Even If You Are a U.S. Company, Don't Ignore the GDPR:
Complying with the EU's New Data Privacy Law

On May 25, 2018, the European Union (EU)'s General Data Protection Regulation (GDPR) comes into force, broadening the scope of privacy obligations for companies doing business in or with Europe. The GDPR applies to all businesses that collect and use personal information of EU residents, including organizations located outside the EU.

U.S. companies, including Data Processors in the United States, may be subject to the GDPR if they offer products or services to EU residents or if they monitor the behavior of such residents even if they do not have a physical presence in the EU.

Below is an overview of GDPR as well as a GDPR Readiness Checklist to help companies prepare for their compliance obligations.

Background

The GDPR replaces the EU's Data Privacy Directive (Directive), adopted in 1995. The Directive established a privacy regime centered on the protection and rights of the individual to control how his/her personal data is collected is used. The Directive was not actually binding on the Member States. Instead, it required that each Member State enact its own national data privacy law consistent with the Directive by the end of 1998. However, these national privacy laws proved not to be consistent, both as enacted as well as enforced by the Member States' Data Protection Authorities (DPAs).

The GDPR, adopted in April 2016 with a two-year implementation period until May 25, 2018, seeks to remedy some of the flaws in the Directive. For example, the GDPR is a regulation, as opposed to a directive, and is therefore automatically applicable as internal law in each and every Member State. Accordingly, there is no requirement that Member States enact their own national data privacy law incorporating the GDPR. Member States, however, will need to revise their current privacy laws in order to supplement the GDPR in areas that are not finally settled by the GDPR, hence the importance of monitoring legal developments at both the EU and national level in the months leading up to the effective date of the GDPR this May.

The intent of the GDPR is to establish a single set of privacy rules across the EU, thus harmonizing data privacy protections in the Member States and making compliance easier. Enforcement, however, will remain with the Member States. The GDPR provides that each Member State is to establish an independent Supervisory Authority (SA) to investigate complaints and conduct other enforcement actions. Where an entity has multiple locations in the EU, the SA in the Member State where the entity has its "main establishment" will be the lead enforcement authority, acting as the "one-stop-shop" overseeing that entity's data processing activities throughout the EU.

Member States also will retain primary jurisdiction over certain privacy issues that are not addressed or finally settled by the GDPR. While entities operating in the EU must take steps to comply with the GDPR, companies looking to comply with EU laws will also need to consider

Member State laws or regulations that are adopted in conjunction with or as a supplement to the GDPR.

Finally, the GDPR does not affect the current ePrivacy Directive, adopted in 2002, and which addresses the processing of Personal Data by providers of electronic communications services, such as Internet Service Providers. (The ePrivacy Directive is informally known as the "Cookie Law" as it requires, among other things, that EU businesses post a notification and obtain user consent if they use cookies on their websites.) While the EU has initiated a review of the ePrivacy Directive to make it consistent with the GDPR, this effort is not expected to be completed by May 25. Like the GDPR, the expectation is that the updated ePrivacy Directive will also be an EU-wide regulation and will therefore not require that Member States implement their own consistent national laws.

Key Provisions/Key Changes in the GDPR from the 1995 Directive

The GDPR seeks to strengthen the ability of EU residents (Data Subjects) to be informed about and control what data is collected about them and how it is used. The definition of Personal Data under the GDPR is even broader than the Directive: "[P]ersonal data is any information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, a home address, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer's IP address."

Moreover, Data Controllers (the entities that collect the Personal Data from an EU resident and control how it is used) and Data Processors (the entities that process Personal Data on behalf of Data Controllers) must provide individuals "access" to information about what Personal Data is collected about them and how it is processed. In certain cases, the individual is entitled to request that their Personal Data be "erased" from the records of the Data Controller and Data Processor.

Below is a summary list of other important changes and requirements found in the GDPR:

- **Consent** -- Companies must get affirmative consent to process the personal information of individuals. Consent must be "freely given, specific, informed and unambiguous." For example, an individual's failure to click an "opt out" box, by itself, is not valid consent. Consent must also be reversible, and specific to each type of data processing.

- **Internal Compliance** -- Businesses will need to implement comprehensive, EU-compliant data protection compliance programs and then be able to provide evidence of these programs to EU data protection authorities, if asked.

- **Built-In Privacy** -- New products and services must encompass "Privacy-by-Design" or "Privacy-by-Default" concepts when personal information is to be collected. In addition, a Data Privacy Impact Assessment (DPIA) may be required to work out risks inherent in new products or in connection with certain activities, and appropriate security and other protections would need to be implemented based on that risk assessment.

- **Data Breach Notification** -- The GDPR imposes notification requirements for data breaches. Businesses will have only 72 hours to notify data protection authorities, and, in certain circumstances, affected individuals, after a data breach. They must also implement a specific data breach response and mitigation plan.

- **Individual Control** -- Businesses must be responsive to requests from individuals to know what personal information is collected about them and how it is being used; and individuals may object to the use of their personal information for "profiling," and request that their information be deleted (under certain circumstances).

- **Data Privacy Officers (DPOs)** – Depending on the nature of their business, non-EU companies may need to appoint a Data Privacy Officer.

- **Data Processor Obligations** – The GDPR imposes new requirements on Data Processors to implement security protections, keep records on their data processing, appoint an internal DPO (if necessary), facilitate responses to requests by individuals about what Personal Data is collected, comply with cross-border data transfer requirements, and notify Data Controllers of a data breach. Data Processors are directly liable under the GDPR for failing to comply with these requirements.

- **Increased Penalties** -- The GDPR includes significantly increased penalties for violations, with fines as high as €10M or 2% of annual worldwide revenue, or €20M or 4% of annual worldwide revenue, depending on the type of violation.

U.S. Companies

In addition to determining whether a U.S. Company is subject to GDPR, even if it has no physical presence in Europe, another important consideration for U.S. companies is whether they are involved with the cross-border transfer of EU residents' Personal Data from the EU to the U.S. for processing. The GDPR retains the 1995 Directive's prohibition against such transfers to any countries that lack "adequate" data protection law. The EU previously determined that United States' laws do not provide adequate data protection, and the GDPR does not change that determination. As a work-around mechanism, in 2016 the EU and U.S. entered into the "Privacy Shield Framework," in which U.S. companies self-certify with the U.S. Department of Commerce that they will comply with EU data protection requirements for Personal Data of EU residents that is transferred to the U.S. for processing.

Be advised, however, that self-certification is not a substitute for complying with the GDPR. The Privacy Shield only addresses the issue of the transfer of the Personal Data from the EU to the U.S. for processing. Self-certifying compliance with EU law under the Privacy Shield means a US company also will have to comply with the GDPR when it becomes law in May 2018.

GDPR Readiness Checklist

Companies should be prepared for the May 25, 2018 implementation of GDPR, and compliance efforts should be underway or begin as soon as possible. The expanded breadth of the GDPR implicates a comprehensive review of current data privacy practices, policies and procedures of

covered organizations. We provide this checklist to highlight those areas in the GDPR that will see the most significant changes from current EU data protection requirements:

___ **Confirm data footprint in EU** – Start by identifying and mapping data flows (document what data is collected, from whom and from where, how it is processed, how long is it retained and why, and to which third parties is it disclosed and why). Determine if fewer categories of data should be collected and processed given the purpose(s) for which the Personal Data is being collected.

___ **Update customer-facing privacy policy** – GDPR requires companies to obtain "express consent" from individuals whose Personal Data is collected, which means users must affirmatively agree – either by statement or a "clear, affirmative action." Pre-clicked boxes will not be sufficient under the GDPR. Privacy policies – and actual practices -- must reflect this updated requirement.

___ **Update vendor agreements** -- Review current vendor agreements for data protection terms and update to include GDPR requirements.

___ **Update processor agreements** – Review current processor agreements to ensure that the specific elements for these agreements as set forth in the GDPR are included.

___ **Determine if a Data Privacy Impact Assessment is necessary** – A formal Data Privacy Impact Assessment (DPIA) is to be conducted where the data processing presents "high risks to the rights and freedoms" of the individuals whose Personal Data is collected. A DPIA, moreover, is required where data processing includes profiling of individuals, large-scale processing of "special categories" of Personal Data, or there is large-scale and systematic monitoring of a public area.

___ **Implement "Privacy by Design"** – "Privacy by Design" (also known as "Privacy by Default") means taking steps to ensure that, by default, when developing a new product that involves data collection and processing, the data practices must be the minimum necessary for the intended purpose. In addition, organizations must implement appropriate technical and non-technical protections for Personal Data they collect.

___ **Appoint a Data Protection Officer (if required)** -- Data Controllers and Data Processors are required to appoint an internal DPO if they "core activities" include data processing that involves "regular and systematic" monitoring of individuals or large-scale processing of certain "special categories" of Personal Data.

___ **Create/update procedures for processing user access requests and complaints** – Organizations must implement internal procedures to respond to individual's requests and complaints regarding how their Personal Data is collected and processed. Under certain circumstances, the individual may be in a position to direct that his/her Personal Data be deleted.

___ **Review and update data breach response policy and procedures** – Organizations must ensure that their Data Breach Mitigation Plan is updated to reflect the GDPR requirements.

___ **Review and update record keeping procedures and policies** – Data Controllers and Data Processors must keep detailed records of their data processing activities.

___ **Develop a cross-border transfer strategy (if implicated)** -- Data Controllers and Data Processors must comply with cross-border transfer restrictions if Personal Data is sent outside the EU for processing. For example, U.S. Data Processors can self-certify under the EU-U.S. Privacy Shield Framework to authorize transfers of Personal Data from the EU to the United States for processing.

___ **Conduct employee training on new requirements, processes and procedures and update employee guidance and policies –** Educate and train employees on new GDPR privacy protection requirements and processes. In addition, employee guidance and policy materials should be updated to reflect the GDPR requirements.

___ **Periodic employee monitoring and security checks for compliance** – Conduct periodic reviews of employee practices and security protections to confirm compliance with GDPR requirements.

Outside GC is well positioned to assist you with determining how to comply with the GDPR. Our team includes U.S. and EU-trained attorneys experienced with data privacy requirements in the EU and well versed in the new obligations imposed by the GDPR as well as other data privacy laws and regulations in individual EU Member States not covered by the GDPR. We are also experienced with obtaining self-certification under the EU-U.S. Privacy Shield Framework for cross-border data transfers.

Stephan Grynwajc served as a senior in-house attorney for several blue-chip technology corporations (e.g., Intel and Symantec) in France, the U.K. and the U.S., and today, focuses his practice on advising U.S.-based clients on navigating the EU privacy landscape.

Mark Johnson has over 20 years of experience advising clients on data privacy regulations and public policy, and is a former member of the Data Privacy practice group at the international law firm, Squire Patton Boggs in Washington D.C.

Lakshmi Sarma Ramani served as the lead global attorney for privacy matters at The Nature Conservancy, where she also managed a wide range of legal and regulatory compliance matters, including cybersecurity, tax, finance, technology, marketing, membership and fundraising.

We would be happy to discuss your specific needs. Feel free to reach out directly to Stephan (Stephan@outsidegc.com), Mark (mjohnson@outsidegc.com) or Lakshmi (lsramani@outsidegc.com), or request more information by visiting our Contact Us page.