GDPR; **EU's** General Data Protection Regulation

5 things to know … Risks / Opportunities

What do U.S. organizations need to do now?

Privacy regulations in the European Union (EU) have long been considered some of the world's toughest, and those laws are now becoming more stringent—even for U.S. organizations.

The EU's General Data Protection Regulation (GDPR), adopted in April 2016, requires all organizations that hold, transmit or process EU resident data to comply with the law—regardless of whether they actually operate in the EU. Learn more at http://www.eugdpr.org

Failure to comply can result in significant financial penalties: up to 4 percent of global revenue or 20 million euro, whichever is greater.

Enforcement is scheduled to start on May 25, 2018.

What do U.S. organizations need to do now?

Here are five key considerations.

1. **GDPR may apply even if you don't have operations in the EU**

GDPR casts a wide net. Companies, government agencies and nonprofit entities that interact with EU residents are all subject to this new law. Many organizations underestimate the amount of EU data they hold and, therefore, may not understand the legislation's potential effect. For example, banks, hospitals, hotels and other organizations that hold data from EU residents are subject to the GDPR. Recent advances in digital communication mean that consumer data can be collected from around the world and stored within seconds in a variety of ways, including websites, email systems, collaboration platforms, mobile platforms and business applications. It is also important to note that the definition of "private data" under the GDPR is much broader than any U.S. regulation and extends, for example, to information such as geolocation data, browser cookies, biometric data or anything else that could be used to identify an individual. To determine if GDPR affects your organization, you need to ask questions such as:

- Do you offer goods and services to EU residents?
- Do you rely on third parties that store or transmit data to or from the EU?
- Do you collect, transmit or process data pertaining to EU residents?

Keep in mind, it doesn't matter if the services are free. It also doesn't matter whether your company operates in the EU.

2. Timing for compliance is sooner than you think

While enforcement isn't set to begin until May 2018, GDPR is already the law of the land in the 28 EU countries. Enforcement agencies have started visiting EU companies to assess compliance and they are expected to do the same in the United States beginning next summer. That doesn't leave much time for organizations to identify what EU data they may hold and how to protect it.

For midmarket companies, time is especially important. Enforcement actions are expected to be taken against midmarket companies first, to make examples of them and set precedent for pursuing actions against larger companies. U.S. companies should be especially alert, as EU regulators look to set the tone for what's expected from them under GDPR, given a historically different—and looser—approach to data privacy between the United States and the EU.

3. Customers can trigger enforcement action

Under GDPR, individuals can request that companies provide all data they maintain about them, and extensive, detailed information about how such data is protected. This includes how each customer's consent is secured and tracked on an ongoing basis; the specific purpose for holding this data; and the nature and extent of protections surrounding that data, including any third parties that might be involved. Consumers can also request that all such data be provided to them in an electronic format suitable for porting to a competitor, or that all their data be completely erased from all systems the company uses, including, again, those from any third parties. Failure to provide timely and complete responses to consumer requests opens companies to formal complaints by consumers to the relevant GDPR supervisory authorities. This, in turn, can trigger the significant penalties mentioned above.

4. Start mapping and analyzing your customer data now

U.S. organizations should begin identifying or "mapping" EU customer data immediately. It is not uncommon for EU data to reside in different departments, divisions or subsidiaries. This data will need to be protected and even segregated from other customer data, much in same way that U.S. organizations now protect and segregate credit card data through network segmentation standards under the Payment Card Industry Data Security Standard. Staff modifications may be necessary—or example, larger organizations will need to appoint a data privacy officer under GDPR.

5. Leverage GDPR compliance as a business differentiator

GDPR represents a broader trend, indicating organizations should prepare for privacy compliance on a global level. U.S. organizations will greatly benefit from assessing and aligning their privacy policies and procedures with this emerging global movement. By doing so, they will not only be able to comply with the requirements of GDPR, but will also be prepared to address additional new privacy laws that may arise from other regions and countries. Instead of looking at privacy compliance as another cost of doing business, organizations should consider it a leading practice that can help them differentiate themselves from competitors.

Note: *(originally published: INSIGHT (August 08, 2017)*