Lawyers Alliance FOR NEW YORK
Connecting Lawyers, Nonprofits, and Communities

Updated August 14, 2025

The European Union's General Data Protection Regulation: What Nonprofits Need to Know

The General Data Protection Regulation (the GDPR) implemented by the European Union (the EU) in 2018 governs the way in which companies and organizations may process, store, and utilize the personal data of individuals. Now in its seventh year of enforcement, the GDPR continues to have far-reaching implications not only for companies and organizations based in the EU, but also for entities around the world that interact with EU residents. This Legal Alert will provide background on the GDPR as well as information and action items for nonprofits who may be subject to the regulation.

What is the GDPR?

In addition to reshaping how personal data is handled, the GDPR expanded the scope of who is covered by European privacy laws and significantly increased the associated fines and penalties. If an entity that is subject to the GDPR fails to comply, it can be hit with a penalty of either up to €20 million[1] or 4% of its worldwide annual revenue of the prior financial year, whichever is higher.[2,3] Note that despite being in force for several years, the GDPR is still evolving. The European Commission and national regulators continue to refine its enforcement mechanisms and clarify its application through guidance, enforcement actions, and case law.

While high-profile enforcement actions have predominantly targeted large corporations, and it remains uncertain how aggressively the EU would pursue enforcement actions against US-based nonprofits, it is important to emphasize that *the GDPR does not include a carve-out for nonprofit organizations*. Like for-profit companies, nonprofits regularly acquire individual personal data. In the nonprofit context, organizations might collect information from their donors, customers, clients, and the individuals they serve in their communities, including names, birth dates, email addresses, payment information and donation and volunteer histories. If EU citizens interact with your nonprofit in a way that generates personal data (e.g., through donations, email sign-ups, or website engagement), your organization may be subject to the GDPR, and it will be particularly important for your organization to understand the rules of the GDPR to ensure proper compliance and avoid violations.

The GDPR and US Entities

Although the GDPR was enacted by the EU, its reach extends far beyond Europe's borders. The law does not only apply to companies that operate within the EU. In fact, the law specifically includes

[1] As of May 28, 2025, €20 million is equal to roughly $22,580,881 USD.
[2] Less severe infringements could result in a fine of up to €10 million, or 2% of the firm's worldwide annual revenue from the preceding financial year, whichever amount is higher. As of May 28, 2025, €10 million is equal to roughly $11,290,440 USD. See https://gdpr.eu/fines/.
[3] Between 2018 and 2025, regulators in EU countries levied large fines against a number of companies, including, but not limited to, big tech firms based in the US such as Amazon, Google, and Meta.

language that applies to companies operating outside of the EU if they otherwise engage people within the EU. Article 3 of the GDPR states:

> "This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
>
> (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
>
> (b) the monitoring of their behavior as far as their behavior takes place within the Union."

In general, this means that even US-based nonprofits without a physical presence in Europe may be required to comply with the GDPR. If your organization "offer(s) goods or services" within the EU or if your organization "monitor(s) the behavior of people" within the EU, then your organization must comply with the GDPR. While there is no exact definition for either term, practically speaking, a nonprofit could be considered to be offering goods and services or monitoring the behavior of people within the EU in several ways.

For example, a nonprofit that sells merchandise through its website and ships to EU countries would likely fall within the GDPR's scope. Even without sales, having a multilingual website tailored to EU audiences, or referencing EU-based donors or funders, may suggest that the nonprofit is "offering goods or services" in the EU.

With respect to monitoring the behavior of people within the EU, any nonprofit that uses cookies to track website visitors or collects analytics data may be deemed to be engaging in behavioral monitoring under the regulation.[4] Organizations should be aware of their methods used to analyze donors, clients, customers, employees or any other individual, whether online or offline.

To summarize, on the most basic level, if your nonprofit has ever received a donation from someone within the EU, or included someone within the EU on your newsletter listserv, your organization has collected personal data and is likely subject to the GDPR.

Frequently Asked Questions About the GDPR and Nonprofits

1. Does the GDPR apply to small US-based nonprofits?

Yes, size does not determine applicability. If your nonprofit collects personal data from individuals in the EU, even a single donation or newsletter signup, it could fall within the GDPR's scope.

2. What counts as "personal data" under the GDPR?

Personal data includes any information that can identify an individual, such as names, addresses, emails, phone numbers, IP addresses, and even cookie data.

3. Do we need to hire a Data Protection Officer (DPO)?

Not necessarily. The GDPR only requires a DPO if your organization engages in large-scale systematic

[4] See generally, https://gdpr.eu/cookies/.

monitoring or processes special categories of data. However, assigning a point person to oversee compliance is recommended.

4. Is consent always required before collecting personal data?

Not always, but it is one of the primary lawful bases for data collection. In most nonprofit contexts (e.g., newsletters, donation platforms), consent is the safest and most practical basis to rely on.

5. What happens if we don't comply?

Your organization may face fines which can be substantial. Your organization may also face reputational risk and loss of donor trust.

Considerations for Nonprofits Potentially Subject to the GDPR

Determining exactly what steps need to be taken can be a challenging question that depends on your organization and specifically what it does with data. If you are worried about your organization's GDPR compliance, you should carefully evaluate your organization's risks and potential gaps in GDPR compliance. At a minimum, your organization should:

- *Audit your data* – Review what personal data your organization collects, where it comes from, how it is stored, and who has access to it.

- *Evaluate GDPR applicability* – Determine whether your organization's activities fall under the GDPR's scope based on your interactions with individuals in the EU.

- *Review your website* – Check for use of cookies, analytics tools, or contact forms that collect data from EU users. Implement cookie banners and consent mechanisms where needed.

- *Update your Privacy Policy* – Ensure your organization's privacy policy is GDPR-compliant and easily accessible. Notify users of any material changes.

- *Train your team* – Educate staff and volunteers about GDPR requirements and their role in ensuring compliance.

Depending on the size of your organization and the amount of data you collect, other potential steps your organization might need to take include:

- *Getting consent* – Prior to the collection of any personal data, data subjects must provide you consent that is "freely given, specific, informed, and unambiguous" through a "clear affirmative action." User and donor consent can be obtained on your website through explicit responses to "opt-in" prompts, such as asking users whether they "accept" or "reject" the site's use of cookies.[5]

[5] See generally, https://gdpr.eu/gdpr-consent-requirements/.

- *Performing a Data Protection Impact Assessment (DPIA)* – A DPIA is an assessment required by companies that are subject to the GDPR any time they "begin a new project that is likely to involve a 'high risk' to other people's personal information."[6] If you collect sensitive data or undertake high-risk processing, you may want to perform a DPIA. Be sure to document your mitigation efforts.

- *Establish a Breach Notification Plan* – Upon discovery of a breach of personal data that is under GDPR jurisdiction, organizations must sound the alarm to the relevant supervisory authority within 72 hours.[7,8] You should ensure your organization can notify the appropriate supervisory authority within 72 hours of a data breach.

- *Respect the "Right to Be Forgotten*" – Article 17 of the GDPR discusses consumers' rights to remove all data from an organization's storage in certain instances, including when the "personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed."[9]

- *Review Vendor Agreements* – Ensure any contracts with third-party service providers (such as CRM platforms or payment processors) include GDPR-compliant data protection clauses.

These are just a few examples of GDPR obligations, and compliance may require additional steps such as updating your privacy policy, revising contracts with third-party vendors, and training staff on data protection practices.

***

Lawyers Alliance and its network of attorneys are available to assist its clients with determining GDPR applicability and building compliant data practices. If you are concerned your organization may be subject to the GDPR, contact Lawyers Alliance as soon as possible.

This alert is meant to provide general information only, not legal advice. If you have questions about the GDPR, please contact Ciarra Chavarria at (212) 219-1800 ext. 228 or visit our website at www.lawyersalliance.org for further information.

For assistance in preparing this Legal Alert, Lawyers Alliance would like to thank Allison Shapiro, extern attorney from Skadden, Arps, Slate, Meagher & Flom.

---

[6] See generally, https://gdpr.eu/data-protection-impact-assessment-template/.
[7] See Article 33 of the GDPR: https://gdpr-info.eu/art-33-gdpr/ (Notification of a Personal Data Breach to the Supervisory Authority).
[8] Although this requirement applies to breaches of personal data that is under GDPR jurisdiction, many US states have passed their own data breach notification laws, such as the Stop Hacks and Improve Electronic Data Security Act (SHIELD Act) in New York. The SHIELD Act governs breach notification requirements for any organization, including nonprofits, which has received, collected, stored, or processed the computerized private information of a New York resident. For additional information, see www.lawyersalliance.org/userFiles/uploads/legal_alerts/SHIELD_Act_Legal_Alert.pdf.
[9] See generally, https://gdpr.eu/right-to-be-forgotten.

Lawyers Alliance for New York is the leading provider of business and transactional legal services for nonprofit organizations and social enterprises that are improving the quality of life in New York City neighborhoods. Our network of pro bono lawyers from law firms and corporations and staff of experienced attorneys collaborate to deliver expert corporate, tax, real estate, employment, intellectual property, and other legal services to community organizations. By connecting lawyers, nonprofits, and communities, Lawyers Alliance for New York helps nonprofits to develop and provide housing, stimulate economic opportunity, improve urban health and education, promote community arts, and operate and advocate for vital programs that benefit low-income New Yorkers of all ages.