LJN LAW JOURNAL NEWSLETTERS

Cybersecurity LAW & STRATEGY®

An ALM Publication

July 2017

GDPR Gets Real

A procrastinator's guide to overcoming technical challenges in GDPR compliance.

By Jason Straight

After years of discussion, debate, lobbying and lamenting, we are now twelve months from the date the European Union's General Data Protection Regulation (GDPR) takes effect. The GDPR replaces the EU's Directive 95/46/EC, which has provided data protection guidance in the EU since 1995. The purported purpose for enacting the GDPR is to create regulatory consistency and certainty for companies operating in the EU with respect to their obligations to protect personal information for citizens of EU states. With a fining mechanism that allows penalties as high as 4% of global turnover (*i.e.*, gross-revenue), any company that has yet to take a hard look at its obligations under the GDPR would be well-advised to do so before it's too late. Moreover, the breadth of the regulation will create compliance headaches for nearly every organization, large and small.

For U.S. companies, the degree of emphasis placed on protecting personal information can be hard to grasp. But as the GDPR explicitly states, protection of personal data is considered a "fundamental right" and further clarifies that "processing of personal data should be designed to serve mankind." Regardless of your view on the sanctity of personal information, the reality is that if you conduct any business in the EU or sell any goods or service to citizens of EU states, your window for procrastination is rapidly closing. Fortunately, even if you are hearing about GDPR for the first time today, you do have time to get ready and be compliant on May 25, 2018. This article targets organizations that have been putting off compliance efforts and for which the GDPR will require a relatively modest adjustment in practices and procedures.

What's the Big Deal?

The most significant changes that are included in GDPR are the introduction of the "Right to be Forgotten," the "Right to Portability" of personal information, and a uniform data breach notification requirement. For social media and large-scale data processors whose business relies on collecting, analyzing and monetizing personal information, complying with the Right to be Forgotten and Right to Portability will be a big deal. The Right to be Forgotten requires organizations to create a mechanism by which an individual's personal information can be deleted or rendered inaccessible if it is deemed no longer relevant, inaccurate or otherwise unfairly characterizes an EU citizen. The Right to Portability requires social media companies, like Facebook,

Jason Straight is the senior vice president and chief privacy officer of Cyber Risk Solutions at UnitedLex. Prior to joining UnitedLex, Jason held numerous leadership positions at a leading global investigations and cyber security company, most recently as a managing director in the cyber investigations practice. Jason began his career as an attorney at Fried, Frank, Harris, Shriver & Jacobsen in New York.

to provide a "portable" version of an individual's personal data to a person upon request so that it may be transferred to an alternative platform. Although these provisions technically apply to every organization subject to GDPR, unless you are a media company or search engine operator, they probably won't cause a major disruption to your business.

For the average U.S.-based company doing business in the UK, the significant changes will be driven by some of the more routine provisions that restrict a company's ability to handle personal data. The following requirements should be top-of-mind:

Data Breach Notification. Companies are required to notify an EU data protection authority within 72 hours of a data breach event that compromises personal information of an EU member-state citizen.

Privacy Impact Assessments/ Privacy By Design. Companies must implement a program under which they will conduct a formal analysis of data protection and privacy implications of any new business process or system.

Data Transfer Restrictions. Like the prior regime of Directive 95/46/EC, organizations must safeguard personal data transferred outside the EU by relying on one of several options including adequacy, consent, binding corporate rules and other contractual provisions.

Data Protection Officer Appointment. Any company that conducts "regular and systematic monitoring of data subjects on a large scale" or processes particularly sensitive personal information as defined in Article 9 of the GDPR, must appoint a Data Protection Officer to advise on and monitor compliance with the GDPR as well as to serve as the primary interface with regulators and with data subjects.

GDPR Basics

For many organizations, the impact of the GDPR will come down to the definition of "personal data" and how such data is "processed," or used. According to the GDPR, personal data is:

Any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, direction or indirection, in particular by reference to an identifier such as 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.

Processing is defined as:

Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Interpreting these definitions will be key to assessing a company's compliance obligation. The first task for many organizations will be to identify the circumstances under which personal data is collected. Among the common circumstances are collection of information through web forms or other marketing mechanisms, collection of employee or contractor data and customer information gathered for purposes of delivering a service. To be clear, companies are not prevented from collecting such information, but must comply with certain restrictions set forth in the GDPR.

Under the GDPR, personal data must be:

- Collected for specified, explicit and legitimate purpose;
- Accurate and up-to-date;
- Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes; and
- Processed in a manner that ensures appropriate security of data, including protection against unauthorized or unlawful processing and against accidental loss, destruction

or damage, using appropriate technical or organizational measures.

In assessing whether a given purpose is legitimate, companies should assess the following factors:

- Has the subject given consent for specific purpose?
- Is processing necessary for performance of contract to which subject is a party?
- Is processing necessary for compliance with legal obligation?
- Is processing necessary to protect vital interests of subject or another person?
- Is processing necessary for task carried out in public interest or in official authority?
- Is processing necessary for purposes of legitimate interests pursued by controller?

Where Is Your EU Data?

Once you have interpreted the GDPR definition of personal data, the next task is to map the locations of such data in your environment. Structured data stores such as marketing databases, personnel records and customer data should be relatively easy to survey and identify. For these data types, an organization should conduct an honest assessment of the business value of retaining and/or processing such data. Many organizations retain far more personal data than they can actually make use of. The GDPR requires organizations to apply a more conservative standard to the decision to retain personal information since the penalty for misuse or loss is so significant.

The bigger challenge will come in identifying personal data contained in unstructured data sources, such as email. User awareness is an important piece of a GDPR compliance readiness effort. Users must be made aware of the consequences of sharing personal data belonging to EU citizens and discouraged from doing so. Companies should consider implementing a mechanism to monitor email communications for instances where personal data is shared to facilitate enforcement of policies intended to minimize those situations.

What Is Your Program?

Once you've identified and located personal data restricted by the GDPR, the next step is to ensure you have a program to protect that data. The GDPR is mercifully vague regarding the specific measures you must implement. This means that an organization with a relatively mature information security program is probably OK as long as it can demonstrate that all identified personal information is covered by the program. For companies that aren't confident that their existing information security program is adequate to withstand scrutiny, the advent of the GDPR represents a great opportunity to conduct a thorough review of security controls with a focus on personal data. An emphasis on security basics such as patching and vulnerability management along with an examination of incident detection and response capabilities will yield positive results.

The Bottom Line

Chances are that if the GDPR presented an existential risk to your organization, you are already well on your way to ensuring compliance. For other organizations, cutting through the density of GDPR and distilling it to a few actionable elements will help you understand your obligations and create a roadmap to get you where you need to be by May 2018.

—❖—