Data Regulations Coming Into Effect May 2018

March 22, 2018

U.S.-based businesses that receive, collect, store, or process the personal data of individuals located anywhere in the European Union (E.U.), including even website cookies, IP addresses, RFID tag data, etc., will fall under new E.U. regulations in two months.

Specifically, effective May 25, 2018, the General Data Protection Regulation (or GDPR) will regulate how personal data of EU individuals (EU data subjects) may be handled by any business (regardless of location), and will be subject to substantial EU fines (up to the higher of 20 million Euros, or 4% of annual worldwide revenue) if the business is found to be in violation of the requirements under the GDPR.

U.S.-based companies (including those with no physical presence or business in the E.U.) can be equally subject to these laws, if they are controlling or processing the personal data of EU data subjects. It may seem counterintuitive to some that an E.U. regulation could apply to a business with no physical presence in the E.U., but the catch is that these regulations apply to businesses that are receiving and controlling or processing the personal information of E.U. data subjects who have certain rights to control the disposition of their personal information.

Certain limited exemptions apply, but most U.S. businesses with E.U. customers or potential customers, or E.U. employees, or subsidiaries or affiliates that have any of the foregoing, will have possible compliance issues. To help U.S.-based businesses get compliant with these E.U. regulations, and to provide a safe harbor from regulatory exposure to those who make the effort, the U.S. Department of Commerce has established a program called the E.U. (and Swiss) – U.S. Privacy Shield program (www.privacyshield.gov). This program allows a certifying business to enjoy certain safe harbor protections from E.U. and European country-level enforcement of data privacy regulations, if the business registers with the program, completes the self-certification process (annually), and complies.

If you think your business may have reason to receive, collect, and/or store personal information (even just through a website, for example) of E.U. data subjects, and you would like more information about how McGlinchey Stafford's Cybersecurity and Data Privacy practice group can help, feel free to contact any member of the firm's **Cybersecurity and Data Privacy Team**.