

THE EU'S NEW DATA PRIVACY LAWS SHOULD BE ON YOUR RADAR

[Matthew L. Venezia](#)

January 2017

Following years of negotiation, on May 4, 2016, the European Union (“EU”) published the General Data Protection Regulation (“GDPR”) in its Official Journal. The GDPR enters into effect on May 25, 2018.

If your first question is “Why should I care?” then it would be prudent to take some time to get acquainted with the broad reaching effects of the GDPR and how it may apply to your business. Below are some of the key points:

- **Extraterritorial Scope:** Per its terms, the GDPR applies to all business offering goods or services to residents, or processing the personal data, of residents of the EU, whether or not the business is located in the EU. As a practical matter, this means EU regulators may view any business with customers in the EU, including customers by way of e-commerce, or those who collect the data of EU residents for purposes of online marketing, as subject to the GDPR. U.S. businesses should be prepared to face the scrutiny of EU regulators, as the extraterritorial scope of the GDPR was an intentional measure meant to allow the EU regulators to reach businesses located outside of the EU.
- **Serious Enforcement Power:** The GDPR allows for fines of up to 20 million euros or 4% of the business’s total worldwide revenue for the preceding year. While the GDPR provides for a one stop shop, where one EU member state assumes primary enforcement authority for a business, an establishment in EU, as well as compliance with relevant provisions, are necessary to take advantage. Businesses that do not take advantage of the one stop shop provision will be subject to the regulatory authorities in every EU member state.
- **Greater Regulatory Requirements:** The GDPR allows individuals greater rights when it comes to their personal data, including a right to receive any of their personal data processed by a business in a “machine-readable format[.]” the right of erasure, that is the right to have their personal data deleted “without undue delay” when no longer necessary, and requirements for unambiguous and explicit consent prior to the processing of data. The GDPR also makes the appointment of a Data Protection Officer mandatory in some instances and requires notification of certain data breaches to be made to the relevant regulatory authority within 72 hours of discovery.

The above is just a small glimpse into the regulatory requirements imposed by the GDPR. Businesses will be expected not only to be compliant, but to be able to demonstrate compliance. In that regard, businesses would be wise to examine their operations now to determine whether they fall under the umbrella of the GDPR. Given its scope, the majority of businesses with an online presence will at least arguably be subject to the GDPR. For businesses that are subject or arguably subject to the GDPR, counsel should be sought now to determine what actions must be taken in order to be prepared when the GDPR goes into effect.

[TroyGould](#) is prepared to assist your business in the path to compliance with the GDPR. If you have any questions as to how the GDPR may apply to you, you may contact [Matthew L. Venezia](#) at (310) 789-1209 or mvenezia@troygould.com.