You may be asking "What is GDPR and why should I care? It shouldn't affect me." In reality, the implications of GDPR are far-reaching and will impact many industries. The European Union's General Data Protection Regulation (GDPR) is a set of regulations strengthening and harmonizing data privacy and protection laws for residents of the European Union (EU). The regulations go into effect May 25, 2018. Non-compliance with the GDPR can carry serious financial consequences, with penalties topping out at 4% of a company's global gross annual revenue or 20 million Euros, whichever is higher.

As we have been counseling clients leading up to the May 25, 2018 deadline, we have encountered a number of widely held myths with respect to GDPR implementation. Companies with existing stringent privacy and security concerns (e.g., healthcare and financial services) will soon be confronted with a different set of regulations that will materially impact their businesses. Simply put, companies cannot ignore the GDPR.

Myth: The GDPR does not affect my industry.

The implications of the GDPR will impact U.S.-based businesses of all industries – including healthcare and retail – that collect, process and maintain personal data of EU residents regardless of the location of the business. Within the context of the GDPR, a “data subject” is a person who is identified or identifiable. The new regulations will impact most U.S. companies because in all likelihood those businesses will process information of data subjects of the Member States of the European Union as well as those in the European Economic Area (i.e., Iceland, Norway, and Liechtenstein) (EEA). The United Kingdom has also adopted the GDPR in its Data Protection Bill, replacing the Data Protection Act.

Myth: The GDPR does not apply to me because my business is only in the United States.
Previously, the EU’s data protection regulations applied only to organizations that collected or used a data subject’s personal data where the organization was established in the EU or where the organization (although established outside of the EU) processed such as data in the EU. The GDPR, however, will extend the EU’s regulatory reach to organizations established outside of the European Union that process the personal data of EU residents if the processing relates to (i) offering goods or services to those residents or (ii) monitoring the behavior of those data subjects. This is arguably the biggest change of the GDPR compared to the EU’s existing data protection regulations.

Myth: The GDPR does not apply to me because I do not collect personal information.

The GDPR broadens the definition of “personal data” and covers “any information relating to an identified or identifiable natural person.” Personal data can include typical identifiers such as a data subject’s name, social security number, photo or credit card information. It can also include email addresses, cookie strings, computer IP addresses or any other identifying data specific to a data subject’s “physical, physiological, mental, economic, cultural or social identity.” Genetic data and biometric data (e.g., fingerprints, facial recognition, retinal scans) will be treated as sensitive personal data under the GDPR when used to identify a specific individual. Sensitive personal data is subject to a higher standard of compliance for data processors, including a requirement for express consent before such data may be collected, used, or otherwise processed.

Pseudonymous data differs from anonymous data. If data is anonymized, because it does not – and cannot identify – a person, it is not covered by the GDPR. Pseudonymous data, however, may have certain elements deleted, but the data could be, for example, combined with other information to determine the identity of a person. Pseudonymous data, therefore, is subject to the GDPR. To fall outside the GDPR, providers must implement technical and organizational measures to obscure or anonymize personal data in a way that the data cannot be linked to a specific individual without additional information.

Unless the data about a person subject to the GDPR is anonymous, any entity processing such data is subject to the GDPR.

Myth: I have an opt-in on my website; I am already compliant.

Under the GDPR, businesses must demonstrate that an individual data subject has consented to the processing of his or her personal data by a clear, affirmative action or agreement. Such consent can no longer be contained within boilerplate terms and conditions of services. It must be presented in a written manner which is clearly distinguishable from other matters, in an intelligible and easily
accessible form, using clear and plain language. Similarly, the data subject has the right to withdraw his or her consent at any time, and the process to withdraw such consent must also be easily accessible and unambiguous. Explicit consent (i.e., a person must "opt in") is required only if a business is processing sensitive personal information. The GDPR also requires parental consent to be obtained to process the personal data of children under the age of 16.

**Myth: Once data is in the custody of my business, it is the property of my business.**

Data subjects have the right to obtain confirmation from the provider as to whether or not their personal data is being processed, where and for what purpose. Further, upon the data subject’s request, the business must provide a copy of the personal data, free of charge, in an electronic format. A business’s policies and procedures must reflect the rights of individuals, which includes the right to erasure, or right to be forgotten, where the data subject has the right to obtain from the provider the erasure of the personal data without undue delay. The GDPR recognizes numerous other rights of individuals, such as the right to object and the right not to be subject to automated decision-making (e.g., profiling).

Policies and procedures must reflect these various rights and internal workflows must reflect the practical implications of these rights. For example, businesses must notify affected parties of a personal data breach without undue delay and, where feasible, no later than 72 hours after the business has become aware of it.

**Myth: Privacy concerns can be monitored appropriately on an as-needed basis.**

Businesses whose core activities consist of processing operations, where by virtue of their nature, require regular and systematic monitoring of data subjects on a large scale (e.g., healthcare providers, insurance companies) must designate a data protection officer (DPO) responsible for compliance. DPOs must also be appointed for large-scale processing of sensitive personal data. Therefore, while not required in all instances, designing systems and establishing a dedicated position to monitor and implement privacy policies is a prudent step for GDPR compliance. Implementing “privacy by design” protocols provides for technical and operational measures that ensure adequate protection of a data subject’s personal data in compliance with the GDPR.

**Myth: I’m in the United States – How would I get caught? What are the risks of non-compliance?**

The GDPR provides every data subject the right to lodge a complaint with the appropriate EU member authority and permits a legal claim against the provider. It also permits severe administrative penalties
for non-compliance – up to 4% of the offender’s total worldwide gross revenues or 20 million Euros – whichever is higher.

What Do U.S. Companies Need to Do To be Prepared?

According to a January 2017 survey by PriceWaterhouseCoopers, 92% of responding U.S. businesses considered compliance with the GDPR a top priority on their data provider and security agendas for 2017. Top priorities for U.S.-based healthcare providers, clinical researchers, healthcare insurance companies and other business should include:

- an immediate review and assessment of existing policies and procedures for personal data protection,
- confirmation that those policies and procedures have an appropriate compliance framework for the GDPR (such as mechanisms for timely responses to “right to be forgotten” requests or 72-hour notice for data breach notifications),
- annual or other periodic privacy risk assessments,
- appointing specific GDPR data protection officer(s), and
- reviewing data subject applications and contracts to ensure the GDPR’s heightened consent requirements are fulfilled.

If your business has not designed and implemented a plan for GDPR compliance, it should do so now before the May 25, 2018 deadline.

For more information, consult the EU’s GDPR website at www.eugdpr.org.

Contact your relationship attorney or a member of Waller’s GDPR group below.

Kevin Brown  
Partner  
512.685.6405  
kevin.brown@wallerlaw.com

Fletcher Brown  
Partner  
512.685.6423  
fletcher.brown@wallerlaw.com
Andy Norwood
Partner
615.850.8491
andy.norwood@wallerlaw.com