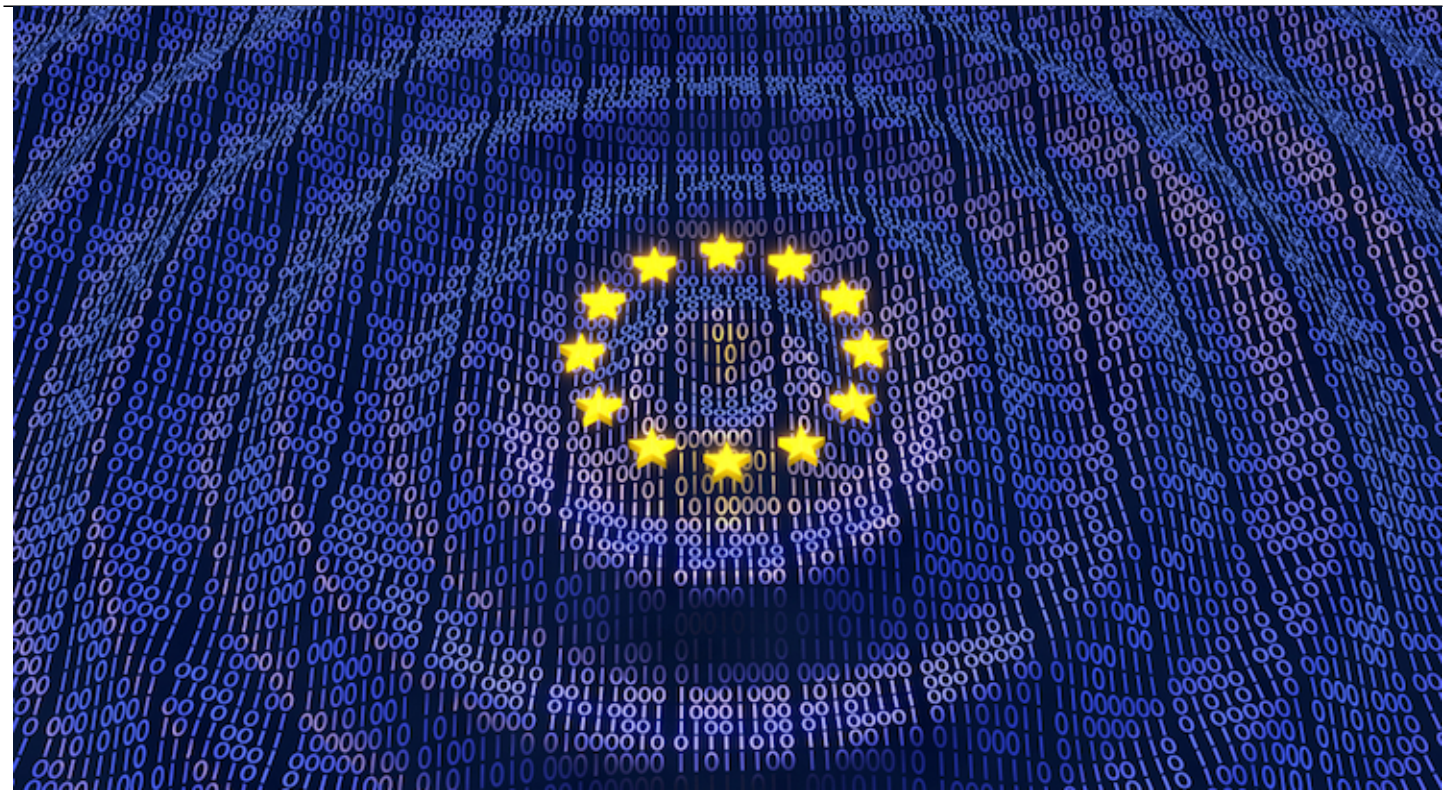
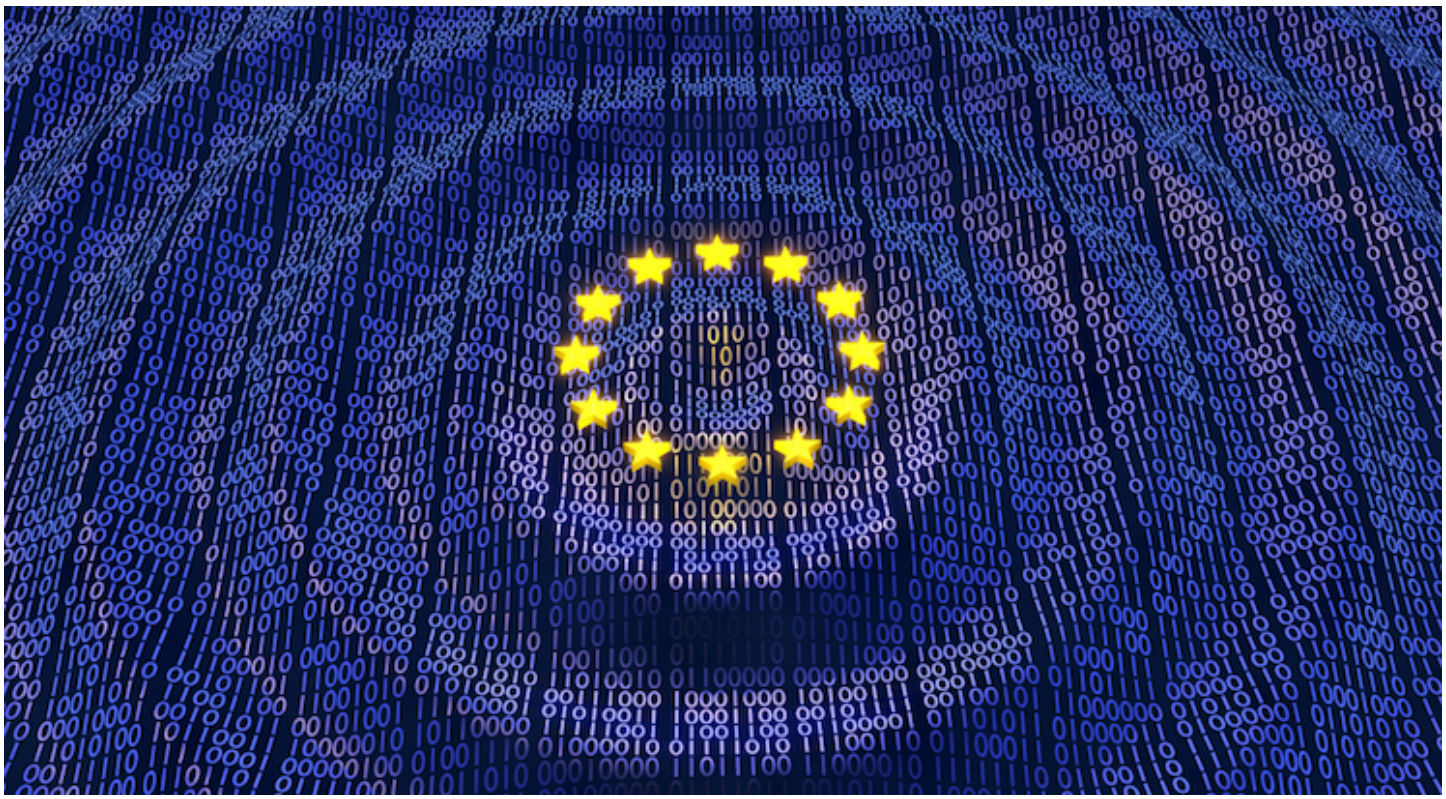
Nonprofit Knowledge: Does GDPR Apply to Nonprofits?

Technology, Privacy, and eCommerce





General Data Protection Regulation (GDPR) will become enforceable on May 25, 2018, after the expiration of the 2-year transition period. As companies prepare for compliance in anticipation of the enforcement date, nonprofits should also ensure that they are complying with GDPR if it applies to

them.

In fact, GDPR applies not only to non-EU for-profit companies, but also to nonprofits that collect or otherwise process any information relating directly or indirectly to identifiable individuals in connection with the offer of goods and/or services to EU residents.

There is no exception for nonprofits in GDPR. A nonprofit organization could be considered to provide “goods and services” by holding conferences or meetings in the European Union or monitoring the online behavior of EU residents who visit a website.

Although nonprofits that operate primarily or exclusively in the United States may consider themselves not subject to GDPR, if a nonprofit organization collects or stores personal data about an EU resident, such as donors, members, grantors, or grantees, or collects website behavior from EU residents, that organization needs to ensure that it is in compliance with GDPR. Below are the main areas for nonprofits to consider:

Financial penalties

Failure to comply with GDPR can expose a nonprofit to significant penalties, at a minimum up to €10 million, or two percent of the worldwide annual revenue of the prior fiscal year, whichever is higher. These penalties could have a serious impact on the finances of a nonprofit, and it is worth spending time now to ensure that you are in compliance.

Cross-functional reach

GDPR compliance reaches into the depths of a nonprofit’s operational structure, and is not limited to IT, legal, or membership. An organization that is subject to GDPR is expected to be transparent in its outward-facing policies about how information is collected, used, stored, and destroyed, as well as ensure that its internal operations are consistent with such policies. For example, does an organization’s eCRM have the ability to honor a donor’s request for their record to be permanently deleted, exercising their “right to erasure” or “right to be forgotten?” Also, your organization will need to be prepared to address the required 72-hour data security breach notifications and other notices as required by GDPR.

International data transfers

Many nonprofits are data controllers that contract with data processors to store and manage the personal data of EU residents on their behalf. These data processors are also subject to GDPR, and nonprofits should, therefore, ensure that their contracts with such companies are amended to ensure compliance. If a nonprofit is a 501(c)(6) trade association, it may be able to avail itself of the self-certification mechanism provided by the EU-US Privacy Shield. However, 501(c)(3)s and other nonprofits likely cannot do so because they are not subject to the jurisdiction of the Federal Trade Commission (FTC). As an alternative to the Privacy Shield self-certification, nonprofits can avail themselves of one of the sets of EU-approved model clauses when amending vendor contracts to help further such compliance.

DPOs

One key component of GDPR is the appointment of a Data Protection Officer (DPO). DPOs are

expected to work cross-functionally and have an impact on an organization as it operates in compliance with GDPR. A DPO is required when organizations "monitor individuals systematically and on a large scale," or that "process special categories of (sensitive) personal data on a large scale." If an organization does not systematically monitor individuals on a large scale, it may not need a DPO, but it should still appoint someone internally to be the "hub" of GDPR compliance.

Smaller organizations

Organizations may assume that they are exempt from GDPR because there is a limited exception from the Article 30 requirements for companies that have fewer than 250 employees. GDPR does provide smaller organizations with less than 250 employees that do not systematically control or process information, with a limited exception from the broader record-keeping requirements, under certain circumstances. This is *not* an exception from GDPR compliance overall, but could minimize the record-keeping necessary to comply. However, the exception is very narrow and organizations should not assume that they will be able to avail themselves of it.

Nonprofit organizations should take GDPR compliance seriously. If your organization has not yet evaluated whether it needs to comply with GDPR, you should do so as quickly as possible before GDPR enforcement takes effect.

Lakshmi Sarma Ramani

Member

Outside GC LLC

Lakshmi Sarma Ramani was the general counsel of the National Association for the Education of Young Children and senior attorney at The Nature Conservancy. She is currently a member of the firm at Outside GC LLC where she is the outside general counsel to multiple nonprofit organizations.