FPLG
FOR PURPOSE LAW GROUP
A Professional Law Corporation

GENERAL

The EU Data-Privacy Law That May Affect U.S. Nonprofits (GDPR)

03.07.18 | Linda J. Rosenthal, JD

If you've never heard of the General Data Protection Regulation (GDPR), you've got a lot of company, especially here in the United States.

First, it's a new data privacy law which – alone – is enough to make most folks' eyes glaze over. Second, it's a law passed by the European Union.
Nevertheless, it's something that legal entities in the U.S., including some nonprofits, may need to know about ASAP. The GDPR is already in effect; legal enforcement begins on May 25, 2018. It's a big deal with big penalties for violations.

The General Data Protection Regulation

The GDPR is a new collection of laws enacted by the European Union in April 2016. The purpose is to replace the existing, inadequate, "Data Protection Directive 95/45/ec" (the "Directive") as the "primary law regulating how companies protect EU citizens' personal data."

It includes " sweeping changes" and "very significant penalties." While it applies to the "use of personal data by European organizations," it also, applies "in many cases" to "non-European Union (EU)-based organizations."

The definition of "personal data" is this new framework is broad; namely, "anything that can be used to directly or indirectly identify an individual," including – for instance – names, photos, email addresses, and social security numbers. It also can refer to "bank details, social media posts, and medical information." "…GDPR directly pertains to data collection, even when it's not being used for the purpose of rendering goods or services. Charities and nonprofit organizations collect a lot of personal data" including these cited examples.

GDPR May Apply to U.S. Nonprofits

From the perspective of any entity outside the European Union, the most significant change from the old Directive to the new GDPR is the expansion of the territorial application.

According to the *Nonprofit Times*, the new law "applies to organizations established in Europe that process the personal data of individuals in Europe and, in a shift from the Directive, to non-EU-based organizations that offer goods or services to individuals in Europe. This means that nonprofits with donors, grantors, or member in Europe might be subject to the new law."

American Technology Services, a U.S. based company that offers services in connection with preparation for the new GDPR, offers helpful examples of how or why United States nonprofits may come within the scope of this new European Union regulatory scheme. ATS first underscores that any nonprofit that already "markets itself to EU countries" will, of course, have to comply with the new GDPR. But what about groups that only operate in the U.S. and are thinking …."this can't possibly affect us." ATS responds: "That seems logical, but if you have a website, you'd be wrong. It really depends on a number of factors, some of which are tricky to understand…."

For instance, "(w)hat if someone in England is researching your association's cause on the Internet," visits your website and fills out an online form providing data covered under GDPR, bearing in mind that "this transnational web transaction doesn't have to be financial; it just has to be data process to fall within the purview of GDPR?" According to ATS, the answer may be yes. And, in the case where "your organization has deliberately targeted an EU audience with intentional marketing (say, copy that targets an EU country audience), yes, GDPR applies." GDPR will not apply, though, if an "EU individual found your website randomly, or even through a Google search."

Conclusion

If nonprofits "comply with U.S. data breach laws [they] will … have a leg up in complying with GDPR." That, however, is a big "if." It's fair to say that even the largest multinational companies don't have a firm handle on cybersecurity and data protection.

For U.S. nonprofits, the need to deal with cybersecurity issues is urgent and ongoing. The coming May 28 deadline for compliance with GDPR is an added layer of complexity that must be faced by some, thought not all, organizations. "T–he point is even if your organization is U.S. only, it's very important that you and your IT team are aware of GDPR and its nuances to mitigate the risk in these areas."

— Linda J. Rosenthal, J.D., FPLG Information & Research Director