Tucker Ellis | LLP

COUNTDOWN TO THE GDPR:

What You Need to Know About the Impact of the European Union's New Cybersecurity Measures on Your American Business

By Dan Messeloff, Bill Berglund, and Emily Knight

As concerns about cybersecurity and data privacy weigh more and more heavily on the minds of in-house counsel and corporate executives around the United States, the European Union has initiated expansive new efforts to protect its citizens from cybersecurity risks. The EU's initiative – the General Data Protection Regulation (GDPR) – might ordinarily be viewed with passing interest from American companies, but the reach of the GDPR is actually far broader than any cybersecurity measure ever seen before in either the European Union or in the United States. More importantly, as a result of the reach of the GDPR, millions of American companies may unknowingly be at risk of violating the new law and thus subject to significant monetary penalties. The good news is, whatever your level of interaction with companies and/or individuals in the EU, there are measures you can take to comply with the GDPR.

WHAT *IS* THE GDPR?

On **May 25, 2018**, the GDPR will go into effect. The GDPR grants EU supervisory authorities the power to investigate compliance with the GDPR, issue warnings, and impose administrative fines on entities that violate the GDPR. Additionally, individuals – or "Data Subjects," as they are called by the GDPR – whose information may have been compromised as a result of any such violations may lodge complaints with supervisory authorities or seek a judicial remedy for entities' violation of the GDPR. The GDPR authorizes fines of up to € 20 million (approx. $25 million) or 4% of a company's global revenue, whichever is greater. Individuals who bring claims against entities that are in violation of the GDPR are also entitled to monetary damages.

IS MY COMPANY SUBJECT TO THE GDPR?

Although the GDPR is not the EU's first foray into data protection, the GDPR's vast territorial reach makes compliance with the new data rules particularly challenging for companies in the United States.

At the most basic level, any company in the world that "processes" (including collecting and/or storing) the Personal Data of any individual in the EU will be subject to the GDPR's requirements, and therefore potentially subject to the GDPR's penalties. The GDPR broadly defines the term "Personal Data," and thereby increases the number of entities that will be considered "processors" of such data. The GDPR also creates a whole new set of rights for EU citizens whose Personal Data is being processed or handled, as well as a whole new set of requirements for entities subject to the law. Altogether, these broad new rules mean that a significant number of American companies, organizations, and individuals alike must begin to understand and prepare to comply with the GDPR's requirements.

There are two primary ways a non-EU entity can become subject to the GDPR:

>> ***Entities Offering Goods or Services in the EU.*** Companies that offer goods or services in the EU and handle personal identifiers (such as acceptance of payment by credit cards and e-mail addresses obtained for order confirmations) are subject to the GDPR. For example, a company whose website is merely accessible by EU residents would not bring the company within the jurisdiction of the GDPR, but if the website offers content in the language of the EU resident, accepts Euros or other European currency for payment, or otherwise appears to be targeting EU residents as customers, this would render the company subject to the GDPR.

>> ***Entities with EU "Establishments."*** "Establishments" are subject to the GDPR, although the definition of "establishment" is not clear. The GDPR explains that a Company's activities, conducted "through stable arrangements" is sufficient for a finding of an "establishment" under the GDPR. For instance, if a U.S. company has an EU subsidiary that handles personal identifiers, that U.S. company is likely an establishment subject to the GDPR. Likewise, having even a single sales representative based in and tasked with selling products in the EU will likely be sufficient to constitute an establishment. On the other hand, merely maintaining a computer server in the EU may not satisfy the definition of "establishment" under the GDPR.

An entity must handle individuals' Personal Data to become subject to the GDPR. The GDPR broadens significantly the scope of what constitutes Personal Data, defining it as any of the "information relating to an identified or individual person." Personal Data includes obvious identifiers, such as an individual's name, photos, e-mail address, bank details, and medical information; however, many less-known identifiers, such as login information, VINs, social media posts, and network addresses, also now fall under the GDPR's new definition of Personal Data. Therefore, if any of this information relating to a resident of the EU is maintained by a U.S. company, the company is subject to the GDPR.

MY COMPANY IS SUBJECT TO THE GDPR. WHAT ARE WE REQUIRED TO DO?

The GDPR creates two classes of entities that handle Personal Data: "controllers" and "processors." A "controller" determines the purposes and means of handling Personal Data and is best understood as the entity that is directly collecting the data. A "processor" is an organization that processes data on behalf of the controller.

For example, if a Company A sells machinery to consumers, and it uses Company B to e-mail consumers on its behalf and track consumers' information, then Company A is the data "controller" and Company B is the data "processor." This distinction is important for a number of reasons. The GDPR treats the data controller as the principal party for collecting consumers' consent, managing consent-revoking, enabling right to access, and other functions. A Data Subject who wishes to revoke his or her consent would be expected to contact the data controller (i.e., Company A) to initiate the request, even if such data lives on servers belonging to the data processor (i.e., Company B). The data controller, upon

receiving this request, would then proceed to request that the data processor remove the revoked data from its servers.

Most U.S. entities will become subject to the GDPR by virtue of soliciting and collecting the information of customers in the EU; such activities will make those U.S. entities "controllers;" however, it is easy to "accidentally" become a "processor," such as when a company obtains Data Subjects' Personal Data in connection with a potential transaction, which would cause the company to become a "processor" under the GDPR.

Controllers and processors are each subject to different rules and requirements, some of which overlap. A few key GDPR requirements for controllers and processors follow.

>> ***Controllers Must Have a Lawful Basis for Collecting and Maintaining Data.*** Controllers must make sure that they are collecting Personal Data for only a lawful reason. The GDPR provides a general list of what constitutes a lawful basis, including the performance of a contract, compliance with laws, protecting the interests of an individual or the public at large, or for any other reason that justifies "overrid[ing] . . . the interests or fundamental rights and freedoms of the Data Subject." If a controller has no lawful basis to collect data, the controller may collect personal information after receiving a Data Subject's affirmative consent in response to a specific request for information; however, controllers may store Personal Data only in a form which permits identification for no longer than is necessary for the purposes for which the Personal Data was processed. Therefore, U.S. companies must now be vigilant in reviewing Data Subject information and culling expired information.

>> ***Controller and Processor Data Protection Requirements.*** The GDPR requires all controllers and processors to implement appropriate organizational safeguards to ensure that any processing of Personal Data is in compliance with GDPR rules and to ensure a level of security appropriate to the risks posed by the data. Such safeguards may include conducting audits of data privacy systems, impact assessments, contractual provisions that ensure that third-party vendors are adequately maintaining the privacy of such data, and similar protections.

>> ***Contractual Relationships Between Controllers and Processors.*** Controllers are permitted to contract only with processors that provide sufficient guarantees, by written contract, that such processors will implement appropriate technical and organizational measures that satisfy all of the requirements of the GDPR. The GDPR prohibits a processor from processing Personal Data in violation of the controller's instructions.

>> ***Controller and Processor Data Breach Notification.*** In the event of a data breach, controllers must notify a supervisory authority within 72 hours of becoming aware of the breach. If the data breach results in a "high risk" to the rights and freedoms of natural persons, the controller must notify the affected Data Subjects "without undue delay." Likewise, processors are required to notify a controller of a data breach "without undue delay." The GDPR is not helpful in determining what constitutes "undue delay," failing even to explain whether undue delay is longer or shorter than 72 hours. Nevertheless, the key takeaway for U.S. companies is that the GDPR sets a new precedent for breach response timeframes, and U.S. companies must be prepared to respond rapidly to a data breach or risk violating the GDPR.

>> ***Controller and Processor Recordkeeping.*** Controllers must maintain documentation of their recordkeeping and processing activities. It is helpful to think of the documentation as a biography of the data collected by the controller that can be read and understood should the controller be audited or accused of violating the GDPR. The documentation must include (1) the individuals responsible for the controller's data retention systems, (2) a description of how and why the data was collected and when and where the data was ever disclosed or otherwise transferred, and (3) the anticipated date for destruction of the data.

>> ***Data Protection Officers.*** In certain circumstances, controllers and processors may be required to retain a Data Protection Officer to serve as an expert on the GDPR. The Data Protection Officer may be an individual from outside the entity or may be an internal candidate. A Data Protection Officer must be designated when a public authority processes the Personal Data

(i.e., if your U.S. company submits tax returns or licenses information to EU authorities); the controller's or processor's activities necessitate regular, systematic processing of Data Subject information; or a controller or processor is handling highly sensitive Personal Data as identified in the GDPR.

>> ***Designated Representatives.*** If a non-EU controller or processor consistently handles Data Subjects' Personal Data or highly sensitive data, then such controller must designate an additional representative in one of the member states where the Data Subjects' Personal Data is obtained in connection with the offering of goods or services or where such Data Subjects' behavior is monitored.

Furthermore, when an EU citizen has personally identifiable information taken from them, he or she becomes a "Data Subject" under the GDPR. Once an individual becomes a Data Subject, he or she retains a set of rights, which companies must be prepared to follow, thereby imposing upon U.S. companies still further obligations.

These rights include:

>> ***The Right to Be Informed and to Access.*** Data Subjects have a right to know who handles their data and a right to receive, at the time the data is collected, information about their data, including the length of time the data will be held, the right to erase the data, and whether the data collector intends to share the information.

>> ***The Right to Erasure/Right to Be Forgotten.*** Data Subjects have the right to demand the erasure of Personal Data without undue delay in certain circumstances.

>> ***The Right of Rectification.*** Data Subjects have the right to demand that their personal information be corrected or supplemented if it is found that an entity is maintaining inaccurate or incomplete information about the Data Subject.

WHAT SHOULD I DO *RIGHT NOW* TO COMPLY WITH THE GDPR?

U.S. companies that are subject to the GDPR should take immediate steps to make sure they will comply with the new law. While the GDPR sets forth a long and complex list of requirements, a few simple actions can go a long way in ensuring GDPR compliance. Instead of considering all of the GDPR compliance requirements, U.S. companies would be well-served to consider some of the more fundamental aspects of the GDPR when deciding how to comply with the law.

1. Review Your Data Retention Policies.

U.S. entities should begin reviewing their data retention policies. Although recent high-profile data breaches have caused many companies to improve their data retention policies, the GDPR includes requirements that may be more intensive than current best practices. For example, the GDPR's requirement that data must be stored for a limited amount of time and be deleted once it is no longer needed is burdensome, costly, and completely new to U.S. companies. Many U.S. companies have policies to keep certain types of records much longer than when "no longer needed," which, in the absence of a legal requirement, may violate the GDPR. By the same token, such companies might not have any policy regarding the retention or destruction of other categories of Personal Data that are completely new. As such, companies should review and understand exactly what they are retaining and what they are destroying, as well as when and why they are doing so.

2. Be Aware of the Expanded Scope of "Personal Data."

The GDPR's definition of Personal Data greatly expands the universe of data that is considered personal information and should give even the most vigilant data hawks cause for concern. For instance, the GDPR suggests that website "cookies," the small bits of information that are collected and stored to preserve website users' login information, is Personal Data. All U.S. companies that may be subject to the GDPR should take a long look at the information they are gathering and seriously review whether they are already collecting Personal Data from Data Subjects in the EU.

3. Be More Prepared Than Ever Before for Potential Data Breaches.

The GDPR's new 72-hour breach notification rule has already proven to be one of the most concerning aspects of the GDPR. The GDPR greatly reduces the amount of time that U.S. companies will have to respond to a data breach that affects Data Subjects, and it is not clear if it is even feasible to isolate, understand, and provide

authorities a notification of a data breach within 72 hours. By way of example, in December 2017, several U.S. senators proposed a data breach disclosure rule that would require companies to disclose a data breach within 30 days of a breach. Even then, many U.S. data breach experts argued that 30 days was far too arduous.

4. Revise Your Outward-Facing Privacy Policies and Notices.
The GDPR creates a whole new set of requirements to lawfully obtain individuals' Personal Data, including notice requirements about what information will be collected and how that information will be handled. U.S. companies should consider how the GDPR's scope and consent requirements affect how such companies interface with consumers, including:

>> ***Personal Data.*** The broadening scope of Personal Data means more individuals will become Data Subjects, which in turn means that U.S. companies must undertake an increased burden to obtain consent to use their information.

>> ***Consent to Collect Personal Data.*** The GDPR's consent requirements will prove to be yet another significant burden for U.S. companies. The GDPR requires entities to make a clear request to collect Personal Data and requires Data Subjects to clearly affirm their consent. While obtaining an affirmative consent might be easy for companies that operate solely in the EU, consider a U.S. company with a website that collects Personal Data: Will that company require all of its visitors to affirmatively consent to the GDPR requirements, regardless of their location? If so, does the consent provide all users, even non-EU users, the rights and privileges established under the GDPR?

>> ***Data Subjects' Control Over Personal Data.*** Along the lines of data retention, U.S. companies that are subject to the GDPR will need to stay vigilant to ensure that Data Subjects' requests are received and satisfied. On a practical level, U.S. companies will need to make sure that an individual who can field and respond to Data Subjects' requests is in place.

5. Ensure That Your Third-Party Providers Are Complying With the GDPR.
The GDPR will make U.S. companies more accountable to their third-party data handlers. The GDPR's system of self-policing between data collectors and data handlers is analogous to the "Business Associate" requirements found in the Health Insurance Portability and Accountability Act (HIPAA), so many U.S. companies may already be prepared to ensure that their third-party vendors are in compliance with the GDPR. Even if your company

has proper procedures in place to comply with HIPAA, it will still be necessary to review all third-party vendors your company deals with because the scope of "Personal Data" under the GDPR is much broader than "Protected Health Information" under HIPAA.

6. Educate Your Upper Management.

Compliance starts at the top of every organization, so directors and managers should undertake a review of their company's policies and procedures. Many executives and directors mistakenly believe data protection requires some sort of advanced skillset; however, the first steps to satisfying the duty of care with respect to data security are well within a management team's capabilities and often begin by asking a few basic questions of their IT Department. Additionally, a director's fiduciary duty likely extends to ensuring that the company institutes sufficient data protection programs and policies. A director's duty of care requires that the director act in a thoughtful and informed manner. Courts recognize that a director's ongoing failure to exercise oversight of the company (for instance, a failure to institute a reporting system to keep the board apprised of company developments) is a breach of the duty of care. Given the recent attention to and increased understanding of the harmful effects of data breaches, directors now almost certainly have a duty to ensure that their companies are prioritizing data security. In this respect, the GDPR presents an opportunity, if not an immediate need, to review your company's data security policies and procedures.

7. Review Your Existing Cybersecurity and Data Privacy Policies (and Add Some New Ones).

Most U.S. companies recognize the increased scrutiny of their cybersecurity and data privacy policies, and many have already taken steps to improve such policies. GDPR or not, every single company that deals with individuals' data should have data security policies and procedures in place. If your company does not currently have data security policies and procedures, you should consider taking immediate steps. If your company already has data security policies and procedures, it is time to take out those policies and review them to ensure compliance with the GDPR and that they reflect the realities of the current data security climate.

8. Audit Your Data Security Procedures.

In addition to reviewing your company's policies, you should consider conducting a data security audit. Such audits typically include a review component, including investigating how your company obtains, uses, and maintains Personal Data, and a review of contracts with third-party vendors to establish a good-faith effort to ensure that your vendors are properly handling individuals' personal information. The most successful data security audits also include a preparedness component, where key executives and employees of the company meet and review the company's data breach policies and then practice data breach scenarios, including how to properly respond to a data breach and how to provide adequate notice to the proper authorities.

9. Think About Your Customers.

Of all the GDPR rules, the requirement to obtain consent to collect data is probably the most unique and difficult to address. To make matters worse, while the GDPR creates the arduous requirement of obtaining consent, the law is short on just how a company can obtain such consent. U.S. companies should begin considering the method they will use to obtain consent from customers in the EU to collect their information. Crafting proper consent procedures will likely be time consuming, so companies should not delay in considering how to comply with the new law.

TUCKER ELLIS CYBERSECURITY TEAM

When the GDPR goes into effect in May 2018, it will be a whole new world for thousands of companies and millions of individuals in the United States and the EU. Tucker Ellis is here to help you navigate these new requirements.

For more information, please contact any member of our Cybersecurity Team:

Daniel Messeloff (certified)
216.696.5898
daniel.messeloff@tuckerellis.com

Robert Hanna
216.696.3463
robert.hanna@tuckerellis.com

Ann Caresani
216.696.4788
ann.caresani@tuckerellis.com

Robert Cutbirth
415.617.2235
robert.cutbirth@tuckerellis.com

William Berglund (certified)
216.696.2698
william.berglund@tuckerellis.com

Paul Janowicz
216.696.5787
paul.janowicz@tuckerellis.com

Emily Knight
216.696.4893
emily.knight@tuckerellis.com

Tucker Ellis | LLP

CHICAGO CLEVELAND COLUMBUS HOUSTON LOS ANGELES SAN FRANCISCO ST. LOUIS | tuckerellis.com