Proskauer

General Data Protection Regulation and Charitable Organizations FAQs

Privacy Law Blog on **July 31, 2018**

In the context of enforcement of the European General Data Protection Regulation ("GDPR)[1] on May 25, 2018, charitable organizations have showed an increased concern as to whether the GDPR applies to them, and what being subject to the GDPR means.

Does the GDPR apply to my organization?

The GDPR applies to charitable organizations that process "personal data," regardless of their size. Personal data encompasses any information that may directly or indirectly identify an individual (for example, a name, date of birth, phone number or photo). The most commonly owned personal data by charitable organizations is the data concerning their donors or potential donors, the beneficiaries of the charity's programs, the volunteers, and more generally, any individual who interacts with the charity (employees, consultants, external service providers, etc.). The definition of personal data is so broad that all charitable organizations necessarily process personal data.

If your organization is located in the European Union (EU), there is no doubt that the GDPR applies to it. For organizations not located in the EU, the GDPR will also apply to them if they offer goods and/or provide services to EU-based individuals, or monitor the behaviors of EU-based individuals. The GDPR expressly provides that the fact that no payment is required for the goods or services is irrelevant.

Therefore, a U.S. charitable organization which, as part of its activities, helps Syrian refugees based in France would need to comply with the GDPR, as it provides services to individuals based in the EU.

Organizations not located in the EU which fall under the scope of the GDPR because of certain data processing usually opt for a partial compliance approach, resulting in complying with the GDPR only with respect to the data of EU-based individuals.

My organization has to comply with GDPR; where should I start?

The first step towards compliance is to identify the type of personal data handled by your organization (this is called the data mapping). This is done by answering questions such as:

- What categories of data is my organization handling (human resources-related data, personal data with respect to donors, volunteers, and the beneficiaries of the organization's programs, etc.)?
- For each category of data, what kind of data does my organization have (name, phone number, personal address, email address, photo, etc.)?
- Does my organization handle any sensitive data? Sensitive data includes health data, data regarding sexual orientation, data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs and trade union membership, as well as any genetic and biometric data. The processing of sensitive data is only allowed in limited instances, thus the need to identify such data to ensure that the organization can legally process it.
- For what purpose is the data collected and used (human resources related obligations, fundraising, organization of events, volunteer management, etc.)?
- Is that data sent to any third party? If data is sent to a third party, where is that third party located? Is the data normally hosted in that country?
- When and how is the data collected and used, and for how long is that data retained?

Once the exercise of identifying all of the data handled by the organization and their purpose is completed, a practical plan for compliance may be established, addressing for each type of data what will need to be done.

What are the key principles of the GDPR that charitable organizations should keep in mind?

1. Limit personal data processing. The GDPR provides that personal data needs to be obtained only for specified and lawful purposes. For example, in order for a charitable organization to manage the payment of its members' contributions, the organization is justified in collecting the names and contact information of its members, and in keeping such data for the duration of the membership.
2. Inform. One of the key principle of the GDPR is transparency, so organizations must inform the individuals what data they have in a concise and intelligible way, and in plain language. For instance, a privacy policy should be short and explanatory, and a link to it should be included in all of the organization's

communications.

3. Insure that data subjects' rights are respected. Under the GDPR individuals have, in particular, the right to ask confirmation as to whether or not personal data concerning them is being processed, and where and for what purpose. They are also entitled to object to the processing of their data, have personal data rectified if it is inaccurate or incomplete, and to request the deletion or removal of personal data. Organizations should designate a reference person who will answer all potential requests.
4. Ensure the security of personal data. The GDPR requires personal data to be processed in a way ensuring its security. Charitable organizations have to ensure that appropriate technical or organizational measures are being used to protect personal data against unauthorized or unlawful processing and against accidental loss, destruction or damage.

Is consent required to send solicitations or communications to donors or potential donors?

Donation solicitations, as well as communications about a charitable organization's activities are deemed marketing communications which when sent via email or text messages fall under the Privacy and Electronic Communications Directive 2002/58/EC on Privacy and Electronic Communications (known as the ePrivacy Directive). Direct marketing under the ePrivacy Directive is allowed in respect to individuals who have given their prior consent.

The ePrivacy Directive provides for an exception to consent, when the communication is sent to individuals to whom services or products are advertised similar to the products or services purchased by them in the past. This exception rarely applies to charitable organizations, as they are not often selling products or services, leaving them with the obligation to obtain consent, which can be a real issue.

To be validly obtained, consent has to be freely given, and be specific, informed and an unambiguous indication of the individual's agreement to the processing of its personal data. Pre-ticked boxes on donation forms therefore need to be unticked.

As communications sent by regular mails do not fall under the ePrivacy Directive, and therefore do not require consent, many European-based charitable organizations seeking funding still spend significant resources in mailing donors and potential donors.

What are the penalties in case of non compliance with the GDPR?

The penalties under the GDPR are the same for all organizations, irrespective of the fact that they conduct charitable activities or not. For the most serious instances of non compliance, organizations may be fined up to 4 percent of the organization's annual revenue or €20 million, whichever is greated, although it seems unlikely that the regulatory authorities would sanction charitable organizations with such high amounts. More likely is the detrimental impact on the organization's reputation that a non-compliance with the GDPR will have, and the risk of losing the trust of supporters and donors.

[1] Regulation (EU) 2016/679

View Original

Related Professionals

- **Stéphanie Martinier**
  Partner