Healthy Habits for GDPR

Good Cyber Hygiene Is Now Required by Law

By Thomas Ciano and Christopher J. Seusing

Thomas Ciano

Christopher J. Seusing

By the time you read this, the most comprehensive and sweeping data security regulation will have just gone into effect. With a May 25, 2018 effective date, the European Union's Global Data Protection Regulation (GDPR) reaches around the globe, including to entities in the U.S. Noncompliance can lead to significant fines of up to four percent of annual global revenue or 20 million euros, as well as civil and even criminal liability.

It is critical for U.S. entities and legal and insurance professionals advising those entities to be aware of the scope of this regulation to determine whether they are subject to it, and to take the necessary steps towards compliance. Even if it is determined that the GDPR is not applicable to your organization, there are a number of practical steps you can take to better your overall cyber hygiene.

What Is the GDPR?

The GDPR is a privacy and data security regulation enacted by the European Union (EU) to protect what it purports is the "fundamental right" to privacy of individuals in the EU. It establishes requirements for any entity that handles or processes the personal data of such individuals for both public or private companies, regardless of size. It also specifies certain rights of individuals to their personal data, including the right to have their data transferred, corrected, or deleted. Compliance is enforced by the 28 data protection authorities (DPAs) of the EU member states, each of which has discretion on how to interpret the GDPR.

U.S. Impacts

With no geographic limitations, the GDPR applies not only to entities located in the EU, but any entity around the world that offers goods or services to individuals in the EU or monitors their behavior (including website "cookies" or other electronic means). Determining whether the GDPR applies to you is not a quick process or cavalier analysis; it requires careful thought about who you collect data from, how you collect it, what type of data it is, what you do with it, and how long you keep it for.

For example, if you have a website in various languages, including those used in the EU, or if you accept EU currency on your website or deliver goods to the EU, then you could be subject to the GDPR. On the other hand, if you have a website that anyone can visit from around the world but is not directly targeted at the EU, then you may not be subject to it.

Similarly, if you are a U.S. retailer, restaurant, or business, and a European tourist visits your establishment and buys something and you process their payment information, it does not necessarily subject you to the GDPR. However, if you also collect that individual's information at the time of the transaction, add them to a marketing or mailing list, and send them information after they return to Europe, then that could subject you to the GDPR. It is crucial, therefore, to determine if you are collecting or processing personal data and what is being done with the information after it's collected.

What Do You Need to Know?

With 99 articles and 173 recitals, the GDPR is a massive regulation that lays out obligations for entities around the world and identifies new rights for individuals in the EU. Some concepts may be familiar to those in the U.S., such as encryption of personal data as a "safe harbor." However, many concepts are foreign and have never before been implemented.

For example, the phrase "personal data" is defined more broadly than here in the U.S., and includes a person's name, email address, and any other piece of information that can identify her, such as an internet protocol address or a website "cookie" identifier. Accordingly, it is important to determine the scope of personal data collected from individuals. If you do have to hold on to personal data, then consider anonymizing it or changing it in such a way that it does not identify the person.

The term "processing" also is very broadly defined as any operation performed on personal data, including collecting, transmitting, and even storing. Processing of personal data is not permitted unless there is a specific lawful purpose to process it, such as the performance of a contract with the individual, other "legitimate interests," or obtaining the consent of an individual. If data is collected only by an individual's consent, then that person must be permitted to later withdraw his consent, and he can request that a copy of his data be transmitted to a third party, corrected, or deleted.

Accordingly, it may be preferable for a company to process

data under lawful grounds other than by consent. For example, an employer collecting personal data of employees in order to effectuate employment, a vendor collecting payment information in order to ship a good, or a hospital collecting personal data of patients in order to provide treatment are all potential lawful grounds to process personal data that do not rely on consent. Individuals cannot prohibit or prevent the processing of their personal data under these circumstances.

One of the tenets of the GDPR is "privacy by design," which encourages privacy and data protection to be implemented at all stages of an organization's processes. When creating or updating information systems, it is advisable to build in privacy considerations. Data minimization is one way to do this. It involves retaining the least amount of personal data necessary for the least amount of time possible. By reducing or deleting the amount of unnecessary personal data, this process also reduces the possibility of a compromise or breach of that data. It is no longer acceptable, or advisable, to indefinitely hold on to archives and databases of personal information if there is no lawful basis to do so.

Another simple step is to limit who in an organization has access to personal data. Does every member of a human resources department really need access to all employee benefits information, or does every member of an IT department really need access to every database of an organization?

The GDPR also provides that any compromise of personal information, such as a data breach, must be reported to the appropriate DPA within 72 hours of discovery. Having an incident response plan in place is crucial so the right people within an organization are notified as soon as possible and the appropriate steps are taken to consult with partners outside the organization, such as insurance professionals, counsel, or other members of a data breach team.

Noncompliance Repercussions

The GDPR empowers the DPAs of the EU's 28 member states to enforce the GDPR. This enforcement can come in many different forms, including the issuance of warnings or public reprimands, the compelled deletion of personal data found not to be in compliance, the temporary or permanent ban on the processing of personal data, and the issuance of fines up to 20 million euros, or four percent of global annual revenue.

For entities that have a presence in the EU, the DPAs can enforce the GDPR directly against them. For those without a presence in the EU, enforcement can still be levied through international law. Individuals who believe their personal information has been processed unlawfully can bring a civil action in the country in which the individual resides or in the country in which the entity has a location (if in the EU). Because there are no GDPR-specific enforcement mechanisms in place against U.S. organizations, it remains to be seen what steps European individuals or DPAs will take to enforce violations of the GDPR against entities here in the U.S.

Additionally, the GDPR requires the appointment of a data protection officer (DPO) for companies that carry out the regular monitoring of individuals on a large scale or the large-scale processing of special categories of data, such as health records. A DPO can be held personally liable either under civil or criminal penalties for noncompliance.

What's Next?

If you determine that your organization is subject to the GDPR, then it is crucial to take steps to evaluate your processes and bring them into compliance. First, identify what information you have, where it is located, and who has access to it. Conduct risk assessments of your IT systems and record retention policies, and ensure that individuals at all levels of the organization and all segments (human resources, IT, marketing, legal, and the C-suite) are aware of and trained on their responsibilities and obligations. Review contracts in place with vendors and other third parties to ensure their compliance, as well as yours, with this new regulation. Create and implement a data breach response team, identifying all necessary parties and steps to take in the event of the inevitable compromise. Finally, evaluate your insurance coverage to determine the scope of coverage for data breach incidents and cyber risk assessments.

Even if an organization is not subject to the GDPR, it can be a catalyst to change practices, procedures, and attitudes towards privacy and data security. This is beneficial not only for an individual's privacy, but also to the relationship between organizations, their employees, and the public. While there may not be comparable national legislation here in the U.S., some states have enacted or are in the process of enacting comparable comprehensive privacy legislation. For example, the New York State Department of Financial Services enacted a cybersecurity regulation last year that requires regulated entities and persons to have cybersecurity policies and an incident response plan in effect, periodically conduct risk assessments, report data breaches within 72 hours, and certify compliance with the regulation. Additionally, the California Consumer Privacy Act will likely appear on the ballot in November 2018, and, if passed, will allow California consumers to find out what personal information is being held by entities doing business in California, instruct such entities not to sell their private information, and recover statutory damages for any violations. It is simply a matter of time before more states enact similar legislation or federal legislation is enacted.

Good cyber hygiene is not merely aspirational, it's a necessity required by law. Compliance with the GDPR can be a crucial step towards maintaining the trust of employees, business partners, and customers in today's digitized world. ■

Thomas Ciano is senior vice president at USI New England. tom.ciano@usi.com

Christopher J. Seusing is partner at Wood, Smith, Henning & Berman LLP. cseusing@wshblaw.com