February 27, 2018

Preparing for Enforcement of the European Union GDPR: Five Key Considerations to Keep in Mind

On May 25, 2018, the European Union General Data Protection Regulation ("GDPR" or "Regulation") will go into effect. The GDPR is a uniform privacy regulation that imposes extensive requirements on organizations that collect information from individuals residing within the EU. For many organizations, complying with the Regulation will take a substantial amount of work, and require a close examination of longstanding policies and practices. To achieve compliance, many organizations will find themselves in the position of having to modify fundamental aspects of how they collect and use personal information, market their services and design their products. As the May 25, 2018, deadline approaches, it is more important than ever that companies develop a realistic plan, prioritize compliance with the Regulation's most material terms, and ultimately strive for full compliance.

Background

The GDPR was adopted on April 8, 2016, to supplant the longstanding EU Data Protection Directive 95/46/EC and further harmonize European privacy laws. In many ways, the Regulation is more far-reaching and stringent than other countries' laws. Unlike the United States, which uses a patchwork framework to regulate privacy based on the industry and information at issue, the EU has asserted jurisdiction over all personal information of EU residents, thereby impacting organizations of all sizes across industries. As such, any organization that collects or processes information from individuals located in the EU should carefully examine if they are subject to the GDPR.

In addition to its wide scope, the GDPR allows for substantial penalties to be imposed on noncompliant organizations. European regulators can order recalcitrant organizations to stop gathering or using information from EU residents and impose fines as high as 4 percent of an organization's annual global revenue. If an organization determines that it must meet the GDPR's requirements, it should immediately begin investing the time and resources needed to take material strides toward compliance by May 25, 2018. Compliance will take time and require a detailed understanding of the organization's information collection, processing, storage and transfer practices. While consultation with specialized counsel is strongly suggested, as a starting point, organizations should keep in mind the following five key considerations.

Initial Steps Toward Compliance

1. **Consent Is Key.** The GDPR requires that an organization receive consent from individuals residing in the EU before collecting or processing their personal data. For consent to be valid, it must be freely given, specific, informed and unambiguous. This means that organizations cannot rely on pre-checked boxes and other "opt out" mechanisms to obtain consent or continue to utilize personal information gathered through such mechanisms. Given that consent is a prerequisite for any data processing activity, organizations should examine their existing consent mechanisms as one of their first steps on the road to compliance.
2. **Know Your Vendors.** Organizations that rely on third-party vendors to collect, store or process data will face increased accountability for those vendors under the GDPR. The Regulation requires organizations that outsource data processing to establish clear agreements with their vendors to ensure that data will be responsibly handled under the GDPR's principles. Additionally, the Regulation imposes new requirements on third-party data processors, requiring them to maintain adequate documentation, carry out periodic assessments, appoint a data protection officer and comply with a number of other rules. If a data processor fails to meet these requirements or violates a data processing agreement, European regulators can subject them to penalties. It is thus important for organizations to coordinate with their vendors, establish new data processing contracts, and ensure the vendors are independently working toward compliance.

© 2017 Brownstein Hyatt Farber Schreck, LLP
www.bhfs.com

3. **More Rights for Data Subjects.** The GDPR establishes that EU residents have certain fundamental rights to control information about themselves. To give force to these rights, the Regulation requires that organizations provide EU residents with clear disclosures at the time information is collected and access to their information after collection has occurred. Specifically, organizations must be able to provide an EU resident with all information that the organization has obtained about the individual upon request. Organizations must also facilitate requests from EU residents to correct or delete any personal information about them that the organization possesses. Providing this level of access and control may require organizations to modify internal policies and technology, and should be considered a priority.
4. **New Breach Notification Requirements.** Unlike its precursor, the GDPR requires organizations that have been the victim of a breach to provide certain types of notice on a very limited timetable. The Regulation requires that an organization notify its European supervisory authority of any breach within 72 hours after becoming aware of it, and subsequently, alert any affected individuals "without undue delay." Notice to the regulator must include specific categories of information such as the number of individuals and records concerned, the likely consequences of the breach and steps the organization is taking to mitigate harm. To ensure they can meet these requirements, organizations should work with experts to create breach response plans or modify their existing plans and conduct tabletop training exercises to prepare the
5. **Increased Accountability and Governance Obligations.** Organizations subject to the GDPR will also be required to make adjustments to many of their internal processes. The Regulation requires that organizations keep detailed records of data processing operations, perform privacy impact assessments of their processing operations, and designate a data protection officer. Although each of these requirements may not be particularly disruptive, they will likely require modifications to numerous existing policies and workflows, and should not be deferred to the last minute.

Attaining Compliance

The five considerations above are only a starting point. Full compliance will require substantial work for many organizations and regular guidance from privacy experts. It also may involve taking a "phased" approach and setting realistic priorities for the next several months, with a longer-term goal of total compliance. In any event, once obtained, organizations will be well positioned to maintain and build upon their strong privacy foundation for years to come.

Tracy L. Lechner
Shareholder
tlechner@bhfs.com
303.223.1274

Esteban M. Morin
Associate
emorin@bhfs.com
303.223.1275

This document is intended to provide you with general information regarding the European Union General Data Protection Regulation. The contents of this document are not intended to provide specific legal advice. If you have any questions about the contents of this document or if you need legal advice as to an issue, please contact the attorneys listed or your regular Brownstein Hyatt Farber Schreck, LLP attorney. This communication may be considered advertising in some jurisdictions.