issues, including failure to keep records according to the Regs, failure to obtain customer consent as proscribed by the Regs, or failure to comply with the notification regime established by the Regs. These are just a few examples of scenarios that may trigger the imposition of penalties.

What should you do to ensure compliance? Begin with the following:

- Determine the extent of your organization's nexus to the personal data of EU residents. Remember, the Regs cover data controllers as well as data processors, which means the GDPR extends to many cloud-based companies.
- Determine whether your organization engages in large-scale data monitoring or large scale data processing. If you fall within either category, the GDPR requires your organization to appoint a Data Protection Officer ("DPO").
- Review the consent requirements under the Regs. Another significant change flowing from the GDPR is that consent must be provided in an easily accessible form, without the typical terms and conditions or legalese we are accustomed to seeing. Also, in order to be effective, the consent must include the purpose for data processing.

Attorneys

Gary Schober

Practices & Industries

Cybersecurity & Privacy

- Review the data breach notification requirements. Under the GDPR, data breaches affecting EU data subjects must be reported to the Supervisory Authority (in accordance with Article 55 of the GDPR) ***and*** individuals affected by the breach "without undue delay, and where feasible, not later than 72 hours after having become aware of" the breach.

Finally, and most significantly, to ensure compliance with the GDPR engage your DPO (or similar corporate privacy or information security officer) early and often.

For more information on the GDPR, and how it may impact your business, contact Jessica L. Copeland or Gary M. Schober.