Bond

BUSINESS AND CYBERSECURITY INFO MEMO

MAY 14, 2018

Will Your Business be in Compliance with the General Data Protection Regulation (GDPR)?

Effective May 25, 2018, the European General Data Protection Regulation (GDPR) imposes new obligations on persons or entities that are "controllers" or "processors" of "personal data" [1] of individuals in the European Union (EU). Unlike U.S. privacy laws or even current privacy laws in Europe, the GDPR (i) can apply to entities that are located *entirely outside* of the EU, and (ii) applies to "personal data" about *anyone in the EU*, regardless of whether they are a citizen or permanent resident of an EU member state. [2]

In contrast to U.S. privacy laws that tend to cover specific kinds of personal data (e.g., healthcare, financial) the GDPR covers all personal information relating to an identified or identifiable individual. Specifically, the GDPR covers all "Personal Data", defined as "information relating to an identified or identifiable natural person who can be identified, directly or indirectly, 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". Moreover, given the broad definition of Personal Data, online identifiers, including IP addresses and cookies will fall within the protections of the GDPR.

Many U.S. businesses will be subject to the GDPR. For example, your business could be considered a controller or processor of Personal Data if, among other things, it:

- Has an affiliate or location within the EU;
- Conducts business in the EU by selling a service or product to persons in the EU;
- Employs individuals residing in the EU (regardless of whether such employees are U.S. or EU citizens);
- Is involved in the transfer of Personal Data to or from the EU;
- Has employees or customers that reside, even if temporarily, in the EU;
- Participates in research that involves collection of personal data from the EU;
- Employs vendors within the EU to process data (i.e., processors); or
- Serves as a processor of personal data for another entity that is required to comply with the GDPR.

Cost of Non-Compliance

Businesses in violation of the individual rights created by the GDPR could face significant fines. Depending on the nature of the violation, an entity in violation of the GDPR could be fined up to €20 million (which amounts to over US$24 million) or up to 4 percent of a company's global revenue, whichever is higher.

---

1 These terms are defined below.

2 Each EU member state will likely adopt its own rules with respect to GDPR compliance; thus businesses with significant contacts in the EU may need the assistance of local counsel in connection each applicable EU member state. Currently, the UK has indicated it intends to follow the GDPR; however, post-Brexit, it is unclear whether the UK will implement its own wholly separate set of rules.

What does the GDPR require?

Among other things, the GDPR requires a business entity to:

- Appoint a person to oversee protection of Personal Data;
- Provide notice to covered individuals regarding the Personal Data it collects;
- Provide notice of how it uses any Personal Data collected;
- Record the uses and disclosures it makes of Personal Data;
- Obtain specific consent for collection of certain kinds of Personal Data;
- Allow covered individuals whose personal data was collected to object to such collection or processing, and ultimately honor an individual's "right to be forgotten," unless an exception applies;
- Ensure that all vendors and third parties to which it provides personal data have adequate privacy and security protections; and
- Enter into contracts containing specific provisions when transferring personal data outside of the EU (including transferring data within the business entity).

Key Definitions

As mentioned above, the GDPR applies to persons or entities that are "*Controllers*" or "*Processors*" of "*Personal Data*."

A "*Controller*" is a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

A "*Processor*" is a natural or legal person, public authority, agency or other body which is processing personal data on behalf of a controller.

"*Processing*" means 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.

GDPR Guiding Principles

The GDPR sets forth certain core principles for data collection, processing and retention, which will require covered businesses to adopt and implement policies that apply at the outset of receiving Personal Data from the data subject or other sources. Those principles include:

(i) transparency to data subjects about the nature, purpose and disclosure of data that will be collected;
(ii) retention of Personal Data for only the minimum necessary time period;
(iii) the collection of Personal Data solely for "legitimate" purposes and further processing consistent with those purposes; and
(iv) processing in a manner that assures appropriate security protections.

While the GDPR sets few specific requirements for data security, it places the burden squarely on the Controller to assure adequate security measures for all Personal Data, including the assurance that any third parties that receive Personal Data as processors also have adequate security measures in place.

The GDPR specifies lawful bases for processing Personal Data, including consent by the data subject or a determination that the data is necessary for performance of a contract or fulfillment of a legal obligation. Rigorous requirements for consent to retain and use Personal Data apply, which essentially reject consent by omission or inaction—consent by silence, pre-filled boxes, or inactivity will not constitute consent. Moreover, if consent provides the lawful basis to process Personal Data, businesses must provide extensive information to the data subject at the time the Personal Data is obtained, including the identity and contact information for the controller, the purposes for processing the data, the intended recipients or categories of recipients of the data, and the rights of the data subject with respect to the data.

Conclusion

The GDPR will require U.S. businesses covered by the GDPR to adopt a new framework for identifying, tracking, managing and protecting Personal Data in accordance with GDPR requirements. GDPR compliance may therefore require new privacy and security procedures for a broad array of business operations, including but not limited to: (i) data collection, use and disclosure; (ii) data retention and deletion; (iii) responses to requests for information about Personal Data by data subjects; (iv) employment policies; (v) communications with current and potential customers; and (vi) marketing procedures.

If you have any questions about this memorandum, please contact Lisa Christensen, Sara Temes, any other member of our Cybersecurity and Data Privacy Practice Group, or the attorney in our firm with whom you are regularly in contact.

Packaged Service Offerings

Bond understands that our clients, especially our small business clients, are focused on running their business while trying to stay compliant with the myriad state and federal (and now European Union) regulations that may be imposed upon them. That is where Bond comes in. Our preeminent Business, Cybersecurity and Data Protection groups have the depth and experience to know the intricate details of existing and pending regulations so that we can advise our clients on compliance and best practices so that you can continue to run your business.

We also understand that predictable costs make running your business easier. Therefore, we are proposing a *fixed fee* related to GDPR documents and policies, which will provide you access to exclusive, copyrighted content that will address the most commonly encountered issues related to GDPR policy implementation.

The GDPR goes into effect on May 25, 2018. Let Bond help you prepare.

Contacts

For more information contact one of the individuals below:

Lisa Christensen
315.218.8279
lchristensen@bsk.com

Sara C. Temes
315.218.8327
stemes@bsk.com

Tracy Miller
646-253-2308
tmiller@bsk.com

BOND SCHOENECK & KING ATTORNEYS