Tick-tock: GDPR enforcement is less than 9 months away

| Tuesday, September 5, 2017

This high-level overview is the first in a 3-part series examining the Global Data Protection Regulation. Stay tuned for future insight on the key differences between the GDPR and current directives and on what GDPR enforcement you can expect.

Does your business operate in the European Union (EU)? Do you have customers or employees residing in the EU? Have you heard of the Global Data Protection Regulation (GDPR)? If you operate overseas but have not yet focused compliance efforts on the GDPR, the time to start is now. The GDPR's enforcement date is May 25, 2018.

What is the GDPR?

The GDPR is an omnibus data protection regulation that replaces the European Data Protection Directive 95/46/EC. The GDPR relates to the processing of "personal data." Personal data means any information related to a natural person (a "data subject" in GDPR parlance) that can be used to directly or indirectly identify the person. This includes name, photo, email address, bank details, posts on social networking websites, medical information, or computer IP address. The GDPR also includes specific provisions for sensitive personal data, or "special categories of data," which includes passwords for access to IT systems and websites, credit card details, Social Security numbers, passport numbers, and genetic and biometric data. The processing of data includes collecting, using, storing, disclosing, and discarding.

Who must comply with the GDPR?

The GDPR applies to all companies processing personal data of data subjects residing in the EU. Specifically, it applies to organizations located within the EU, as well as organizations located outside of the EU if they offer goods or services to, or monitor the behavior of, EU data subjects.

Entities subject to the GDPR are called data controllers or data processors, and different rules apply whether you are a controller or a processor. In theory, the distinction between a data controller and a data processor seems simple enough. A data controller determines the purposes, conditions and means of the processing of personal data. A data processor processes personal data on behalf of the controller. In practice, though, relationships between entities and their subsidiaries, partners, vendors, and suppliers are exceedingly complex, making it sometimes difficult to determine who is the controller and who is the processor. And, to further complicate the issue, the way in which an entity processes personal data might make it both a data controller and a data processor.

What does the GDPR require?

The GDPR is dense and includes many requirements, both for data controllers and data processors. This alert provides a high-level review of some of the requirements of data controllers. This list is not comprehensive – but we will be providing more detailed information on these and other aspects of the GDPR in future alerts.

Data protection principles and data protection by design

The GDPR codifies the data protection principles and requires that personal data be processed:

- In a manner that is lawful, fair, and transparent.
- Only for the purpose for which it was collected.
- Only in an amount that is necessary to fulfill the stated purpose.
- In a manner that ensures its accuracy.
- Only for a duration of time which is necessary for the stated purpose.
- In a manner that protects its integrity and confidentiality.

The last principle is accountability – data controllers must demonstrate the specific manner in which they meet the other data protection principles.

The GDPR requires data controllers to bake data protection into all aspects of the processing of personal data. This “data protection by design” concept is nothing new, but what is important here is that a data controller is required to implement safeguards that directly address the risks it faces in order to comply with the data protection principles. Measures that meet the principles of data protection by design could include:

- Data minimization
- Pseudonymization
- Transparency
- Allowing individuals to monitor processing
- Creating and improving security features on an ongoing basis

Consent from data subjects

All personal data must be processed, according to the first data protection principle, in a manner that is

lawful, fair and transparent. To meet this principle, a data controller is required to process data under certain enumerated conditions, one of which is processing only after obtaining consent from the data subject. The definition of consent in the GDPR is any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. Consent cannot be inferred by silence or through the use of pre-selected check boxes; it must be explicit, opt-in consent.

Appointment of a Data Protection Officer

Data controllers are required to appoint a Data Protection Officer (DPO) if they carry out large-scale systematic monitoring of data subjects or carry out large-scale processing of special categories of data. The DPO advises the data controller of its obligations to comply with the GDPR, monitors compliance, and acts as the point of contact for regulatory authorities and/or data subjects. Depending on the size of the organization, a data controller might appoint one DPO, or it might appoint several that operate in different EU jurisdictions.

Honoring a data subject's right to be forgotten

A data subject has the right to request that a data controller erase that data subject's personal data from its records. This right of erasure, or right to be forgotten, is not absolute. The data controller is only required to erase the data in certain circumstances, namely that the:

- Data is no longer necessary for the purpose it was collected
- Data subject withdraws consent
- Data subject objects to the processing and there is no legitimate interest for continued processing
- Data was unlawfully processed in the first place
- Data must be erased to comply with a legal obligation
- Data is processed in relation to online services to a child

This right to be forgotten exists in the GDPR to allow data subjects to take control over their own data when there is no compelling reason for that data to be held. A data controller can refuse to erase the data if the personal data is processed for public health purposes in the public interest, to comply with a legal obligation, or in the exercise or defense of a legal claim, among other reasons.

Data breach notification

The GDPR requires entities that suffer data security breaches to notify the relevant Data Protection Authority within 72 hours of discovery and to notify the affected data subjects without undue delay. In the United States, there is no general federal data breach notification law. Instead, whether notification is necessary depends on the state of residence of the affected individual and/or what information was compromised. There are 48 state data breach notification laws, and notification requirements for the compromise of protected health information under the Health Insurance Portability and Accountability Act (HIPAA). Data breach notification in the EU is a new requirement. The already onerous requirement in the United States will now be further complicated by this GDPR requirement.

Why should I worry about complying with the GDPR?

In a word: penalties. The GDPR authorizes penalties of up to 4 percent of revenue (or "global annual turnover") or €20 million, which is approximately $23 million. Those penalties are reserved for the most egregious violations of the GDPR, but there are tiered penalties for other violations. For example, a company can be fined 2 percent of its global annual turnover for failing to notify affected individuals in the

event of a data security breach.

How should my company comply with the GDPR?

Compliance requires more than just writing and adopting an internal policy. When embarking on any kind of data protection compliance project, the first step is almost always conducting an analysis of what data you collect and use, how and where it is stored, with whom you share it with, and how it is discarded when no longer needed. This data mapping is essential. Without a clear picture of how data flows to, from, and within your environment – whether your environment is a sophisticated network or a single computer – you will not be able to fulfill the other requirements of the GDPR.

After the initial data mapping is complete, a data controller should assess its current policies and procedures for processing personal data and make necessary adjustments that are in line with the data protection principles. A data controller should assess whether it needs to appoint a DPO. Further, a data controller should analyze the manner in which it obtains consent from data subjects, and make changes to that process as needed.

When was the GDPR passed and when should I start to worry about complying?

The European Commission began its reform process in 2012. On Dec. 15, 2015, the European Parliament, the Council and the Commission reached agreement on the new data protection rules. On April 14, 2016 the European Parliament adopted GDPR. The official text of the GDPR was published on May 4, 2016 with an effective date of May 24, 2016. The text gives entities covered by the GDPR two years to comply. The enforcement date is thus May 25, 2018.

Large data controllers that process personal data on a significant number of EU residents may have began addressing compliance as soon as the GDPR was officially adopted. Smaller data controllers may just be learning about the GDPR now and thinking through whether the regulation applies and how to comply. Because compliance is a process that includes data mapping and engaging in data protection by design, every entity that processes personal data on EU residents should start compliance efforts now.

For questions regarding the GDPR, please contact one of the data privacy and cybersecurity attorneys listed below.