FPLG
FOR PURPOSE LAW GROUP
A Professional Law Corporation

GENERAL

More About GDPR and Nonprofits

01.22.19 | Linda J. Rosenthal, JD

Back in early March 2018, we posted *The EU Data-Privacy Law That May Affect U.S. Nonprofits (GDPR)* to alert readers of a set of rules in the European Union that may apply to more than a few American organizations. There are hefty penalties for violations; the 2016 law included a grace period until May 25, 2018, after which these penalties would take effect.

We correctly guessed that few readers back in March had ever heard of GDPR and likely wondered how this unknown GDPR thing could possibly be relevant to nonprofit organizations based in the United States. But a month or so later, most of us started noticing our inbox full of "We've Updated Our Privacy Policy" messages from our favorite websites.

It's time now to revisit this topic with a bit more information.

What is GDPR?

The General Data Protection Regulation (GDPR) is a regulation "designed to give individuals more security and peace of mind with the activities online." It focuses on the "collection of personal data, and the use of that data. And a lot of it boils down to getting informed consent from individuals before doing anything with that data." It "raises the bar for the protection of personal data, which is any data that can be linked to an individual."

Why did the EU adopt this new law? "In Europe, privacy is a fundamental right, and the EU is dedicated to protecting it. The EU's operational philosophy is built on the concept that personal data belongs to the individual. This is different than how the United States operates, where information collected on an individual is seen as the property of the organization that collects it."

Since "data breaches have become part of our everyday life," the European Union wanted to be the world leader requiring "companies to be more principled and transparent around data use and invest in security and data protection. Any company or agency collecting or utilizing personal information

may do so only if they have lawful basis to process the information."

Before enactment of the GDPR in 2016, the EU had a rule called "Data Protection Directive 95/45/ec" (the "Directive") that had been the "primary law regulating how companies protect EU citizens' personal data." It was ineffective, though, to meet the current realities about the easy hack-ability and misuse of personal data.

How Does GDPR Apply to U.S.-based Nonprofits?

Perhaps the biggest change relevant to entities and organizations based outside the European Union is that the territorial scope of the GDPR has been broadened over the prior law.

The General Data Protection Regulation "imposes new rules on companies, government agencies, nonprofits, and other organizations" – wherever located – that "offer goods and services to people in the European Union (EU) or that collect and analyze data tied to EU residents."

GDPR represents " sweeping changes" over prior rules. "From the perspective of a U.S. nonprofit organization, the primary difference is the concept of a new, broader geographical reach": now, "in many cases," to "non-European Union (EU)-based organizations." "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."

What are Key Requirements of GDPR?

"The average person will have more explicit rights under GDPR to know who stores, processes, and has access to their personal data. Under GDPR, EU residents can request access to, rectification of,

and deletion of their data."

Organizations collecting this personal data "need to review their data governance practices" and eliminate older data that wasn't collected under the GDPR standard.
"The GDPR requires enhanced security, data protection, appropriate technical and organizational measures, transparency, record keeping, accountability, and supporting data subject requests. It also requires a 72-hour personal data breach notification by data controllers to the authorities."

Key principles" include:

- Processing must be lawful, fair and transparent, and done in a way that "ensures security of the data and protects it from unauthorized use."
- Personal data must be collected for "specified, explicit and legitimate purposes and not further processed in an incompatible way"; also, "limited to what is necessary to achieve the purposes for which it was collected" and "not be kept in identifiable form for longer than necessary."

The main feature is "… getting *freely given consent, with a statement of clear affirmative action*. This basically means that you gave individuals all the autonomy and choice to opt into your communications.

For example, in the nonprofit sector, this may affect "how you interact with and build your various mailing lists. From soliciting new donors to stewarding relationships with existing donors, a lot of your communication with constituents is through email marketing.

"A simple change you can make to get more GDPR compliant is to change all of your sign-up forms (or anything that captures data, online) into forms that have double or even triple opt in processes. Most sign up form-builders and email marketing platforms will give you this option and flexibility. Even things like having an option for "Subscribe to my Newsletter" left unchecked by default will help.

Conclusion

Additional resources include:

- Nonprofit Guidelines for Cybersecurity and Privacy white paper (PDF)
- Security and Compliance Information for Nonprofit Organizations
- Microsoft Trust Center — GDPR

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