Strategic Perspectives

February 23, 2018

Inside

By *Kelly J. Rooney, J.D., M.P.H.*
Associate Managing Editor

The clock is ticking…Does your organization need to worry about GDPR compliance?

The international data privacy industry is abuzz about the new European General Data Protection Regulation (GDPR) which goes into effect on May 25, 2018. GDPR grants citizens of the European Union (E.U.) more control over their personal data and provides a uniform set of rules to which businesses must abide. Compliance with this law stretches far beyond the borders of the E.U., yet many companies are completely unaware of whether GDPR applies to them or how the law affects its business and the handling of personal data. This Strategic Perspective aims to provoke knowledge of GDPR among U.S. businesses, particularly the data-heavy health care industry.

What is the GDPR?

E.U. Regulation 2016/679, GDPR, protects the processing and free movement of personal data of E.U. citizens by an individual, a company, or an organization. In the E.U., citizens have the right to protect their personal data and to access and correct the data that has been collected on them. For citizens, this means they are provided tools to gain control of their personal data, considered a fundamental right in the E.U. Among the new tools are the right to erasure (the "right to be forgotten") of their data and the right to know when their data has been compromised. For businesses, new opportunities are being provided over data, "the currency of today's digital economy," and the GDPR provides clarity and consistent application of rules. One of the biggest benefits touted by the E.U. is that GDPR provides a "one-stop-shop" for businesses in that they will need only comply with one authority, rather than the authority for each member country.

Personal data protected by GDPR, defined broadly, includes information relating to an "identified or identifiable living individual" or pieces of information which, when pieced together, can lead to the identification of an individual. Personal data includes data that has been de-identified, encrypted, or pseudonymized but can be used to re-identify an individual. (Data is no longer considered personal data when rendered anonymous irreversibly and cannot be used to re-identify an individual.) Some examples of personal data include: names, home addresses, and data held by a hospital or doctor.

Personal health data, under GDPR, includes all data related to the health status of an individual which reveal information about the individual's past, current, or future physical or mental health status. This includes data collected

"in the court of the registration for, or the provision of, health care services, [. . .] information derived from the testing or examination of a body part of bodily substance, including from genetic data or biological samples; and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test."

GDPR's definition of the processing of personal data is broad and applies to both manual or automated processing including "the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of personal data." It applies to both the processors and controllers of personal data.

The reach of the law is potentially world-wide; it applies to companies or entities that process personal data as part of the activities within the E.U. regardless of where the data is processed or a company outside the E.U. offering goods or services or monitoring of individuals' behavior in the E.U.

Failing to comply with data protections rules can lead the Data Protection Authorities (DPAs) overseeing GDPR to issue a warning in the case of likely infringement or, in the case of infringement, a reprimand, temporary or definitive ban on data processing, and/or a fine of up to €20 million (nearly $28 million U.S.) or 4 percent of the company's total annual worldwide revenue. The DPAs will take into account the nature, gravity, and duration of the infringement, whether it was intentional or negligent, actions taken to mitigate damage to individuals, and the degree of cooperation from the organization.

You don't know what you don't know

The uncertainly around the applicability and enforceability of GDPR in the U.S. is rampant just three months before the effective date of May 25, 2018. Joseph Dickinson, partner at Smith, Anderson, Blount, Dorsett, Mitchell & Jernigan, L.L.P., said that one of the biggest misconceptions among U.S. businesses is that GDPR does not apply to them. Stephen Wu, shareholder with the Silicon Valley Law Group, elaborated, saying that the "average business in the U.S. [believes] it doesn't need to worry at all about GDPR ... They don't think it applies to them. Some are right, but many will be wrong."

Regardless of whether a business is aware of GDPR's reach, when it comes to the potential for enforcement actions being brought against U.S. companies, Dickinson noted that many mistakenly believe "that supervising authorities will not be successful in enforcing GDPR against a U.S. company." Wu gave the example that "if [a company has] a breach affecting residents of member states of the European Economic Area (EEA), [it] may find that [DPAs] in Europe want to investigate [it] for possible GDPR violations. Then, [the company] will be surprised to learn that [DPAs] believe [it is] covered."

Does GDPR apply to your business?

The GDPR clearly applies to companies doing business within the E.U. and collecting or processing personal data as part of their activities, regardless of where the data is processed. Things get a big fuzzier beyond that. The E.U. site discussing the requirements provides these somewhat vague details:

- The law also applies to "a company established outside the E.U. offering goods/services (paid or for free) or monitoring the behavior of individuals in the E.U."
- "If processing personal data isn't a core part of your business and your activity doesn't create risks for individuals, then some obligations of the GDPR will not apply to you."

Wu translated this language in a recent blog post titled "Countdown to GDPR Compliance Deadline: May 25, 2018" saying that GDPR applies: (1) when a business is located in the U.S. and "it is offering goods or services to EEA residents while they are located in the EEA" (including analyzing residents' web browsing behavior); and (2) to "businesses processing data for companies collecting personal data in Europe."

What about health care providers?

Wolters Kluwer asked the experts specifically about whether health care providers are subject to GDPR. Dickinson cautioned that "all health care providers should assess the potential applicability of GDPR and document that assessment." He warned, "most health care organizations have not adequately assessed the applicability of GDPR. They believe that they aren't 'doing business' in the E.U. and therefore aren't subject to GDPR."

Wu presented a couple of situations that may confront a health care provider assessing the applicability of GDPR in a blog post titled "GDPR: Long Arm of E.U. Law in the U.S.":

> Let's imagine that you run a local health clinic in San Francisco, California and treat tourists from E.U. member states. Your clinic advertises locally with a simple website that does not monitor visitors' behavior. The business has no locations in Europe and does not market its services in Europe. Is your clinic covered by GDPR? Under the facts given, the clinic is not covered by GDPR. The clinic is located only in San Francisco. It has no European operations. It does not attempt to market its services in Europe. And it is not monitoring the behavior of residents of the E.U.
>
> If we change the facts, though, the result could be different. If the clinic has a branch in the E.U., markets its services to E.U. residents, or monitors the behavior of website visitors, then GDPR applies to it. Any one of those factors would be sufficient to bring the clinic within GDPR. Indeed, any business globally with a website monitoring E.U. residents' behavior is covered. Consequently, the long arm of the E.U.'s GDPR law potentially reaches everywhere.

If you don't know if GDPR applies, what should you do first?

Dickinson suggests that the first thing an organization should do in taking steps toward GDPR compliance is to "do a privacy audit and create a data map so you understand the flow of data into, within, and out of your organization." Wu expanded on this idea in his blog post "Six Steps Towards GDPR (and Other Data Protection) Compliance" saying: "you will need to understand your organization, its business context, its culture, and the types of personal data it processes. You will need to understand in a detailed way what kinds of personal data the business is collecting and receiving, how it uses personal data, its practices in sharing and transmitting personal data, its retention of personal data, and its disposal of personal data. Your business should understand its entire personal data lifecycle and where personal data flow through your business's systems. You need to assess the strengths and weaknesses of your current data protection program. Once you have made this assessment, you can plan future steps to enhance the data protection function within your business. You can then assess its effectiveness and make improvements."

> *"Most health care organizations have not adequately assessed the applicability of GDPR."*
>
> *— Joseph Dickinson*
> *Partner, Smith, Anderson, Blount, Dorsett, Mitchell & Jernigan, L.L.P.*

Tips for health care entities. Polsinelli, P.C.'s Lisa Acevedo, shareholder, and Katie Kenney, attorney and author of Wolters Kluwer's HIPAA: A Guide to Health Care Privacy and Security Law, cautioned that health care entities have long to-do lists to comply with GDPR and "its broad-sweeping changes to data privacy" before the May 25th effective date. Acevedo and Kenney expanded on the other experts' suggestions: "To the extent an organization is already governed by HIPAA, identifying the similarities and differences between HIPAA and GDPR is a helpful starting point given the significant overlap between the two."

Three items on their health care clients' GDPR to-do lists include:

1. Determine if your organization is a data controller or processor or both (the answer significantly

impacts the steps an organization needs to take with respect to GDPR preparedness);
2. Map your data (where is it? how is it being processed? how long is it retained?); and
3. Collect and re-evaluate agreements with data processors and/or sub-processors as applicable (clarify duties and responsibilities in agreements, including, but not limited to, GDPR's new breach requirements and security measures).

For more analysis on whether GDPR applies to U.S. businesses, see *Why and How Europe's New General Data Protection Regulation Impacts US Companies*, December 18, 2017.

If GDPR applies, what could that mean for providers?

Underlying the GDPR is the belief that the processing of personal data is a fundamental right. In order to protect that right, specifically related to health information, some of GDPR's requirements are that:

- Consent for an individual's data to be processed for a specific purpose should to be given by the individual through a clear affirmative act before data is processed.
- It should be transparent to the individual that personal data concerning him or her is collected, used, consulted, or processed, as well as the extent the data is or will be processed. That data is or will be processed must be communicated to the information and communication provided regarding the processing of personal data must be easily accessible and easy to understand.
- As indicated in a blog post by the firm Arent Fox, individuals "have rights with respect to their personal data that may not be available under HIPAA or other U.S. privacy laws, such as the right to erasure."
- GDPR restricts how and when data on E.U. residents can be transferred outside E.U. members' borders. According to Brian Eaton an associate attorney with Taft, GDPR requires that when transferring data to a country not subject to GDPR, "the sending entity must ensure that [the] receiving country has been deemed to have equal or better data protection laws in place. Only a handful of non-E.U. countries currently meet that criteria. You may (or may not) be surprised to learn that the U.S. is not one of them."

Conclusion

There are only three short months before the effective date of GDPR, May 25, 2018, so it is important to take steps to determine if it is applicable to your organization now. Furthermore, Wu warned that "GDPR compliance should be part of an overall compliance effort. If your business focuses on GDPR in isolation, it will likely duplicate efforts and spend more time than it otherwise would if it integrated GDRP with other compliance obligations."