BARNES & THORNBURG LLP

INSIGHTS

GDPR And European Data Privacy: What You Need To Know Now

February 1, 2018 | Atlanta | Chicago | Columbus | Dallas | Delaware | Elkhart | Fort Wayne | Grand Rapids | Indianapolis | Los Angeles | Minneapolis | New York | South Bend

This is the first in a series on the new General Data Protection Regulation (GDPR) that becomes effective this spring. This article focuses on what GDPR is, whether it may apply to you, and why you should care.

What is the GDPR?

The European Union General Data Protection Regulation is a new set of rules that regulates the collection, storage, disclosure, and use of "personal data" of European residents. Effective on May 25, 2018, the GDPR ushers in the biggest changes in privacy and data protection laws in more than 20 years and is designed to provide individuals greater protection and control over their personal data.

Does the GDPR Apply to You?

The GDPR applies to any organization that "controls" (e.g., collects) or "processes" the "personal data" of European residents. "Personal data" is any information relating to an identified or identifiable natural person. "Processing" is essentially any activity an organization does with personal data, such as storage, manipulation, or transfer.

The GDPR affects organizations large and small, public and private, for-profit and nonprofit, across all industries and in all geographic locations, whether or not the organization is based in an EU country or even has an EU presence. For example, a U.S. company having no offices or employees in the EU, but that has a distributor in the EU that collects the personal data of EU residents and transmits that data to the

RELATED PEOPLE

Jason A. Bernstein
Partner
Atlanta

P 404-264-4040
F 404-264-4033
jason.bernstein@btlaw.com

Brian J. McGinnis
Partner
Indianapolis

P 317-231-6437
F 317-231-7433
brian.mcginnis@btlaw.com

U.S., is subject to the GDPR despite having no physical presence there. GDPR impacts any organization that receives the personal data of EU residents.

Determining whether your organization is subject to the GDPR is the key threshold question. Answering that question involves working with an adviser to assess your organization's current data collection and use practices, perform gap analyses mapped to GDPR standards, and to help you develop and implement data protection programs that will allow you to strategically comply with the new regulation's requirements.

Why You Should Care

Compliance Requires Change. If the GDPR applies to your organization, there is a good chance you will have to change the way you handle and document security of data collection, storage and processing. Some of these changes will take time to implement and may involve significant cost. For example, data breach notice requirements under the GDPR are significantly more stringent than under U.S. law, including notification obligations to Data Protection Authorities not later than 72 hours from the time of an incident.

Substantial Penalties. The GDPR includes significant enforcement capabilities, including fines and penalties as high as 4% of an organization's worldwide gross annual revenue. And, the EU authorities can collect the penalty even if you have no offices or relationships in the EU.

Customer Requirements. GDPR requires controllers of personal data be responsible for that data throughout its lifecycle. Customers, vendors, and business partners are increasingly requiring that the entities they do business with comply with the GDPR and are adding various contractual provisions regarding data protection and security to new and existing contracts. These must be reviewed carefully, and your organization should clearly understand these provisions before agreeing to them.

Lost Business. The GDPR is already having a global impact. Failure to meet its requirements will increasingly lead to business opportunities lost to competitors who are compliant.

Insurance Coverage. If you are required to comply with the GDPR but you don't, it remains to be seen whether and how insurance companies will provide coverage for GDPR violation penalties.

Cross-Border Data Transfers. If you transfer EU personal data outside the EU, or your U.S. team has access to such data, you must identify a valid legal transfer mechanism to legally process that data.

Next Steps

1. **Determine whether the GDPR applies to your organization**. Consider working with your advisers to assess how your company collects, stores, and processes data and what you need to do to get ready to comply with the GDPR if it applies.
2. **Assess the current state of your data security policies and procedures**. It may be a good time to review, with someone who understands the new GDPR requirements, your current practices

and determine what changes must be implemented to ensure compliance.
3. **Close the gaps**. If you don't have a plan already in place, consider developing and implementing a plan to close any gaps and become GDPR compliant.
4. **Review your vendor and customer agreements**. Going over your template agreements on a regular basis with your advisers to ensure your vendors and partners also comply with the new requirements is just good best practice. Consider discussing with counsel the need to negotiate new agreements to implement new data protection and security requirements, along with updating your online and mobile app terms of use and privacy policy to incorporate new requirements.
5. **Review your cyber insurance**. Consider working with counsel that understand cyber insurance to review your current policy to determine whether coverage is adequate or needs to be revised.

With only weeks remaining before the GDPR comes into force, time is short to ensure your organization is compliant with these heightened requirements. That work starts now.

Barnes & Thornburg is hosting a webinar, The GDPR's Impact on Non-Profit and Meeting Industry Organizations, on Wednesday, Feb. 28, 2018. Registration is open.

For more information, please contact the Barnes & Thornburg attorney with whom you work or Jason Bernstein at 404-264-4040 or jason.bernstein@btlaw.com, or Brian McGinnis at 317-231-6437 or brian.mcginnis@btlaw.com.

Visit us online at www.btlaw.com and follow us on Twitter @BTLawNews.