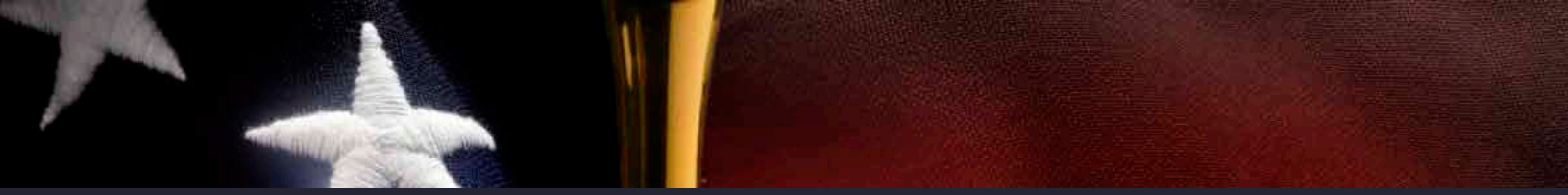

U.S. Companies Still Grappling with GDPR

Prepared by:
Anjali Das
Wilson Elser

LORMAN®
Published on www.lorman.com - November 2018

INTRODUCING

Lorman's New Approach to Continuing Education

ALL-ACCESS PASS

The All-Access Pass grants you UNLIMITED access to Lorman's ever-growing library of training resources:

- ☑ **Unlimited Live Webinars** - 120 live webinars added every month
- ☑ **Unlimited OnDemand and MP3 Downloads** - Over 1,500 courses available
- ☑ **Videos -** More than 1300 available
- ☑ **Slide Decks -** More than 2300 available
- ☑ White Papers
- ☑ Reports
- ☑ Articles
- ☑ ... and much more!

Join the thousands of other pass-holders that have already trusted us for their professional development by choosing the All-Access Pass.

Get Your All-Access Pass Today!

SAVE 20%

Learn more: www.lorman.com/pass/?s=special20

Use Discount Code Q7014393 and Priority Code 18536 to receive the 20% AAP discount.

*Discount cannot be combined with any other discounts.

U.S. Companies Still Grappling with GDPR

Written by Anjali C. Das 8-21-18

Several months after the European Union's (EU's) new sweeping privacy law known as the **General Data Protection Regulation** (GDPR) went into effect on May 25, 2018, U.S. companies are still struggling to understand the implications for their businesses. This article highlights some of the key threshold issues that companies should consider in analyzing the potential impact the GDPR may have on their operations, including restrictions on the collection and use of personal information of EU residents.

What Is the GDPR?

The GDPR (or Regulation) is perhaps the most comprehensive privacy law of its kind in the world, emphasizing the growing social, political and legal concerns about the potential misuse and abuse of individuals' personal data. This is no surprise given the rapid advances in technology and the impact of the new economic reality of "big data" and data analytics on consumer information.

The GDPR has set a new precedent for the high stakes of protecting individuals' privacy, which is being watched closely and even shaping the privacy laws in other countries. The GDPR replaced the Data Protection Directive of 1995 and sets stricter standards for companies that collect or process data on citizens and residents of EU member countries. While considered a milestone achievement for individuals' data protection laws, the GDPR presents complex challenges for companies that must now take steps to become GDPR compliant or run the risk of being subject to audits, lawsuits and/or stiff financial penalties.

Which Organizations Are Subject to the GDPR?

There is a big misconception in the U.S. business community that the GDPR only applies to EU companies. The new Regulation expands the territorial reach of the GDPR to include companies established outside

the EU. This means that a company that has no offices, staff or even customers in any EU country may nonetheless need to comply with the GDPR if it processes and stores personal data on EU residents in any way. In other words, U.S. companies may be subject to the GDPR if they control or process data of EU residents.

The GDPR focuses in particular on the activities of data "controllers" and data "processors." A data controller is an individual or entity that "determines the purposes and means of processing personal data." A data processor is any individual or entity that processes (*i.e.*, collects, stores, uses) personal data at the direction of the data controller. A positive response (yes) to one or more of the questions below may signal that an organization is subject to the GDPR.

Does your organization process or store data on EU residents?
The GDPR broadly defines the term "data processing" to include "collection, recording, organization, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment, combination, restriction, erasure or destruction." In reality, virtually any activity involving personal data of EU subjects may be closely scrutinized and classified as a processing activity within the definition of the Regulation, to the extent it is performed at the request of a data controller.

Does your organization offer goods or services to EU residents?
The GDPR expressly states that the Regulation applies to organizations outside the EU that offer goods or services to data subjects within the EU regardless of whether a fee is charged for such goods or services. Thus, an organization should consider whether it:

- Offers services in a language or currency of a EU member state
- Enables EU residents to place orders in such other language
- References EU customers in its publications.

It is noteworthy that merely having a website that is accessible by EU residents is not conclusive for purposes of determining whether an organization is subject to the GDPR.

Does your organization monitor the behavior of EU residents as that behavior occurs in the EU?
The GDPR also applies to non-EU organizations that monitor the behavior and activities of EU residents within the EU. This includes tracking EU residents on the internet to create profiles or to analyze or predict individual preferences and behavior.

What Is Protected Personal Data Under the GDPR?
The GDPR protects "personal data," which is broadly defined in Article 4(1) to encompass:

"…any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier…"

The definition provides a broad range of identifiers, including "a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." For example, personal data may include a photo, racial or ethnic data, an email address, bank details, posts on social networking websites, political opinions, health and genetic information, a computer IP address and so on.

The GDPR also refers to sensitive personal data as "special categories of personal data," which include genetic data and biometric data, where processed to uniquely identify an individual, and data concerning health. Processing of such data is prohibited unless the data subject gives explicit consent. Otherwise there are very few exceptions in which processing of such special categories of personal data also is possible (*e. g.*, if it is necessary to defend or enforce a legal claim).

When a data controller collects personal data from an individual, including a third party, the controller must provide information to the data subject regarding processing activities, including:

- Contact information for the controller and Data Protection Officer, if applicable

- Purpose of the collection and processing of personal data
- Intended recipients of the personal data, if any
- Whether personal data will be transferred outside the EU
- Time period for which the personal data will be stored
- Individuals' right to request access to, correction or erasure of their personal data
- Individuals' right to file a complaint with an EU privacy regulator (Supervisory Authority) with respect to the collection or use of their personal data.

What Are Consent Requirements for Processing Personal Data?
Consent remains one of six lawful bases to process personal data, as listed in Article 6 of the GDPR. However, the requirements for validly obtaining consent have been increased to place a higher burden on data controllers. Article 7 sets out what is meant by consent, and the Information Commissioner's Office (ICO) has published detailed guidance on consent under the GDPR. In brief, consent must be "freely given, specific, informed and unambiguous." Organizations should review how they seek, record and manage consent, and whether they need to make any changes to their policies and procedures. In evaluating compliance with the GDPR's expanded consent requirements, organizations should note the following characteristics:

- **Active Opt-in:** There must be "clear affirmative action"; consent cannot be inferred from silence, pre-ticked boxes or inactivity.
- **Unbundled:** Consent requests must be separate from other terms and conditions and should not be a precondition of signing up to a service unless necessary for that service.
- **Granular:** Granular options to consent separately to different types of processing should be given wherever appropriate.
- **Named:** Name your organization and any third parties that will be relying on consent; even precisely defined categories of third-party organizations will not be acceptable under the GDPR.

- **Verifiable:** Keep records to demonstrate what the individual has consented to, including what they were told and when and how they consented.
- **Easy to Withdraw:** There must be simple ways for people to withdraw consent – tell people about their right to withdraw and offer them easy ways to withdraw consent at any time.
- **No Imbalance in the Relationship:** Consent is not "freely given" if there is imbalance in the relationship between the individual and the data controller.

What Rights Do Individuals Have to Protect Personal Data?
One of the key premises of the GDPR is to expand the rights of individuals to protect their personal data. This includes an individual's right to access, rectify and/or seek erasure of their personal data.

Right to Access
Individuals have the right to access their personal data and request the following information from a data controller:

- Copy of their personal data
- Purpose of processing the personal data
- Categories of personal data
- Recipients of the personal data
- Time period the personal data will be stored
- Individual's right to request alteration (rectification), erasure and/or restrictions on processing their personal data
- Right to file a complaint with a Supervisory Authority
- Extent to which decisions about the individual are made based on automated processing or profiling of personal data
- Appropriate safeguards for transfers of personal data outside the EU.

Right to Rectification
An individual has the right to request the data controller to correct their personal data without undue delay.

Right to Be Forgotten
The GDPR recognizes an individual's so-called "right to be forgotten," subject to limited exceptions. In other words, an individual has the right to request the data controller to erase their personal data without undue delay in certain circumstances, including the following:

- Personal data is no longer required for processing
- Individual withdraws consent to the processing of their personal data
- Individual objects to the processing of their personal data
- Personal data has been unlawfully processed.

What Are the Record-Keeping Requirements Under the GDPR?
Data controllers and processors must maintain written documentation of all activities related to the processing of personal data (including documentation of all steps made in order to be GDPR compliant). These records should include the following information:

- Contact information for the data controller
- Purpose for processing the personal data
- Description of the personal data
- Recipients of the personal data
- Safeguards to protect personal data transferred outside the EU
- Anticipated time frame for erasing personal data
- Technical safeguards employed to protect personal data.

These records of processing activities must be produced to a Supervisory Authority upon request. Notably, the GDPR's record-

keeping requirement does not apply to organizations with fewer than 250 employees.

What Security Measures Are Required to Safeguard Personal Data?

The GDPR does not dictate specific technical security measures that must be implemented by data controllers or processors to safeguard personal data. However, the Regulation does require organizations to conduct a risk assessment to ensure an appropriate level of security based on a cost-benefit analysis. The size of the organization and the nature and scope of processing activities are key factors to consider. Such security measures may include the pseudonymization of personal data (so that data cannot be linked to a specific individual); encryption of personal data; ability to restore and back up personal data; periodic security audits to test and evaluate processing activities; and adherence to recognized industry standard certification requirements to protect data.

What Is a Data Protection Officer?

The GDPR requires data controllers and processors to appoint a Data Protection Officer (DPO) when an organization's "core activities" consist of processing personal data on a "large scale." Germany qualifies this requirement to include instances where there is a minimum of 10 people processing personal data automatically. An organization may designate an employee or hire a third party to serve as a DPO, based on their expert knowledge of data protection laws and regulations. A DPO is responsible for monitoring an organization's compliance with the GDPR, training employees and staff, oversight of any data protection impact assessments, cooperating with the Supervisory Authority, and acting as the liaison between the organization and the Supervisory Authority. In addition, the DPO may be responsible for responding to inquiries by individuals concerning their personal data.

Is an Organization Required to Report a Data Breach?

The GDPR introduces additional mandatory data breach reporting requirements. A data controller must report security breaches to the relevant Supervisory Authority "without undue delay, and where feasible, not later than 72 hours" after it first becomes aware of the

incident. If the notification is made after 72 hours, a reasonable justification for the delay must be provided. The breach only needs to be reported if it is likely "to result in a risk for the rights and freedoms" of data subjects – if, for example, the breach could result in discrimination, damage to reputation, financial loss, loss of confidentiality, or any other significant economic or social disadvantage.

A data controller also must notify individuals of a security breach "without undue delay" where the breach "is likely to result in a high risk" to the rights and freedoms of data subjects. However, notification to individuals is not required if (1) the organization has implemented appropriate security measures that render the data unintelligible to any unauthorized person (*i.e.*, encryption); (2) the organization has taken subsequent measures to ensure that a high risk to data subjects does not materialize (*i.e.*, remediation); or (3) it would involve a disproportionate effort, in which case a public communication will suffice (*i.e.*, media notice or publication on the organization's website).

The contents of the breach notification communication should include the following information where available in "clear and plain" language:

- Nature of the incident
- Type of personal data
- Number of affected persons
- Number of personal data records
- Contact information for the DPO
- Likely consequences of the data breach
- Steps taken by the organization to contain and mitigate the exposure.

Notably, the breach notification requirements set forth above apply to data "controllers." However, in the event of a breach experienced by a

data "processor," the processor is required to notify the controller "without undue delay."

Are There Any Repercussions for Failure to Comply with the GDPR?

The most serious infringement of the GDPR can result in administrative fines by a Supervisory Authority of up to €20 million or 4 percent of the offending company's global annual revenue, whichever is higher. For lesser noncompliance offenses, company audits and a tiered fine structure may be imposed.

Under the GDPR, data controllers and processors also may be subject to liability and damages for legal proceedings commenced by a data subject in a court of law or a complaint lodged with a Supervisory Authority. Such complaints may be filed in the jurisdiction where the data subject resides or works, or the location of the alleged infringement of the Regulation concerning the processing of the individual's personal data. Data controllers and processors may have joint liability for compensatory damages awarded to an individual to ensure they are made whole.

The GDPR also grants Supervisory Authorities the following powers to:

- Conduct investigations of data controllers and processors
- Perform data protection audits
- Issue warnings or reprimands
- Order an organization to comply with a data subject's request regarding personal data (including rectification, erasure and restrictions on processing)
- Require an organization to bring its processing activities into compliance with the GDPR
- Order an organization to notify individuals of a data breach
- Order the suspension of data flows.

Summary

In summary, U.S. companies are well advised to consider their compliance obligations, if any, under the GDPR. The extraterritorial reach of the EU's new privacy Regulation means that non-EU companies may be subject to the law. A critical factor in evaluating the potential application of the GDPR to U.S. companies is whether a company collects, stores, transfers or otherwise processes personal data of EU residents. If so, the company may be required to obtain an individual's express consent to the use of their personal data, in addition to maintaining internal records of the company's personal data processing activities. Moreover, companies may have a mere 72 hours to notify EU regulatory authorities of a data breach involving the personal data of EU residents. Failure to comply with the GDPR's extensive requirements may result in regulatory investigations, legal proceedings, compensatory damages, injunction orders or hefty administrative fines.