BACKGROUND AND UNIQUENESS OF THE GDPR
The European General Data Protection Regulation (the “GDPR” or the “Regulation”) is set to go live on May 25, 2018. Although the GDPR is a European Union (EU) regulation, it is expected to have a significant and wide-reaching impact that extends far beyond the physical boundaries of the EU. Any company that offers goods or services to, or communicates with, EU citizens (“data subjects”) could be impacted by GDPR to some degree, regardless of company size or physical location.

The GDPR will supersede the Data Protection Directive (“Directive”), which has been in place in the EU since 1995. However, the reach and influence of the GDPR far exceeds that of the Directive. The Directive was merely a set of data protection guidelines set forth for EU Member States. The Member States were each required, separately, to implement the requirements set forth by the Directive. As a result, data protection laws and regulations currently vary from country to country within the EU. In contrast, the GDPR will be directly effective in all 27 EU Member States, as well as the UK, without the immediate need for implementing legislation. This will bring greater consistency throughout the EU as respects data protection laws. Further, the focus of the GDPR is not on the physical location of the company, but rather on the data itself. The Regulation protects and follows the data. For this reason, many U.S.-based companies run the risk of falling within the reach and influence of the GDPR.

The full text of the GDPR can be found here.

IMPACT ON U.S. COMPANIES
Privacy and legal experts generally agree that the GDPR will have an extraterritorial impact with respect to companies that offer goods or services to EU citizens or “monitor” their behavior – such as online tracking or profiling. Companies falling within the reach of the GDPR, regardless of their physical location, will be subject to a multitude of new requirements. Failure to comply with such requirements could result in significant financial consequences.
Challenges GDPR Requirements Present to U.S. Companies

The right to privacy is a highly developed area of law in the EU. The EU Member States generally view privacy as a fundamental human right and, as a result, approach privacy regulation in a comprehensive manner. In contrast, the U.S. does not protect privacy as a fundamental right. Accordingly, U.S. privacy laws are more reactive and narrow in nature. In the U.S., privacy laws and regulations tend to arise in response to specific needs and within specific industry verticals. Further, in terms of scope, U.S. laws provide varying degrees of protection based on the type of personal data at issue (e.g. health care, financial) rather than to all personal data. U.S. companies that do fall within the purview of the GDPR will likely find many of its requirements challenging, since achieving compliance could mean significant changes to the manner in which they do business.

From a practical standpoint, the requirements that could be the most challenging for U.S. companies are as follows:

- **Definition of Personal Data:** The GDPR defines “personal data” broadly. Personal Data under the GDPR is defined as any information relating to an identified or identifiable natural person (e.g. name, home address, photo, email address, bank details, social media posts, medical information, or even an IP address). This definition is significantly broader in scope than the manner in which most U.S. laws define “personally identifiable information” (PII). U.S. companies need to fully understand and appreciate the difference between the two terms – PII and personal data.

- **Privacy by Design:** The concept of “privacy by design” requires proactive consideration and involvement of data privacy in the design and operation of IT systems and business practices. This is not a new concept but the GDPR represents the first time it will be codified. The GDPR will make privacy by design a legal obligation, which means that U.S. organizations that fail to comply with the regulatory requirements may be subject to fines and penalties.

- **Rights and Control:** One of the core goals of the GDPR is to strengthen and enhance data privacy rights of EU citizens. To that end, the GDPR gives EU citizens broad control and rights with respect to their data. Some examples include: (1) **Right to Access:** Under the GDPR, EU citizens will have the right to access their data and know the reasons for collection/use and will have the right to obtain a copy (free of charge) of their personal data; (2) **Right to be “Forgotten”:** The GDPR mandates that EU citizens have the right to have data erased upon request; and, (3) **Consent:** The consent requirements set forth by the GDPR are extensive. Consent must be freely given, specific, informed, and unambiguous. Additionally, it must be affirmative, “active” consent. Further, consent must be easy to withdraw.

U.S. organizations generally do not provide such broad data privacy rights to their customers/clients.

- **Data Retention:** The GDPR’s “storage limitation” and “data minimization” principles mandate that “the period for which personal data are stored is limited to a strict minimum” (with some narrow exceptions). Personal data can only be stored for as long as it is needed, and then must be deleted or returned. U.S companies could find this requirement challenging in so far as it may necessitate significant changes to existing document retention policies and procedures.

- **Breach Notification:** Under the GDPR, companies must notify EU Data Protection Authorities within **72 hours** of a breach and must notify their customers/clients “without undue delay.” There are two specific challenges here: (1) **Timing:** Most U.S. laws provide as much as 30-45 days to provide notification following a breach. U.S. companies that do not yet have an incident response plan in place will likely find the 72 hour notification challenging; and, (2) **Definition of Breach:** Most U.S. laws require notification if there has been unauthorized “access or acquisition” of PII. Under the GDPR, the scope of what...
constitutes a “breach” is more expansive and includes “the accidental or unlawful destruction, loss, alteration...” of personal data. Accordingly, an incident involving an authorized employee who accidentally deletes or destroys personal data could constitute a breach under the GDPR and thus trigger notification obligations.

U.S. companies that do fall within the scope of the GDPR will likely need to make significant adjustments to their current business practices as respects the personal data they hold.

Fines and Penalties for Non-Compliance
The GDPR sets forth a two-tiered approach to fines and penalties for compliance violations. A significant violation could result in a fine of up to 4 percent of a company’s annual global revenue, or €20 million, whichever is greater. The high-tier violations can be based on failing to obtain appropriate customer consent or failing to allow data subjects to exercise their right to be forgotten. Less serious violations could result in a fine of up to 2 percent of annual global revenue, or €10 million, whichever is greater. The lower-tier violations might include failing to maintain records of customer/client consent or failing to adhere to notification requirements. In either event, the potential fines/penalties for non-compliance are significant.

CONCLUSION
There is no question that the GDPR may have a significant impact on U.S. companies, as well as companies around the world. Given the difference in approach to privacy rights, and the potential imposition of substantial fines, organizations need to carefully review their business activities as respects EU citizens. Significant changes to business practices may be necessary.

U.S. cyber policies are fairly robust. However, many do not necessarily extend coverage to the risks associated with the full range of rights and obligations set forth by the GDPR. In addition, the extent to which GDPR fines/penalties are insurable is an open item, to be determined. Accordingly, careful attention needs to be paid to the precise language in existing U.S. cyber policies for those companies that may be impacted by GDPR to ensure that the scope of coverage is broad enough to capture violations.

ABOUT THE AUTHOR
Kelly Geary is Integro’s Cyber Practice leader in the US. In the insurance industry for over 20 years, she has served as broker, underwriter, insurance attorney and underwriting counsel, as well as a corporate legal and claims executive. Reach Kelly at kelly.geary@integrogroup.com

Contributing author Richard May is a senior broker within Integro’s Cyber Practice.

ABOUT INTEGRO
Integro is an international insurance brokerage and risk management firm. Clients credit Integro’s superior technical abilities and creative, collaborative work style for securing superior program results and pricing. The firm’s acknowledged capabilities in brokerage, risk analytics and claims are rewriting industry standards for service and quality. Launched in 2005, Integro and its family of specialty insurance and reinsurance companies, some having served clients for more than 150 years, operate from offices in the United States, Bermuda, and the United Kingdom. Its U.S. headquarter office is located at 1 State Street Plaza, 9th Floor, New York, NY 10004. 877.688.8701. www.integrogroup.com

This material is for informational purposes only and not for the purpose of providing legal or insurance advice. Insurance coverage, and the terms and conditions relating to such coverage, will vary. No representations or promises are made that any particular insurance coverage will be available to any individual or entity seeking such coverage. Integro is not a law firm and does not provide legal advice. If such advice is needed