WEBSTER, CHAMBERLAIN & BEAN, LLP | NONPROFIT ALERT

EU GENERAL DATA PROTECTION REGULATION (GDPR): OVERVIEW FOR U.S. NONPROFIT ORGANIZATIONS

Beginning on May 25, 2018, new privacy legislation in the European Union could require companies around the world, including some U.S. nonprofit organizations, to change the way they collect and handle personal information of individuals in the EU. In general, the EU General Data Protection Regulation (GDPR) has a broad territorial scope and could apply to some U.S. based nonprofit organizations if certain criteria are met.

The GDPR applies to U.S. based nonprofit organizations in three general circumstances: (1) the U.S. nonprofit organization has a physical presence in the EU, *i.e.*, an office or one or more employees in the EU; (2) the U.S. nonprofit organization offers goods or services to individuals in the EU; or (3) the U.S. nonprofit organization monitors the online behavior of individuals in the EU.

Whether or not a U.S. based nonprofit organization will be subject to the GDPR depends on a review of specific facts and circumstances surrounding the activities of the organization. For example, without more, a U.S. nonprofit organization that offers publications or resources for download by anyone on a website that is accessible around the world may not be sufficient to fall under the scope of the GDPR. However, running advertisements in an EU-focused magazine or website, marketing goods or services in different EU languages, or allowing customers to pay with EU currency could suggest targeting of individuals in the EU and trigger application of the GDPR.

If a U.S. nonprofit organization is subject to the GDPR, then a review of its personal data collection and data privacy practices and policies, as applied to individuals in the EU, should be conducted as soon as practicable in order to evaluate its compliance with the GDPR. Personal data could include names, email addresses (including business email addresses), phone numbers, and physical addresses. The evaluation of compliance should include the legal basis (there are six legal bases) for collecting the personal data, and ensuring that the data subjects are afforded certain rights with respect to their data.

Under the GDPR, consent is not required for most typical uses by a nonprofit organization of personal data. An organization can rely on another legal basis such as the "legitimate interests" of the organization in order to use and store most types of personal data. This includes existing databases of EU residents who are members, attendees, customers, etc.

In addition, an evaluation of data security measures, including a review of vendor contracts that process or store personal data, will be important.

Evaluation of the application and effect of the GDPR is a fact intensive effort, and U.S. nonprofit organizations should take note and seek guidance promptly.

* * *